ΧΡΗΣΗ CAMENISCH-LYSYANSKAYA ΨΗΦΙΑΚΩΝ ΥΠΟΓΡΑΦΩΝ ΚΑΙ ΑΠΟΔΕΙΚΤΙΚΩΝ ΠΡΩΤΟΚΟΛΛΩΝ ΜΗΔΕΝΙΚΗΣ ΓΝΩΣΗΣ ΣΕ ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ

του Θεόφιλου Κανακάρη

Μεταπτυχιακό Μάθημα : Διπλωματική Εργασία

Επιβλέποντες Καθηγητές :
Ιωάννης Σταματίου, Κωνσταντίνος Λαμπρινουδάκης

Μεταπτυχιακό Πρόγραμμα Σπουδών :
Ασφάλεια Ψηφιακών Συστημάτων

Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιά

ΠΕΡΙΕΧΟΜΕΝΑ

Ενότητα **Σελίδα**

1. Εισαγωγή

Η συγκεκριμένη εργασία γράφτηκε στα πλαίσια του μαθήματος με τίτλο '**Διπλωματική Εργασία**' του **Μεταπτυχιακού Προγράμματος Σπουδών** με τίτλο '**Ασφάλεια Ψηφιακών Συστημάτων**' του **Τμήματος Ψηφιακών Συστημάτων** του **Πανεπιστημίου Πειραιά**. Προσωπικά θα ήθελα να ευχαριστήσω τους δύο επιβλέποντες καθηγητές, τους κυρίους **Ιωάννη Σταματίου**, **Επίκουρο Καθηγητή** στο **Τμήμα Μαθηματικών** του **Πανεπιστημίου Ιωαννίνων** και **Κωνσταντίνο Λαμπρινουδάκη**, **Αναπληρωτή Καθηγητή** στο Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιά. Ιδιαίτερα τον πρώτο για την ανάθεση του θέματος αυτής της εργασίας σε εμένα, τη γνωστοποίηση των επιστημονικών πηγών στις οποίες βασίστηκα σε πολύ σημαντικό βαθμό για να συγγράψω την εργασία, καθώς και για τη διόρθωσή της.

Η συγκεκριμένη εργασία αφορά την χρήση των *Camenisch-Lysyanskaya (CL) Ψηφιακών Υπογραφών* και των *Αποδεικτικών Πρωτοκόλλων Μηδενικής Γνώσης (Zero Knowledge Proof (zkp) Protocols)* σε *Ψηφιακά Πιστοποιητικά*. Συγκεκριμένα μελετάται ο τρόπος με τον οποίο εφαρμόζεται το προηγούμενο σχήμα υπογραφών σε *ηλεκτρονικά* πιστοποιητικά, από μια αρμόδια *Αρχή* που τα εκδίδει. Αυτά χρησιμοποιούνται σε ηλεκτρονικές συναλλαγές των νομίμων κατόχων τους με διάφορους *φορείς*. Επίσης περιγράφονται αναλυτικά διάφορα zkp πρωτόκολλα που εκτελούνται σε τέτοιες ηλεκτρονικές συναλλαγές και αποδεικνύουν την ισχύ προτάσεων σχετικών με το περιεχόμενο των παραπάνω πιστοποιητικών, χωρίς όμως το τελευταίο να αποκαλύπτεται.
Στην ενότητα 2 παρουσιάζεται η έννοια του πιστοποιητικού, καθώς και ο τρόπος με τον οποίο συμμετέχει σε συναλλαγές του νομίμου κατόχου του. Στην ενότητα 3 αναφέρονται σχολαστικά διάφορα μαθηματικά εργαλεία που είναι απαραίτητα για τη θεμελίωση των CL υπογραφών και των zkp πρωτοκόλλων που θα χρησιμοποιηθούν. Στην ενότητα 4 αναλύεται αυτό το σχήμα ψηφιακών υπογραφών και τέλος στην πέμπτη ενότητα περιγράφονται διεξοδικά τα παραπάνω zkp πρωτόκολλα.

2. Πιστοποιητικό και Χρήση του σε Συναλλαγές

Πιστοποιητικό είναι ένα έγγραφο [1] εκδιδόμενο από μια επίσημη Αρχή του οποίου το περιεχόμενο τεκμηριώνει κάποια στοιχεία για τον νόμιμο ιδιοκτήτη του. Ο τελευταίος μπορεί να είναι ένα άτομο ή ένας οργανισμός. Το πιστοποιητικό μπορεί να τεκμηριώνει μια ιδιότητα όπως μια εργασιακή θέση κάποιου, για παράδειγμα προϊστάμενος, υπάλληλος, ή έναν τύπο εταιρείας, για παράδειγμα ανώνυμη, εταιρεία τροφίμων. Επίσης το πιστοποιητικό μπορεί να αποδεικνύει μια κατάσταση, όπως ατομικά στοιχεία κάποιου, ένα προσόν, για παράδειγμα πτυχίο, ένα προνόμιο, όπως βεβαίωση φοροαπαλλαγής, ή ένα δικαίωμα, όπως δίπλωμα οδήγησης. Το περιεχόμενό του αποτελείται από πληροφορίες που αφορούν τον νόμιμο ιδιοκτήτη του και είναι κατηγοριοποιημένες ως τιμές σε διάφορα *πεδία* του πιστοποιητικού. Τέτοια είναι για παράδειγμα, το όνομα του νόμιμου κατόχου, η ημερομηνία ισχύος σε ένα δίπλωμα οδήγησης, ο αριθμός τέκνων σε ένα πιστοποιητικό οικογενειακής κατάστασης, το χρώμα των ματιών και το ύψος σε μια αστυνομική ταυτότητα. Οι παραπάνω πληροφορίες έχουν χαρακτήρα *προσωπικών δεδομένων* από τη στιγμή που αφορούν τον νόμιμο ιδιοκτήτη του πιστοποιητικού και για αυτόν τον λόγο η Αρχή που το εκδίδει το αποστέλλει μονάχα σε αυτόν δίχως να το κοινοποιεί δημόσια. Για τον ίδιο λόγο επίσης, ο νόμιμος κάτοχός του θεωρείται ότι ακολουθεί την ίδια πολιτική. [1] Όταν εκδίδεται ένα πιστοποιητικό από την Αρχή, αυτή το υπογράφει

προκειμένου να καθίσταται δυνατή μια μελλοντική επιβεβαίωση της εγκυρότητάς του.

Με βάση τις τιμές κάποιων από τα πεδία ενός πιστοποιητικού, είναι δυνατή ή μη η εκχώρηση δικαιωμάτων στον νόμιμο κάτοχο, ή η πρόσβασή του σε υπηρεσίες. Για παράδειγμα, αν η τιμή του πεδίου της ημερομηνίας ισχύος στο δίπλωμα οδήγησης είναι μεταγενέστερη της τωρινής ημερομηνίας, τότε ο ιδιοκτήτης του μπορεί να οδηγήσει, διαφορετικά όχι. Αν πάλι ο αριθμός τέκνων που αναγράφεται σε ένα πιστοποιητικό οικογενειακής κατάστασης είναι μεγαλύτερος από μια προκαθορισμένη τιμή, τότε ο νόμιμος κάτοχός του μπορεί να αποκτήσει το δικαίωμα φορολογικής ελάφρυνσης και μόνο τότε. Τέλος, αν η πρόσβαση σε υπηρεσίες ενός δήμου επιτρέπεται μόνο στους δημότες του, τότε κάποιος πολίτης μπορεί να έχει πρόσβαση σε αυτές μόνο εφόσον στο πιστοποιητικό εντοπιότητάς του αναγράφεται ο συγκεκριμένος δήμος. Το πιστοποιητικό ελέγχεται ως προς τις τιμές συγκεκριμένων πεδίων από έναν αρμόδιο φορέα, όπως η Αστυνομία και η εφορία στην περίπτωση του διπλώματος οδήγησης και πιστοποιητικού οικογενειακής κατάστασης αντίστοιχα, εφόσον προηγούμενα επιβεβαιωθεί η εγκυρότητά του από την υπογραφή της Αρχής που το εξέδωσε. Αν αυτές οι τιμές ικανοποιούν τα κριτήρια που έχουν τεθεί, τότε και μόνο τότε ο ιδιοκτήτης αποκτάει το αντίστοιχο δικαίωμα, ή του επιτρέπεται η πρόσβαση σε υπηρεσίες. Προκειμένου ο φορέας να επιβεβαιώσει την εγκυρότητα και να κάνει μετά τον έλεγχο, έχει πρόσβαση στο πιστοποιητικό, δηλαδή στις τιμές των υπό εξέταση πεδίων του καθώς και σε εκείνες όλων των άλλων των υπολοίπων πεδίων του. Με τον τρόπο αυτό όμως εγείρεται θέμα *ασφάλειας* αφού παραβιάζεται η *ιδιωτικότητα* των τιμών όλων των πεδίων. Μάλιστα το πρόβλημα εντείνεται όταν κάποιες από αυτές τις τιμές εκτός από προσωπικά έχουν και χαρακτήρα *ευαίσθητων* δεδομένων. Για παράδειγμα, ο αριθμός τέκνων, το χρώμα των ματιών και το βάρος είναι προσωπικά δεδομένα τα οποία πρέπει να μένουν εμπιστευτικά, το ίδιο όμως ισχύει σε μεγαλύτερο βαθμό για ευαίσθητα δεδομένα όπως το ονοματεπώνυμο, τα αποτελέσματα ιατρικών εξετάσεων, ή το ποινικό ιστορικό.

Το πρόβλημα αντιμετωπίζεται στην περίπτωση που το πιστοποιητικό είναι ηλεκτρονικό έγγραφο, οπότε και λέγεται ψηφιακό ή ηλεκτρονικό πιστοποιητικό. Δηλαδή ένας φορέας μπορεί να επιβεβαιώσει την εγκυρότητα ενός ψηφιακού πιστοποιητικού και να ελέγξει αν ικανοποιούνται τα προκαθορισμένα κριτήρια από τις τιμές συγκεκριμένων πεδίων του, χωρίς να έχει πρόσβαση σε αυτό. Έτσι από τη στιγμή που δεν μπορεί να έχει πρόσβαση σε καμία τιμή των πεδίων του πιστοποιητικού, τότε το παραπάνω πρόβλημα ασφάλειας λύνεται και η ιδιωτικότητα των τιμών όλων των πεδίων τηρείται. Παρόλο που ο φορέας δεν έχει πλέον πρόσβαση στις τιμές των υπό εξέταση πεδίων, ο έλεγχος σχετικά με το αν τηρούν τα κριτήρια μπορεί να διενεργηθεί με την χρήση zkp πρωτοκόλλων. Με την εκτέλεση των τελευταίων, μεταξύ του νομίμου κατόχου και του φορέα, ελέγχεται αν οι προηγούμενες τιμές ικανοποιούν τα προκαθορισμένα κριτήρια εξασφαλίζοντας παράλληλα την ιδιωτικότητά τους αλλά και την ιδιωτικότητα των τιμών των υπολοίπων πεδίων. Πριν από αυτόν τον έλεγχο εξετάζεται επίσης μέσω της εκτέλεσης των zkp πρωτοκόλλων η εγκυρότητα του ψηφιακού πιστοποιητικού. [1] Για παράδειγμα, αν το κριτήριο για φορολογική ελάφρυνση είναι η ύπαρξη τουλάχιστον τριών τέκνων, τότε ένας που έχει τέσσερα τέκνα θα εκτελέσει με τον φορέα το αντίστοιχο zkp πρωτόκολλο ώστε να του αποδείξει την εγκυρότητα του πιστοποιητικού του και μετά ένα άλλο zkp πρωτόκολλο για να του αποδείξει πως η τιμή που αναγράφεται στο πεδίο του αριθμού τέκνων είναι μεγαλύτερη ή ίση του 3. Ο φορέας δε θα μάθει ότι η τιμή σε αυτό το πεδίο είναι ίση με 4, άλλωστε δεν το

χρειάζεται. Αυτό που τον νοιάζει είναι αν αυτή η τιμή είναι μεγαλύτερη ή ίση του 3, προκειμένου να εκχωρήσει το δικαίωμα της φορολογικής ελάφρυνσης στον συγκεκριμένο πολίτη, ή μικρότερή του για να του το αρνηθεί.
Παρόλο που τα ψηφιακά πιστοποιητικά είναι απόρρητα σε όλους εκτός από τους νομίμους κατόχους τους και την εκδότρια Αρχή, η ιδιωτικότητα αυτή αναγκαστικά καταστρατηγείται στην περίπτωση που τα κριτήρια ελέγχου απαιτούν από κάποια πεδία του πιστοποιητικού να έχουν κάποιες δεδομένες τιμές. Αν το πιστοποιητικό ενός πολίτη τηρεί αυτήν την απαίτηση, τότε με την χρήση του αντίστοιχου zkp πρωτοκόλλου αποδεικνύεται στον φορέα πως τα υπό εξέταση πεδία του συγκεκριμένου πιστοποιητικού έχουν όντως αυτές τις δεδομένες τιμές. Έτσι όμως παραβιάζεται η ιδιωτικότητα των τιμών που έχουν αυτά τα πεδία. Από την άλλη τηρείται η ιδιωτικότητα των τιμών των υπολοίπων πεδίων από τη στιγμή που ο φορέας δεν έχει πρόσβαση στο πιστοποιητικό και η εκτέλεση του zkp πρωτοκόλλου δεν αποκαλύπτει καμιά από αυτές. Για παράδειγμα, αν ένα επίδομα δίνεται μόνο στους δημοσίους υπαλλήλους με πανεπιστημιακή μόρφωση, τότε κάποιος εργαζόμενος του δημοσίου τομέα που τηρεί αυτό το κριτήριο θα κληθεί να αποδείξει στον φορέα με την χρήση ενός zkp πρωτοκόλλου ότι το αντίστοιχο πιστοποιητικό του είναι έγκυρο και με ένα άλλο zkp πρωτόκολλο ότι στο πεδίο που αφορά το επίπεδο μόρφωσης αναγράφεται η ένδειξη '*Πανεπιστήμιο*'. Ο φορέας θα πειστεί και θα κινήσει τις διαδικασίες για την παροχή του επιδόματος στο συγκεκριμένο δημόσιο υπάλληλο, ταυτόχρονα όμως θα γνωρίζει και το επίπεδο μόρφωσής του παραβιάζοντας την ιδιωτικότητα της τιμής '*Πανεπιστήμιο*' η οποία περιέχεται στο πεδίο που σχετίζεται με την μόρφωση. Περισσότερα σχετικά με τον ορισμό και την χρήση των zkp πρωτοκόλλων στις ηλεκτρονικές συναλλαγές των ψηφιακών πιστοποιητικών αναφέρονται στην ενότητα 5.

3. Μαθηματικά Εργαλεία

Στην ενότητα αυτή παρουσιάζονται μαθηματικά εργαλεία, όπως ορισμοί, προτάσεις, θεωρήματα και ισχυρισμοί, τα οποία είναι απαραίτητα για την οικοδόμηση του σχήματος των CL υπογραφών και των zkp πρωτοκόλλων που αναπτύσσονται στις επόμενες ενότητες. Σχεδόν για όλες τις προτάσεις παρατίθενται και οι αποδείξεις τους. Τα μαθηματικά εργαλεία είναι τα εξής [2]:

Ορισμός 1

1. *Πρώτος αριθμός* είναι ο φυσικός αριθμός που είναι μεγαλύτερος του 1 και οι διαιρέτες του είναι ο εαυτός του και το 1.
2. Δύο αριθμοί είναι *μεταξύ τους πρώτοι* όταν ο *μέγιστος κοινός διαιρέτης* τους είναι το 1.

Πρόταση 1

Έστω p πρώτος αριθμός και $n \in \mathbb{N}$, τότε αν οι p, n είναι πρώτοι μεταξύ τους, το p δεν είναι διαιρέτης του n και αντιστρόφως.

Απόδειξη

Έστω η περίπτωση που οι p, n είναι πρώτοι μεταξύ τους. Τίθεται ο ισχυρισμός ότι το p είναι διαιρέτης του n. Αυτό σημαίνει πως ο μέγιστος κοινός διαιρέτης των p, n είναι το p, το οποίο ως πρώτος αριθμός, λόγω της πρότασης 1 του Ορισμού 1, είναι μεγαλύτερο από το 1 και άρα διαφορετικό του. Δηλαδή ο μέγιστος κοινός διαιρέτης των p, n, διαφέρει από το 1. Το συμπέρασμα αυτό όμως καταλήγει σε άτοπο, καθώς

τα p,n ως πρώτοι που είναι μεταξύ τους, θα έχουν ως μέγιστο κοινό τους διαιρέτη το 1 σύμφωνα με την πρόταση 2 του Ορισμού 1. Επομένως το p δε διαιρεί το n.
Αντίστροφα, έστω η περίπτωση που το p δεν είναι διαιρέτης του n. Τότε το p δεν είναι κοινός διαιρέτης των p,n. Το 1 είναι κοινός τους διαιρέτης και επειδή δεν υπάρχει άλλος διαιρέτης του p εκτός από τους 1 και p, το 1 θα είναι και ο μοναδικός κοινός τους διαιρέτης, άρα και ο μέγιστος κοινός τους. Επομένως σύμφωνα με την πρόταση 2 του Ορισμού 1, οι p,n είναι πρώτοι μεταξύ τους.

Πρόταση 2

Αν p,q πρώτοι αριθμοί με $p \neq q$, τότε είναι πρώτοι μεταξύ τους.

Απόδειξη

Οι διαιρέτες του πρώτου αριθμού p είναι το 1 και το ίδιο το p. Σύμφωνα με την υπόθεση ισχύει $q \neq p$ και λόγω της πρότασης 1 του Ορισμού 1 θα είναι $q > 1$ και άρα $q \neq 1$. Δηλαδή το q διαφέρει από όλους τους διαιρέτες του p και συνεπώς δεν το διαιρεί. Λόγω του τελευταίου συμπεράσματος και του γεγονότος ότι το q είναι πρώτος, τα p,q είναι πρώτοι μεταξύ τους σύμφωνα με την Πρόταση 1.

Πρόταση 3

Έστω $a,b \in \mathbb{N}$, τότε αν οι a,b είναι πρώτοι μεταξύ τους $\exists x, y \in \mathbb{Z}$ ώστε

$$a \cdot x + b \cdot y = 1$$

και αντιστρόφως. Όταν τα a,b είναι πρώτοι μεταξύ τους και δοθούν ως είσοδοι στον *επεκτεινόμενο Ευκλείδειο αλγόριθμο*, τότε υπολογίζονται από αυτόν $x, y \in \mathbb{Z}$ που ικανοποιούν την προηγούμενη εξίσωση.

Πρόταση 4

Αν p πρώτος αριθμός, $a,b \in \mathbb{N}$ και το p διαιρεί το γινόμενο $a \cdot b$, τότε το p διαιρεί το a ή το b.

Απόδειξη

Έστω ότι το p δε διαιρεί κανένα από τα a,b. Τότε, μια και το p είναι πρώτος, σύμφωνα με την Πρόταση 1 τα p,a είναι πρώτοι μεταξύ τους, όπως επίσης και τα p,b. Επομένως λόγω της Πρότασης 3 $\exists x_1, y_1, x_2, y_2 \in \mathbb{Z}$ ώστε

$$\begin{cases} p \cdot x_1 + a \cdot y_1 = 1 \\ p \cdot x_2 + b \cdot y_2 = 1 \end{cases}.$$

Από αυτό το σύστημα εξισώσεων συνεπάγεται πως

$$\begin{cases} a \cdot y_1 = 1 - p \cdot x_1 \\ b \cdot y_2 = 1 - p \cdot x_2 \end{cases} \Rightarrow a \cdot y_1 \cdot b \cdot y_2 = (1 - p \cdot x_1) \cdot (1 - p \cdot x_2) \Rightarrow$$

$$a \cdot b \cdot y_1 \cdot y_2 = 1 - p \cdot x_2 - p \cdot x_1 + p^2 \cdot x_1 \cdot x_2 \Rightarrow a \cdot b \cdot y_1 \cdot y_2 = 1 - p \cdot (x_2 + x_1 - p \cdot x_1 \cdot x_2) \quad (1).$$

Έστω

$$\begin{cases} y_3 = y_1 \cdot y_2 \\ z = x_2 + x_1 - p \cdot x_1 \cdot x_2 \end{cases},$$

τότε $y_3, z \in \mathbb{Z}$ και η (1) γίνεται

$$a \cdot b \cdot y_3 = 1 - p \cdot z \Rightarrow (a \cdot b) \cdot y_3 + p \cdot z = 1.$$

Έτσι για τα $a\cdot b, p\in\mathbb{N}$, $\exists y_3, z\in\mathbb{Z}$ ώστε να ισχύει η τελευταία εξίσωση. Αυτό σύμφωνα με την Πρόταση 3 σημαίνει ότι τα $a\cdot b, p$ είναι πρώτοι μεταξύ τους και επειδή το p είναι πρώτος αριθμός, τότε σύμφωνα με την Πρόταση 1 δε διαιρεί το $a\cdot b$. Το τελευταίο συμπέρασμα καταλήγει σε άτοπο αφού έρχεται σε αντίθεση με την υπόθεση ότι το p διαιρεί το $a\cdot b$. Επομένως το p διαιρεί το a ή το b.

Πρόταση 5

Έστω $b,n,c\in\mathbb{N}$ με $n\geq 2$, $m\in\mathbb{N}^*$ και $\forall i\in\{1,..,n\}$ $a_i\in\mathbb{N}$. Τότε ισχύουν τα εξής:

1. Αν $\forall i\in\{1,..,n\}$ το a_i είναι πρώτος με το b, τότε το b είναι πρώτος με το γινόμενο $\prod_{i=1}^{n} a_i$ και αντιστρόφως.
2. Αν το c είναι πρώτος με το b, τότε το b είναι πρώτος με το c^m.

Απόδειξη

1.

Έστω η περίπτωση που $\forall i\in\{1,..,n\}$ το a_i είναι πρώτος με το b. Ισχύει $n\in\mathbb{N}$ με $n\geq 2$, οπότε για $n=2$ τα a_1, a_2 είναι το καθένα πρώτος με το b. Έτσι σύμφωνα με την Πρόταση 3 $\exists x_1, x_2, y_1, y_2\in\mathbb{Z}$ ώστε

$$\begin{cases} a_1\cdot x_1 + b\cdot y_1 = 1 \\ a_2\cdot x_2 + b\cdot y_2 = 1 \end{cases}.$$

Από αυτό το σύστημα εξισώσεων συνεπάγεται πως

$$(a_1\cdot x_1 + b\cdot y_1)\cdot(a_2\cdot x_2 + b\cdot y_2) = 1\cdot 1 = 1 \Rightarrow$$
$$a_1\cdot x_1\cdot a_2\cdot x_2 + a_1\cdot x_1\cdot b\cdot y_2 + b\cdot y_1\cdot a_2\cdot x_2 + b\cdot y_1\cdot b\cdot y_2 = 1 \Rightarrow$$
$$a_1\cdot a_2\cdot x_1\cdot x_2 + b\cdot(a_1\cdot x_1\cdot y_2 + y_1\cdot a_2\cdot x_2 + y_1\cdot b\cdot y_2) = 1 \quad (2).$$

Έστω

$$\begin{cases} x_3 = x_1\cdot x_2 \\ z = a_1\cdot x_1\cdot y_2 + y_1\cdot a_2\cdot x_2 + y_1\cdot b\cdot y_2 \end{cases},$$

τότε $x_3, z\in\mathbb{Z}$ και η (2) γίνεται

$$(a_1\cdot a_2)\cdot x_3 + b\cdot z = 1.$$

Έτσι για τα $a_1\cdot a_2, b\in\mathbb{N}$, $\exists x_3, z\in\mathbb{Z}$ ώστε να ισχύει η τελευταία εξίσωση. Αυτό σύμφωνα με την Πρόταση 3 σημαίνει ότι τα $a_1\cdot a_2, b$ είναι πρώτοι μεταξύ τους.

Έστω $n\geq 3$, τότε θα δειχτεί με τέλεια επαγωγή ότι $\forall k\in\{2,..,n\}$ τα $\prod_{i=1}^{k} a_i, b$ είναι πρώτοι μεταξύ τους. Για $k=2$ η απόδειξη είναι η ίδια όπως και προηγουμένως. Έστω ότι για κάποιο $k\in\{2,..,n-1\}$ τα $\prod_{i=1}^{k} a_i, b$ είναι πρώτοι μεταξύ τους. Θα δειχτεί ότι και τα $\prod_{i=1}^{k+1} a_i, b$ είναι πρώτοι μεταξύ τους. Λόγω της παραπάνω υπόθεσης τα a_{k+1}, b είναι πρώτοι μεταξύ τους. Εφόσον τα $\prod_{i=1}^{k} a_i, a_{k+1}$ είναι το καθένα πρώτος με το

b, τότε αποδεικνύεται παρόμοια όπως και προηγουμένως ότι τα $\prod_{i=1}^{k+1} a_i, b$ είναι πρώτοι μεταξύ τους. Άρα $\forall k \in \{2,..,n\}$, το b είναι πρώτος με το $\prod_{i=1}^{k} a_i$ και επομένως για $k = n$ είναι πρώτος με $\prod_{i=1}^{n} a_i$.

Έστω η περίπτωση που το γινόμενο $\prod_{i=1}^{n} a_i$ είναι πρώτος με το b. Τότε σύμφωνα με την Πρόταση 3 $\exists x, y \in \mathbb{Z}$ ώστε

$$\left(\prod_{i=1}^{n} a_i\right) \cdot x + b \cdot y = 1.$$

$\forall k \in \{1,..,n\}$ η τελευταία εξίσωση γίνεται

$$a_k \cdot \left(\prod_{i=1, i\neq k}^{n} a_i\right) \cdot x + b \cdot y = 1 \ (3).$$

Έστω ότι $\forall k \in \{1,..,n\}$

$$z_k = \left(\prod_{i=1, i\neq k}^{n} a_i\right) \cdot x,$$

τότε $z_k \in \mathbb{Z}$ και η (3) γίνεται

$$a_k \cdot z_k + b \cdot y = 1.$$

Έτσι $\forall k \in \{1,..,n\}$, για τα $a_k, b \in \mathbb{N}$, $\exists z_k, y \in \mathbb{Z}$ ώστε να ισχύει η τελευταία εξίσωση. Αυτό σύμφωνα με την Πρόταση 3 σημαίνει ότι τα a_k, b είναι πρώτοι μεταξύ τους. Συνεπώς $\forall i \in \{1,..,n\}$ το a_i είναι πρώτος με το b.

2.

Έστω $m = 1$, τότε σύμφωνα με την υπόθεση το b είναι πρώτος με το c, δηλαδή με το $c^1 = c^m$.

Έστω $m \geq 2$. Αν τεθούν $n = m$ και $\forall i \in \{1,..,n\}$ $a_i = c$, τότε $\forall i \in \{1,..,n\}$ το a_i θα είναι πρώτος με το b και έτσι σύμφωνα με την Πρόταση 5.1 το b είναι πρώτος με το γινόμενο

$$\prod_{i=1}^{n} a_i = \prod_{i=1}^{n} c = c^n = c^m.$$

<u>Πρόταση 6</u>

Έστω p, q πρώτοι αριθμοί με $p \neq q$ και $a \in \mathbb{N}$, τότε αν καθένα από τα p, q διαιρεί το a, αυτό διαιρείται επίσης και από το γινόμενο $p \cdot q$ και αντιστρόφως.

<u>Απόδειξη</u>

Έστω η περίπτωση που καθένα από τα p, q διαιρεί το a. Τότε $\exists d_1, d_2 \in \mathbb{N}$ ώστε

$$\begin{cases} a = p \cdot d_1 \\ a = q \cdot d_2 \end{cases} \ (4).$$

Από αυτό το σύστημα εξισώσεων προκύπτει πως

$$p \cdot d_1 = q \cdot d_2.$$

Η τελευταία εξίσωση δηλώνει πως ο πρώτος αριθμός p διαιρεί το γινόμενο $q \cdot d_2$ και άρα λόγω της Πρότασης 4 θα διαιρεί το q ή το d_2. Επειδή το q είναι πρώτος όπως και το p με $p \neq q$, τότε λόγω της Πρότασης 2 τα p, q είναι πρώτοι μεταξύ τους και άρα σύμφωνα με την Πρόταση 1 ο πρώτος p δε διαιρεί το q. Επομένως το p διαιρεί το d_2 και έτσι $\exists d_3 \in \mathbb{N}$ ώστε

$$d_2 = p \cdot d_3 .$$

Λόγω της τελευταίας σχέσης, η δεύτερη εξίσωση της (4) γίνεται

$$a = q \cdot p \cdot d_3 \Rightarrow a = (p \cdot q) \cdot d_3 .$$

Από την τελευταία σχέση προκύπτει πως το γινόμενο $p \cdot q$ διαιρεί το a.

Έστω η περίπτωση που το γινόμενο $p \cdot q$ διαιρεί το a. Τότε $\exists d \in \mathbb{N}$ ώστε

$$a = p \cdot q \cdot d$$

και επομένως

$$\begin{cases} a = p \cdot (q \cdot d) \\ a = q \cdot (p \cdot d) \end{cases}.$$

Από την πρώτη και δεύτερη εξίσωση του τελευταίου συστήματος, προκύπτει πως τα p, q αντίστοιχα διαιρούν το a.

Ορισμός 2

1. Αν $n \in \mathbb{N}^*$, $\phi(n)$ είναι η *συνάρτηση φι του Euler* της οποίας η τιμή είναι ίση με το πλήθος όλων των φυσικών αριθμών από το σύνολο $\{1,..,n\}$, που είναι πρώτοι με το n.
2. Αν $n \in \mathbb{N}^*$ με $n \geq 2$, το $\mathbb{Z}_n^*$ είναι το σύνολο που περιέχει όλους τους φυσικούς αριθμούς από το σύνολο $\{1,..,n-1\}$, οι οποίοι είναι πρώτοι με το n.

Πρόταση 7

Αν p πρώτος αριθμός, τότε

$$\mathbb{Z}_p^* = \{1,..,p-1\} .$$

Απόδειξη

Όλοι οι αριθμοί του συνόλου $\{1,..,p-1\}$ είναι μικρότεροι ή ίσοι από το $p-1$ και συνεπώς μικρότεροι από το p. Από το τελευταίο συμπέρασμα προκύπτει πως κανένας τους δεν το έχει ως διαιρέτη του. Επομένως, σύμφωνα με την Πρόταση 1, μια και το p είναι πρώτος αριθμός, ο κάθε αριθμός του $\{1,..,p-1\}$ είναι πρώτος με το p. Άρα

$$\mathbb{Z}_p^* = \{1,..,p-1\} .$$

Ορισμός 3

Αν $a, b \in \mathbb{Z}$ και $n \in \mathbb{N}^*$, τα $adivn$, $a \bmod n$ είναι αντίστοιχα το *πηλίκο* και το *υπόλοιπο* της ακέραιας διαίρεσης του a με το n. Η σχέση

$$a \equiv b \bmod n$$

λέγεται *ισοδυναμία* και δηλώνει πως τα a, b είναι ισοϋπόλοιπα ως προς n, δηλαδή η ακέραια διαίρεση καθενός από αυτά με το το n παράγει το ίδιο υπόλοιπο.

Πρόταση 8

Αν $a,b,c,d \in \mathbb{Z}$, $n \in \mathbb{N}^*$, τότε ισχύουν τα εξής:

1. $(a \bmod n) \in \{0,..,n-1\}$.
2. Αν $a = b \bmod n$, τότε $a \equiv b \bmod n$.
3. Αν $a \equiv 0 \bmod n$, τότε το a είναι ακέραιο πολλαπλάσιο του n.
4. $(a \bmod n) \bmod n = a \bmod n$.
5. $(a+b) m \bmod n = \big((am \bmod n) + (bm \bmod n)\big) \bmod n$.
6. $(a \cdot b) m \bmod n = \big((am \bmod n) \cdot (bm \bmod n)\big) \bmod n$.
7. Αν $a \equiv b \bmod n$, τότε:
    1. $(a-b) \equiv 0 \bmod n$.
    2. $(a \cdot c) \equiv (b \cdot c) \bmod n$.
    3. Αν $c \equiv d \bmod n$, τότε $(a \cdot c) \equiv (b \cdot d) \bmod n$.

Ορισμός 4

Αν $n \in \mathbb{N}^*$ με $n \geq 2$ και $a \in \mathbb{Z}_n^*$, το $a^{-1} \in \mathbb{Z}_n^*$ είναι ο *αντίστροφος modulo* n του a όπου

$$\left(a \cdot a^{-1}\right) \bmod n = 1.$$

Πρόταση 9

Αν $n \in \mathbb{N}^*$ με $n \geq 2$ και $a \in \mathbb{Z}_n^*$, τότε υπάρχει ο αντίστροφος του a, είναι μοναδικός και υπολογίζεται από τον επεκτεινόμενο Ευκλείδειο αλγόριθμο.

Ορισμός 5

Αν $n \in \mathbb{N}^*$ με $n \geq 2$, $a \in \mathbb{Z}_n^*$ και $m \in \mathbb{Z}_-^*$, τότε

$$a^m \bmod n = \left(a^{-1}\right)^{-m} \bmod n.$$

Πρόταση 10

Αν $n \in \mathbb{N}^*$ με $n \geq 2$, $a \in \mathbb{Z}_n^*$, $b,c,m,k \in \mathbb{Z}$, τότε ισχύουν τα εξής:

1. Αν $a \equiv b \bmod n$, τότε $a^m \equiv b^m \bmod n$.
2. Αν $\left(a^m \cdot a^k \cdot b\right) \equiv c \bmod n$, τότε $\left(a^{m+k} \cdot b\right) \equiv c \bmod n$.
3. Αν $(a \cdot b)^m \equiv c \bmod n$, τότε $\left(a^m \cdot b^m\right) \equiv c \bmod n$.
4. Αν $\left(\left(a^m\right)^k \cdot b\right) \equiv c \bmod n$, τότε $\left(a^{m \cdot k} \cdot b\right) \equiv c \bmod n$.
5. Αν $\left(a^m \cdot b\right) \equiv c \bmod n$, τότε $b \equiv \left(a^{-m} \cdot c\right) \bmod n$.

Πρόταση 11

Αν $a,b \in \mathbb{Z}$, $n \in \mathbb{N}^*$ με

$$a \equiv b \bmod n$$

και οι b,n είναι πρώτοι αριθμοί μεταξύ τους, τότε και οι a,n είναι επίσης πρώτοι μεταξύ τους.

Απόδειξη

Επειδή

$$a \equiv b \bmod n,$$

τότε σύμφωνα με την Πρόταση 8.7.1 θα ισχύει

$$(a-b) \equiv 0 \bmod n$$

και συνεπώς λόγω της Πρότασης 8.3, το $a-b$ είναι ακέραιο πολλαπλάσιο του n. Δηλαδή $\exists d \in \mathbb{Z}$ ώστε

$$a-b = n \cdot d \quad (5).$$

Εφόσον οι b,n είναι πρώτοι μεταξύ τους, τότε σύμφωνα με την Πρόταση 3 $\exists x, y \in \mathbb{Z}$ ώστε

$$b \cdot x + n \cdot y = 1.$$

Η τελευταία εξίσωση συνεπάγεται ότι

$$b \cdot x = 1 - n \cdot y \quad (6).$$

Από την (5) προκύπτει ότι

$$(a-b) \cdot x = n \cdot d \cdot x \Rightarrow a \cdot x - b \cdot x = n \cdot d \cdot x \Rightarrow a \cdot x = n \cdot d \cdot x + b \cdot x \xrightarrow{(6)}$$

$$a \cdot x = n \cdot d \cdot x + 1 - n \cdot y \Rightarrow a \cdot x = n \cdot (d \cdot x - y) + 1 \Rightarrow a \cdot x - n \cdot (d \cdot x - y) = 1 \Rightarrow$$

$$a \cdot x + n \cdot (y - d \cdot x) = 1 \quad (7).$$

Έστω

$$z = y - d \cdot x,$$

τότε $z \in \mathbb{Z}$ και λόγω της (7) θα ισχύει

$$a \cdot x + n \cdot z = 1.$$

Έτσι για τα $a,n \in \mathbb{N}$, $\exists x, z \in \mathbb{Z}$ ώστε να ισχύει η τελευταία εξίσωση. Αυτό σύμφωνα με την Πρόταση 3 σημαίνει ότι τα a,n είναι πρώτοι μεταξύ τους.

Κινέζικο θεώρημα των υπολοίπων

Αν $k \in \mathbb{N}^*$ με $k \geq 2$, $\forall i \in \{1,..,k\}$ ισχύει $a_i \in \mathbb{Z}$, $n_i \in \mathbb{N}^*$ με $n_i \geq 2$, οι n_i είναι ανά δύο πρώτοι μεταξύ τους και

$$n = \prod_{i=1}^{k} n_i,$$

τότε $\exists x \in \{0,..,n-1\}$ μοναδικό στο σύνολο $\{0,..,n-1\}$, έτσι ώστε $\forall i \in \{1,..,k\}$ να ισχύει

$$x \equiv a_i \bmod n_i.$$

Έστω ότι $\forall i \in \{1,..,k\}$ είναι

$$N_i = \frac{n}{n_i},$$

τότε $\exists M_i \in \mathbb{Z}^*$ όπου

$$(N_i \cdot M_i) \bmod n_i = 1.$$

Η τιμή του x θα δίνεται από τη σχέση

$$x = \left(\sum_{i=1}^{k} (a_i \cdot N_i \cdot M_i) \right) \bmod n.$$

Πρόταση 12

Αν p,q είναι πρώτοι αριθμοί με $p \neq q$, $a \in \mathbb{Z}_p^*$, $b \in \mathbb{Z}_q^*$ και $n = p \cdot q$, τότε $\exists x \in \mathbb{Z}_n^*$ μοναδικό στο σύνολο $\mathbb{Z}_n^*$, έτσι ώστε να ισχύει

$$\begin{cases} x \equiv a \bmod p \\ x \equiv b \bmod q \end{cases}.$$

Απόδειξη

Επειδή τα p,q είναι πρώτοι αριθμοί με $p \neq q$, τότε λόγω της Πρότασης 2 αυτά θα είναι και πρώτοι μεταξύ τους αριθμοί. Άρα τηρούνται οι προϋποθέσεις του προηγούμενου θεωρήματος και για αυτό $\exists x \in \{0,..,n-1\}$ μοναδικό στο σύνολο $\{0,..,n-1\}$ ώστε να ισχύουν οι δύο ισοδυναμίες της παρούσας Πρότασης.

Θα δειχτεί ότι $x \in \mathbb{Z}_n^*$. Επειδή $a \in \mathbb{Z}_p^*$, τότε οι a, p είναι πρώτοι μεταξύ τους. Επιπλέον ισχύει ότι

$$x \equiv a \bmod p$$

και άρα σύμφωνα με την Πρόταση 11 και οι x, p θα είναι πρώτοι μεταξύ τους. Παρόμοια, επειδή $b \in \mathbb{Z}_q^*$, τότε οι b, q είναι πρώτοι μεταξύ τους. Επιπλέον ισχύει ότι

$$x \equiv b \bmod q$$

και άρα σύμφωνα με την Πρόταση 11 και οι x, q θα είναι πρώτοι μεταξύ τους. Επομένως λόγω της Πρότασης 5.1 το x θα είναι πρώτος με το γινόμενο

$$n = p \cdot q$$

των p,q εφόσον είναι πρώτος με το καθένα από αυτά. Για αυτόν τον λόγο, το $x \in \{0,..,n-1\}$ θα ανήκει συγκεκριμένα στο $\mathbb{Z}_n^*$ και επειδή είναι μοναδικό στο $\{0,..,n-1\}$ θα είναι και μοναδικό στο $\mathbb{Z}_n^*$.

Ορισμός 6

Αν $n \in \mathbb{N}^*$ με $n \geq 2$ και $a \in \mathbb{Z}_n^*$ για το οποίο $\exists x \in \mathbb{Z}_n^*$ ώστε

$$a = x^2 \bmod n,$$

τότε το a λέγεται *τετραγωνικό υπόλοιπο modulo* n. Το QR_n^* είναι το σύνολο που περιέχει όλα τα τετραγωνικά υπόλοιπα modulo n.

Πρόταση 13 [3]

Αν p, p' είναι περιττοί πρώτοι αριθμοί με

$$p = 2 \cdot p' + 1,$$

τότε το πλήθος του QR_p^* είναι ίσο με p'.

Απόδειξη

Εφόσον p πρώτος, τότε σύμφωνα με την Πρόταση 7 είναι

$$\mathbb{Z}_p^* = \{1,.., p-1\}.$$

Επειδή το p μάλιστα είναι και περιττός θα ισχύει $p \geq 3$, μια και το 3 είναι ο μικρότερος περιττός πρώτος αριθμός.

Θα δειχτεί αρχικά πως $QR_p^* \neq \varnothing$. Ισχύει $1 \in \mathbb{Z}_p^*$ και επίσης

$$1 = 1^2 \bmod p,$$

αφού $p \geq 3 > 1$. Δηλαδή για το $1 \in \mathbb{Z}_p^*$ $\exists x \in \mathbb{Z}_p^*$ ώστε

$$1 = x^2 \bmod p .$$

Στη συγκεκριμένη περίπτωση είναι $x = 1$. Συνεπώς το 1 είναι τετραγωνικό υπόλοιπο modulo p. Αυτό σημαίνει πως το QR_p^* έχει τουλάχιστον ένα στοιχείο και άρα $QR_p^* \neq \varnothing$. Ισχύει

$$p = 2 \cdot p' + 1 \Rightarrow p - 1 = 2 \cdot p' \Rightarrow p' = \frac{p-1}{2} \quad (8).$$

Ισχύει λόγω και της (8) ότι

$$p \geq 3 > 1 \Rightarrow p - 1 > 0 \Rightarrow \frac{p-1}{2} > 0 \Rightarrow 2 \cdot \frac{(p-1)}{2} > \frac{p-1}{2} \Rightarrow p - 1 > \frac{p-1}{2} \Rightarrow p - 1 > p' \quad (9)$$

και επομένως

$$\{1, .., p'\} \subset \mathbb{Z}_p^* .$$

Στη συνέχεια θα δειχτεί ότι τα τετραγωνικά υπόλοιπα modulo p που προκύπτουν από τα στοιχεία του υποσυνόλου $\{1, .., p'\}$ του $\mathbb{Z}_p^*$ είναι διαφορετικά μεταξύ τους, δηλαδή $\forall x, y \in \{1, .., p'\}$ με $x \neq y$ ισχύει ότι

$$x^2 \bmod p \neq y^2 \bmod p .$$

Έστω πως αυτή η υπόθεση δεν ευσταθεί και $\exists x, y \in \{1, .., p'\}$ με $x \neq y$ ώστε

$$x^2 \bmod p = y^2 \bmod p .$$

Τότε σύμφωνα με την Πρόταση 8.7.1, συνεπάγεται από την τελευταία εξίσωση πως

$$x^2 \equiv y^2 \bmod p \Rightarrow \left(x^2 - y^2\right) \equiv 0 \bmod p \Rightarrow \left((x+y) \cdot (x-y)\right) \equiv 0 \bmod p ,$$

δηλαδή ο πρώτος αριθμός p διαιρεί το γινόμενο $(x+y) \cdot (x-y)$ και άρα λόγω της Πρότασης 4 θα ισχύει η διάζευξη: το p διαιρεί το $x+y$ ή το $x-y$.

Θα δειχτεί πως το p δε διαιρεί το $x+y$. Επειδή $x, y \in \{1, .., p'\}$ θα ισχύει και λόγω της (8) ότι

$$\begin{cases} 1 \leq x \leq p' \\ 1 \leq y \leq p' \end{cases} \Rightarrow 2 \leq x + y \leq 2 \cdot p' = 2 \cdot \frac{(p-1)}{2} = p - 1 \Rightarrow$$

$$0 < 2 \leq x + y \leq p - 1 < p \Rightarrow 0 < x + y < p \Rightarrow 0 \cdot p < x + y < 1 \cdot p .$$

Από την τελευταία διπλή ανισότητα προκύπτει πως το $x+y$ βρίσκεται μεταξύ δύο διαδοχικών ακεραίων πολλαπλασίων του p χωρίς να ισούται με κανένα από αυτά. Άρα το $x+y$ δεν είναι ακέραιο πολλαπλάσιο του p και συνεπώς δε διαιρείται από αυτό. Αυτό σημαίνει πως εφόσον ισχύει η παραπάνω διάζευξη, το p θα διαιρεί το $x-y$, δηλαδή το $x-y$ είναι πολλαπλάσιο του p. Εξαιτίας και της (8) ισχύει ότι

$$\begin{cases} 1 \leq x \leq p' \\ 1 \leq y \leq p' \end{cases} \Rightarrow \begin{cases} 1 \leq x \leq p' \\ -p' \leq -y \leq -1 \end{cases} \Rightarrow 1 - p' \leq x - y \leq p' - 1 \Rightarrow -\left(p' - 1\right) \leq x - y \leq p' - 1 \Rightarrow$$

$$-\left(\frac{p-1}{2} - 1\right) \leq x - y \leq \frac{p-1}{2} - 1 \Rightarrow -\frac{(p-3)}{2} \leq x - y \leq \frac{p-3}{2} \Rightarrow |x - y| \leq \frac{p-3}{2} \quad (10).$$

Ισχύει ότι

$$p > 1 \Rightarrow p > -3 \Rightarrow 2 \cdot p > p - 3 \Rightarrow p > \frac{p-3}{2} \quad (11).$$

Από τις (10), (11) συνεπάγεται πως

$$|x - y| < p \Rightarrow -p < x - y < p .$$

Επειδή το $x-y$ είναι πολλαπλάσιο του p, $\exists k \in \mathbb{Z}$ ώστε

$$x-y=k\cdot p$$

και για αυτό από την τελευταία διπλή ανισότητα και το γεγονός πως

$$p>1 \Rightarrow p>0$$

συνεπάγεται ότι

$$-p<k\cdot p<p \Rightarrow -1<k<1.$$

Επειδή $k \in \mathbb{Z}$, τότε από την τελευταία διπλή ανσότητα προκύπτει πως $k=0$. Άρα

$$x-y=0\cdot p=0 \Rightarrow x=y,$$

που καταλήγει σε άτοπο αφού $x \neq y$. Επομένως δεν $\exists x, y \in \{1,..,p'\}$ με $x \neq y$ ώστε

$$x^2 \bmod n = y^2 \bmod n$$

και άρα $\forall x, y \in \{1,..,p'\}$ με $x \neq y$ ισχύει ότι

$$x^2 \bmod n \neq y^2 \bmod n.$$

Αυτό σημαίνει πως τα p' τετραγωνικά υπόλοιπα modulo p που προκύπτουν από τα p' στοιχεία του συνόλου $\{1,..,p'\}$ είναι διαφορετικά μεταξύ τους.

Λόγω της (9) υπάρχει το σύνολο $\{p'+1,..,p-1\}$ και συγκεκριμένα

$$\{p'+1,..,p-1\} \subset \mathbb{Z}_p^*.$$

Αυτό το υποσύνολο έχει

$$p-1-p'=p-1-\frac{(p-1)}{2}=\frac{p-1}{2}=p'$$

στοιχεία. Θα δειχτεί ότι τα τετραγωνικά υπόλοιπα modulo p που προκύπτουν από τα p' στοιχεία του συνόλου $\{p'+1,..,p-1\}$, ανήκουν στο σύνολο εκείνων που προκύπτουν από τα p' στοιχεία του συνόλου $\{1,..,p'\}$. $\forall x \in \{p'+1,..,p-1\}$, ισχύει λόγω και της (8) ότι

$$p'+1 \le x \le p-1 \Rightarrow -(p'+1) \ge -x \ge -(p-1) \Rightarrow p-p'-1 \ge p-x \ge p-p+1 \Rightarrow$$

$$p-1-\frac{(p-1)}{2} \ge p-x \ge 1 \Rightarrow \frac{p-1}{2} \ge p-x \ge 1 \Rightarrow p' \ge p-x \ge 1 \Rightarrow$$

$$(p-x) \in \{1,..,p'\} \quad (12).$$

[4] $\forall x \in \{p'+1,..,p-1\}$ ισχύει σύμφωνα και με την Πρόταση 8.5 ότι

$$(p-x) \bmod p = \big((p \bmod p)+((-x) \bmod p)\big) \bmod p.$$

Όμως

$$p \bmod p = 0$$

και άρα λόγω και των Προτάσεων 8.4, 10.1 θα συνεπάγεται από την τελευταία εξίσωση ότι.

$$(p-x) \bmod p = \big(0+((-x) \bmod p)\big) \bmod p = ((-x) \bmod p) \bmod p \Rightarrow$$

$$(p-x) \bmod p = (-x) \bmod p \Rightarrow (p-x) \equiv (-x) \bmod p \Rightarrow (p-x)^2 \equiv (-x)^2 \bmod p \Rightarrow$$

$$(p-x)^2 \bmod p = x^2 \bmod p.$$

Από την τελευταία σχέση και την (12) αποδεικνύεται πως $\forall x \in \{p'+1,..,p-1\}$, το τετραγωνικό υπόλοιπο modulo p που προκύπτει από το x είναι ίδιο με αυτό που προκύπτει από κάποιο στοιχείο του $\{1,..,p'\}$, δηλαδή είναι ένα από τα p'

διαφορετικά τετραγωνικά υπόλοιπα modulo p που αναφέρθηκαν παραπάνω. Επομένως τα τετραγωνικά υπόλοιπα modulo p που προκύπτουν από τα στοιχεία του συνόλου $\{p'+1,..,p-1\}$, ανήκουν στο σύνολο των p' διαφορετικών τετραγωνικών υπολοίπων modulo p που προκύπτουν από τα στοιχεία του $\{1,..,p'\}$. Συνεπώς αυτά τα p' διαφορετικά τετραγωνικά υπόλοιπα modulo p, είναι όλα όσα προκύπτουν από τα στοιχεία του συνόλου

$$\{1,..,p'\}\cup\{p'+1,..,p-1\}=\mathbb{Z}_p^*$$

και άρα όλα όσα αποτελούν το QR_p^*. Το τελευταίο σημαίνει πως το πλήθος του QR_p^* είναι ίσο με p'.

Θεώρημα Euler

Αν $n\in\mathbb{N}^*$ με $n\geq 2$ και $a\in\mathbb{Z}_n^*$, τότε

$$a^{\phi(n)}\equiv 1 \bmod n.$$

Μικρό θεώρημα του Fermat

Αν $a\in\mathbb{N}^*$, p είναι πρώτος αριθμός και οι a, p πρώτοι μεταξύ τους, τότε

$$a^{p-1}\equiv 1 \bmod p.$$

Ορισμός 7

Αν $n\in\mathbb{N}^*$ με $n\geq 2$ και $a\in\mathbb{Z}_n^*$, *τάξη του* a *ως προς* n είναι ο ελάχιστος μη μηδενικός φυσικός αριθμός m για τον οποίο ισχύει

$$a^m\equiv 1 \bmod n.$$

Πρόταση 14

Αν $n\in\mathbb{N}^*$ με $n\geq 2$ και $a\in\mathbb{Z}_n^*$, υπάρχει η τάξη του a ως προς n. Στην περίπτωση που $n\geq 3$ και $a\geq 2$, η τάξη αυτή είναι μεγαλύτερη ή ίση με 2.

Απόδειξη

Εξαιτίας του θεωρήματος του Euler και του γεγονότος πως $\phi(n)\in\mathbb{N}^*$, $\exists m\in\mathbb{N}^*$, όπου $m=\phi(n)$, για το οποίο ισχύει

$$a^m\equiv 1 \bmod n.$$

Δηλαδή το σύνολο των μη μηδενικών φυσικών αριθμών m για τους οποίους ισχύει αυτή η ισοδυναμία είναι μη κενό και άρα έχει ελάχιστο στοιχείο το οποίο είναι η τάξη του a ως προς n. Επομένως η τελευταία υπάρχει.

Έστω $n\geq 3$ και $a\geq 2$. Εφόσον $n\geq 3$ τότε $n-1\geq 2$, οπότε

$$2\in\mathbb{Z}_n^*=\{1,..,n-1\}.$$

Άρα

$$\exists a\in\mathbb{Z}_n^*=\{1,..,n-1\}$$

με $a\geq 2$. Θα δειχτεί ότι για την τάξη t του a ως προς n ισχύει $t\geq 2$. Έστω πως $t<2$, δηλαδή $t=1$ μια και το t ως τάξη που είναι, είναι μεγαλύτερο του 0. Τότε θα ισχύει

$$a^t\equiv 1 \bmod n\Rightarrow a^1\equiv 1 \bmod n\Rightarrow a\equiv 1 \bmod n \quad (13).$$

Επειδή $n\geq 3>1$, θα είναι

$$1 \bmod n=1 \quad (14).$$

Επίσης αφού

$$a \in \mathbb{Z}_n^* = \{1,..,n-1\},$$

θα ισχύει

$$a \le n-1 < n \Rightarrow a < n \Rightarrow a \bmod n = a \quad (15).$$

Λόγω των (14) και (15) προκύπτει από την (13) ότι $a = 1$. Η τελευταία ισότητα καταλήγει σε άτοπο, αφού από την υπόθεση είναι $a \ge 2 > 1$ και άρα $a \ne 1$. Συνεπώς για την τάξη t του a θα ισχύει $t \ge 2$.

Πρόταση 15

Αν $n,t \in \mathbb{N}^*$ με $n \ge 3$, $a \in \mathbb{Z}_n^*$ με $a \ge 2$, $m,k \in \mathbb{Z}$ και t η τάξη του a ως προς n, τότε ισχύουν τα εξής:

1. Αν $a^m \equiv 1 \bmod n$, τότε $m \equiv 0 \bmod t$.
2. Αν $a^m \equiv a^k \bmod n$, τότε $(m-k) \equiv 0 \bmod t$.
3. Αν $t \ge 3$, τότε $\forall m,k \in \{1,..,t-1\}$ με $m \ne k$, ισχύει $a^m \bmod n \ne a^k \bmod n$.

Απόδειξη

1.

Έστω

$$v = m \bmod t \quad (16) \text{ και } d = mdivt,$$

τότε

$$m = t \cdot d + v$$

και λόγω των Προτάσεων 10.2, 8.6, 10.4 θα ισχύει ότι

$$a^m \bmod n = a^{t \cdot d + v} \bmod n = \left(a^{t \cdot d} \cdot a^v\right) \bmod n = \left(\left(a^{t \cdot d} \bmod n\right) \cdot \left(a^v \bmod n\right)\right) \bmod n \Rightarrow$$

$$a^m \bmod n = \left(\left(\left(a^t\right)^d \bmod n\right) \cdot \left(a^v \bmod n\right)\right) \bmod n \quad (17).$$

Επειδή το t είναι η τάξη του a ως προς n, τότε

$$a^t \equiv 1 \bmod n$$

και επομένως λόγω της Πρότασης 10.1 θα ισχύει ότι

$$\left(a^t\right)^d \equiv 1 \bmod n.$$

Λόγω της τελευταίας ισοδυναμίας η (17) συνεπάγεται ότι

$$a^m \bmod n = \left(1 \cdot \left(a^v \bmod n\right)\right) \bmod n = \left(a^v \bmod n\right) \bmod n \Rightarrow a^m \bmod n = a^v \bmod n \quad (18).$$

Όμως από την υπόθεση ισχύει πως

$$a^m \equiv 1 \bmod n = 1$$

και συνεπώς λόγω της (18) θα είναι

$$a^v \bmod n = 1 \quad (19).$$

Λόγω της (16) και της Πρότασης 8.1 θα ισχύει

$$0 \le v \le t-1 < t \Rightarrow 0 \le v < t.$$

Επειδή $n \ge 3$ και $a \ge 2$, σύμφωνα με την Πρόταση 14 θα ισχύει για την τάξη t του a ως προς n ότι $t \ge 2$. Έστω

$$0 < v < t,$$

τότε το v θα είναι μη μηδενικός φυσικός αριθμός, μικρότερος από την τάξη t του a ως προς n και θα ικανοποιεί την (19). Αυτό είναι άτοπο καθώς το t είναι ο ελάχιστος φυσικός αριθμός r διάφορος του μηδέν, για τον οποίο ισχύει

$$a^r \equiv 1 \bmod n.$$

Συνεπώς $v = 0$ και πράγματι η (19) γίνεται

$$a^0 \bmod n = 1 \bmod n = 1,$$

αφού $n \geq 3 > 1$. Η (16) λοιπόν συνεπάγεται ότι

$$m \bmod t = 0 \Rightarrow m \equiv 0 \bmod t .$$

2.

Επειδή $a \in \mathbb{Z}_n^*$, τότε λόγω των Προτάσεων 10.5, 10.2 και 15.1 θα ισχύει

$$a^m \equiv a^k \bmod n \Rightarrow \left(a^m \cdot a^{-k}\right) \equiv 1 \bmod n \Rightarrow a^{m-k} \equiv 1 \bmod n \Rightarrow \left(m-k\right) \equiv 0 \bmod t .$$

3.

Όπως αναφέρθηκε στην απόδειξη της Πρότασης 15.1, είναι $t \geq 2$. Αν συγκεκριμένα είναι $t \geq 3$, τότε $t-1 \geq 2$ και επομένως υπάρχει το σύνολο $\{1,..,t-1\}$ στο οποίο υπάρχουν τουλάχιστον δύο αριθμοί διαφορετικοί μεταξύ τους. Έστω ότι η υπόθεση δεν αληθεύει και $\exists m,k \in \{1,..,t-1\}$, με $m \neq k$, ώστε να ισχύει

$$a^m \equiv a^k \bmod n .$$

Τότε λόγω της Πρότασης 15.2 θα ισχύει

$$\left(m-k\right) \equiv 0 \bmod t$$

και άρα εξαιτίας της Πρότασης 8.3 θα $\exists d \in \mathbb{Z}$ ώστε

$$m-k = t \cdot d \quad (20).$$

Επειδή $m,k \in \{1,..,t-1\}$ θα ισχύει

$$\begin{cases} 1 \leq m \leq t-1 \\ 1 \leq k \leq t-1 \end{cases} \Rightarrow \begin{cases} 1 \leq m \leq t-1 \\ -\left(t-1\right) \leq -k \leq -1 \end{cases} \Rightarrow 1-\left(t-1\right) \leq m-k \leq t-1-1 \Rightarrow$$

$$1-t+1 \leq m-k \leq t-2 \Rightarrow -t+2 \leq m-k \leq t-2 \Rightarrow -\left(t-2\right) \leq m-k \leq t-2 < t \quad (21).$$

Ισχύει

$$t > t-2 \Rightarrow -t < -\left(t-2\right) \xrightarrow{(21)} -t < m-k < t \xrightarrow{(20)} -t < t \cdot d < t \Rightarrow -1 < d < 1,$$

εφόσον $t > 0$. Επειδή $d \in \mathbb{Z}$, τότε από την τελευταία διπλή ανισότητα προκύπτει πως $d = 0$ και συνεπώς η (20) συνεπάγεται ότι

$$m-k = t \cdot 0 = 0 \Rightarrow m = k .$$

Η τελευταία ισότητα καταλήγει σε άτοπο, αφού $m \neq k$. Επομένως η υπόθεση αληθεύει και άρα $\forall m,k \in \{1,..,t-1\}$, με $m \neq k$, ισχύει

$$a^m \bmod n \neq a^k \bmod n .$$

<u>Πρόταση 16</u>

Αν p, p' είναι περιττοί πρώτοι αριθμοί με

$$p = 2 \cdot p' + 1,$$

τότε η τάξη ως προς p κάθε στοιχείου, διαφορετικού του 1, του QR_p^* είναι ίση με p'

<u>Απόδειξη</u>

Έστω $a \in QR_p^*$ με $a \neq 1$, δηλαδή $a \geq 2$. Τότε $\exists x \in \mathbb{Z}_p^*$ ώστε

$$a = x^2 \bmod p .$$

Ισχύει ότι

$$a = x^2 \bmod p \Rightarrow a \bmod p = \left(x^2 \bmod p\right) \bmod p \Rightarrow a \bmod p = x^2 \bmod p \Rightarrow$$

$$a \equiv x^2 \bmod p \Rightarrow a^{p'} \equiv \left(x^2\right)^{p'} \bmod p \Rightarrow a^{p'} \equiv x^{2 \cdot p'} \bmod p \quad (22).$$

Ισχύει ότι

$$p = 2 \cdot p' + 1 \Rightarrow p - 1 = 2 \cdot p'$$

και λόγω της τελευταίας ισότητας η (22) γίνεται

$$a^{p'} \equiv x^{p-1} \bmod p \quad (23).$$

Επειδή $x \in \mathbb{N}^*$, το p είναι πρώτος αριθμός και οι x, p πρώτοι μεταξύ τους, αφού $x \in \mathbb{Z}_p^*$, τότε πληρούνται οι προϋποθέσεις του μικρού θεωρήματος του Fermat και επομένως θα ισχύει

$$x^{p-1} \equiv 1 \bmod p .$$

Έτσι η (23) συνεπάγεται ότι

$$a^{p'} \equiv 1 \bmod p \quad (24).$$

Επειδή το p' είναι περριτός πρώτος αριθμός θα ισχύει $p' \geq 3 > 0$, μια και το 3 είναι ο μικρότερος περιττός πρώτος. Δηλαδή το p' είναι μη μηδενικός φυσικός αριθμός. Επιπλέον είναι και ένας από τους μη μηδενικούς φυσικούς m οι οποίοι ικανοποιούν την ισοδυναμία

$$a^m \equiv 1 \bmod p .$$

Άρα αν t η τάξη του a ως προς p, τότε θα ισχύει $t \leq p'$, αφού το t είναι ο μικρότερος $m \in \mathbb{N}^*$ που ικανοποιεί την ισοδυναμία

$$a^m \equiv 1 \bmod p .$$

Έστω πως η τάξη t δεν είναι ίση με p', δηλαδή $t < p'$. Το p όπως και το p' είναι περιττός πρώτος αριθμός, άρα $p \geq 3 > 0$. Ισχύουν $p, t \in \mathbb{N}^*$ με $p \geq 3$, $a \in \mathbb{Z}_p^*$, μια και $a \in QR_p^*$, όπου $a \geq 2$ όπως αναφέρθηκε στην αρχή της απόδειξης, $p' \in \mathbb{Z}$ και η σχέση (24). Τότε πληρούνται οι προϋποθέσεις της Πρότασης 15.1 και για αυτό θα είναι

$$p' \equiv 0 \bmod t .$$

Δηλαδή $\exists d \in \mathbb{Z}$ ώστε

$$p' = t \cdot d .$$

Επομένως το t διαιρεί το p', το οποίο ως πρώτος αριθμός έχει ως μοναδικούς διαιρέτες τα $1, p'$. Άρα το t που είναι διαιρέτης του p', θα ισούται με 1 ή p'. Επειδή όμως σύμφωνα με τον προηγούμενο ισχυρισμό είναι $t \neq p'$, θα ισχύει $t = 1$. Η τελευταία ισότητα καταλήγει σε άτοπο, καθώς $p \geq 3$ και $a \geq 2$ και επομένως σύμφωνα με την Πρόταση 14 θα ισχύει για την τάξη t του a ως προς p, ότι $t \geq 2 > 1$ και άρα $t \neq 1$. Συνεπώς $t = p'$ και έτσι $\forall a \in QR_p^*$ με $a \neq 1$, η τάξη του a ως προς p είναι ίση με p'.

Ορισμός 8

Αν $n \in \mathbb{N}^*$ με $n \geq 3$, $a \in QR_n^*$ με $a \neq 1$ και $\forall x \in QR_n^*$ $\exists m \in \mathbb{N}^*$ ώστε

$$x = a^m \bmod n ,$$

τότε το a *παράγει* το QR_n^* και λέγεται *γεννήτοράς* του.

Πρόταση 17

Αν p, p' είναι περιττοί πρώτοι αριθμοί με

$$p = 2 \cdot p' + 1,$$

τότε το QR_p^* παράγεται από κάθε στοιχείο του που είναι διαφορετικό του 1.

Απόδειξη

Έστω $a \in QR_p^*$ με $a \neq 1$, δηλαδή $a \geq 2$. Τότε σύμφωνα με την Πρόταση 16 η τάξη του a ως προς p είναι ίση με p', όπου $p' \geq 3$. Με βάση το τελευταίο, λόγω της Πρότασης 15.3 θα ισχύει ότι $\forall m,k \in \{1,..,p'-1\}$, με $m \neq k$,

$$a^m \bmod p \neq a^k \bmod p .$$

Δηλαδή οι $p'-1$ το πλήθος αριθμοί

$$a^1 \bmod p, a^2 \bmod p, .., a^{p'-1} \bmod p$$

είναι διαφορετικοί μεταξύ τους. Επειδή p' είναι η τάξη του a ως προς p, το p' είναι ο ελάχιστος μη μηδενικός φυσικός αριθμός r για τον οποίο

$$a^r \equiv 1 \bmod p \text{, δηλαδή } a^r \bmod p = 1$$

μια και $p \geq 3 > 1$. Αυτό σημαίνει πως αφού $\forall m \in \{1,..,p'-1\}$ είναι $m < p'$, θα ισχύει

$$a^m \bmod p \neq 1.$$

Άρα και με βάση το προηγούμενο συμπέρασμα ότι τα

$$a^1 \bmod p, a^2 \bmod p, .., a^{p'-1} \bmod p$$

είναι διαφορετικά μεταξύ τους, οι

$$p'-1+1 = p'$$

το πλήθος αριθμοί

$$1, a^1 \bmod p, a^2 \bmod p, .., a^{p'-1} \bmod p$$

θα είναι και αυτοί διαφορετικοί μεταξύ τους.

Επειδή $a \in QR_p^*$ $\exists x \in \mathbb{Z}_p^*$ ώστε

$$a = x^2 \bmod p$$

και συνεπώς $\forall m \in \{1,..,p'-1\}$ θα ισχύει λόγω των Προτάσεων 8.2, 10.1 και 10.4 ότι

$$a = x^2 \bmod p \Rightarrow a \equiv x^2 \bmod p \Rightarrow a^m \equiv \left(x^2\right)^m \bmod p = x^{2 \cdot m} \bmod p \Rightarrow$$

$$a^m \equiv \left(x^m\right)^2 \bmod p \ (25).$$

Έστω

$$y = x^m \bmod p ,$$

τότε λόγω της Πρότασης 8.2 θα είναι

$$y \equiv x^m \bmod p \ (26).$$

Από την τελευταία ισοδυναμία θα συνεπάγεται ότι

$$y^2 \equiv \left(x^m\right)^2 \bmod p \xrightarrow{(25)} a^m \equiv y^2 \bmod p \Rightarrow a^m \bmod p = y^2 \bmod p \ (27).$$

Εφόσον $y = x^m \bmod p$, τότε λόγω της Πρότασης 8.1

$$y \in \{0,..,p-1\} .$$

Θα δειχτεί ότι $y \in \mathbb{Z}_p^*$. Επειδή $x \in \mathbb{Z}_p^*$, το x είναι πρώτος με το p. Συνεπώς, μια και $m \in \mathbb{N}^*$, λόγω της Πρότασης 5.2 τα x^m, p είναι πρώτοι μεταξύ τους. Επιπλέον ισχύει και η (26), οπότε σύμφωνα με την Πρόταση 11 το y είναι πρώτος με το p και επειδή $y \in \{0,..,p-1\}$, τότε το y θα ανήκει συγκεκριμένα στο

$$\{1,..,p-1\} = \mathbb{Z}_p^* .$$

Αν

$$z = a^m \bmod p ,$$

τότε λόγω των Προτάσεων 8.1 και 8.2 θα ισχύουν αντίστοιχα ότι

$$z \in \{0,..,p-1\} \text{ και } z \equiv a^m \bmod p \text{ (28).}$$

Θα δειχτεί ότι $z \in \mathbb{Z}_p^*$. Επειδή $a \in \mathbb{Z}_p^*$, αφού $a \in QR_p^*$, το a είναι πρώτος με το p. Συνεπώς, μια και $m \in \mathbb{N}^*$, λόγω της Πρότασης 5.2 τα a^m, p είναι πρώτοι μεταξύ τους. Επιπλέον ισχύει και η (28), οπότε σύμφωνα με την Πρόταση 11 το z είναι πρώτος με το p και επειδή $z \in \{0,..,p-1\}$, τότε το z θα ανήκει συγκεκριμένα στο

$$\{1,..,p-1\} = \mathbb{Z}_p^*.$$

Έτσι $\forall m \in \{1,..,p'-1\}$, $\exists y \in \mathbb{Z}_p^*$ για τον αριθμό $z = a^m \bmod p$ ο οποίος ανήκει στο $\mathbb{Z}_p^*$, ώστε να ισχύει η (27). Αυτό σημαίνει πως το $a^m \bmod p$ είναι τετραγωνικό υπόλοιπο modulo p, δηλαδή

$$\left(a^m \bmod p\right) \in QR_p^*.$$

Επιπλέον $1 \in QR_p^*$ και άρα οι αριθμοί

$$1, a^1 \bmod p, a^2 \bmod p, .., a^{p'-1} \bmod p,$$

εκτός από διαφορετικοί μεταξύ τους, είναι και τετραγωνικά υπόλοιπα modulo p. Δηλαδή αποτελούν p' το πλήθος διαφορετικά τετραγωνικά υπόλοιπα modulo p. Όμως λόγω της Πρότασης 13 το πλήθος του QR_p^* είναι p' και επομένως αυτά τα p' διαφορετικά τετραγωνικά υπόλοιπα είναι όλα όσα απαρτίζουν το QR_p^*. Δηλαδή

$$QR_p^* = \left\{1, a^1 \bmod p, a^2 \bmod p, .., a^{p'-1} \bmod p\right\}$$

και επειδή

$$1 = a^{p'} \bmod n,$$

τότε

$$QR_p^* = \left\{a^1 \bmod p, a^2 \bmod p, .., a^{p'-1} \bmod p, a^{p'} \bmod p\right\}.$$

Αυτό σημαίνει πως $\forall x \in QR_p^*$ $\exists m \in \mathbb{N}^*$ ώστε

$$x = a^m \bmod p,$$

δηλαδή το $a \in QR_p^*$ αποτελεί γεννήτορα του QR_p^*. Επομένως $\forall a \in QR_p^*$ με $a \neq 1$, το a παράγει το QR_p^*.

<u>Πρόταση 18</u>

Αν p, p', q, q' είναι περιττοί πρώτοι αριθμοί με $p \neq q$, $p' \neq q'$,

$$p = 2 \cdot p' + 1,\ q = 2 \cdot q' + 1,$$

$a \in QR_p^*$ με $a \neq 1$, $b \in QR_q^*$ με $b \neq 1$, $n = p \cdot q$ και $x \in \mathbb{Z}_n^*$ ο μοναδικός αριθμός στο $\mathbb{Z}_n^*$ για τον οποίο

$$\begin{cases} x \equiv a \bmod p \\ x \equiv b \bmod q \end{cases},$$

τότε ισχύουν τα εξής:

1. Η τάξη του x ως προς n είναι ίση με $p' \cdot q'$.
2. Το x είναι τετραγωνικό υπόλοιπο modulo n.
3. Το x είναι γεννήτορας του QR_n^*.

4. $QR_n^* = \left\{x^1 \bmod n, .., x^{p'\cdot q'} \bmod n\right\}$ και το πλήθος του QR_n^* είναι ίσο με $p'\cdot q'$.

5. Η τάξη ως προς n κάθε στοιχείου, διαφορετικού του 1, του QR_n^* είναι ίση με p' ή q' ή $p'\cdot q'$.

6. $\forall c \in QR_n^*$ ισχύει $c^{p'\cdot q'} \equiv 1 \bmod n$.

Απόδειξη

1.

Επειδή $a \in QR_p^*$ και $b \in QR_q^*$, θα είναι $a \in \mathbb{Z}_p^*$ και $b \in \mathbb{Z}_q^*$. Επίσης τα p, q είναι πρώτοι αριθμοί με $p \neq q$. Συνεπώς πληρούνται οι προϋποθέσεις της Πρότασης 12 και για αυτό $\exists x \in \mathbb{Z}_n^*$ μοναδικό στο σύνολο $\mathbb{Z}_n^*$, ώστε να ισχύει το σύστημα ισοδυναμιών της υπόθεσης.

Επειδή $a \in \mathbb{Z}_p^*$ και $b \in \mathbb{Z}_q^*$, θα ισχύει $a < p$ και $b < q$. Από τις δύο τελευταίες ανισότητες προκύπτει πως

$$\begin{cases} x \equiv a \bmod p = a \\ x \equiv b \bmod q = b \end{cases}.$$

Θα δειχτεί πως $x \neq 1$. Έστω $x = 1$, τότε από το τελευταίο σύστημα ισοδυναμιών προκύπτει πως

$$\begin{cases} 1 \bmod p = a \\ 1 \bmod q = b \end{cases} \Rightarrow \begin{cases} a = 1 \\ b = 1 \end{cases},$$

που καταλήγει σε άτοπο αφού από την υπόθεση είναι $a \neq 1$ και $b \neq 1$. Επομένως $x \neq 1$, δηλαδή $x \geq 2$.

Επίσης p, q περιττοί πρώτοι αριθμοί και για αυτό ισχύει $p \geq 3$ και $q \geq 3$. Συνεπώς

$$n = p \cdot q \geq 3 \cdot 3 \Rightarrow n \geq 9.$$

Επειδή $a \in QR_p^*$ με $a \neq 1$ και $b \in QR_q^*$ με $b \neq 1$, τότε οι τάξεις των a ως προς p και b ως προς q είναι ίσες με p' και q' αντίστοιχα. Άρα θα ισχύει

$$\begin{cases} a^{p'} \equiv 1 \bmod p \\ b^{q'} \equiv 1 \bmod q \end{cases} \Rightarrow \begin{cases} \left(a^{p'}\right)^{q'} \equiv 1^{q'} \bmod p \\ \left(b^{q'}\right)^{p'} \equiv 1^{p'} \bmod q \end{cases} \Rightarrow \begin{cases} a^{p'\cdot q'} \equiv 1 \bmod p \\ b^{p'\cdot q'} \equiv 1 \bmod q \end{cases} \quad (29).$$

Επίσης

$$\begin{cases} x \equiv a \bmod p \\ x \equiv b \bmod q \end{cases} \Rightarrow \begin{cases} x^{p'\cdot q'} \equiv a^{p'\cdot q'} \bmod p \\ x^{p'\cdot q'} \equiv b^{p'\cdot q'} \bmod q \end{cases} \xrightarrow{(29)} \begin{cases} x^{p'\cdot q'} \equiv 1 \bmod p \\ x^{p'\cdot q'} \equiv 1 \bmod q \end{cases} \Rightarrow \begin{cases} \left(x^{p'\cdot q'} - 1\right) \equiv 0 \bmod p \\ \left(x^{p'\cdot q'} - 1\right) \equiv 0 \bmod q \end{cases}.$$

Οι p, q είναι πρώτοι αριθμοί με $p \neq q$ και λόγω της Πρότασης 6, το τελευταίο σύστημα ισοδυναμιών συνεπάγεται ότι

$$\left(x^{p'\cdot q'} - 1\right) \equiv 0 \bmod \left(p \cdot q\right) \Rightarrow x^{p'\cdot q'} \equiv 1 \bmod n \quad (30).$$

Έστω t η τάξη του x ως προς n. Επειδή $n \geq 9 > 3$ και $x \geq 2$, τότε λόγω της Πρότασης 15.1 η (30) συνεπάγεται πως

$$p' \cdot q' \equiv 0 \bmod t,$$

δηλαδή $\exists d \in \mathbb{Z}$ ώστε

$$p' \cdot q' = t \cdot d \quad (31).$$

Λόγω του ότι το t είναι η τάξη του x ως προς n, θα ισχύει

$$x^t \equiv 1 \bmod n \Rightarrow \left(x^t - 1\right) \equiv 0 \bmod n \Rightarrow \left(x^t - 1\right) \equiv 0 \bmod \left(p \cdot q\right)$$

και επειδή οι p,q είναι πρώτοι αριθμοί με $p \neq q$, σύμφωνα με την Πρόταση 6 η τελευταία ισοδυναμία συνεπάγεται ότι

$$\begin{cases} \left(x^t - 1\right) \equiv 0 \bmod p \\ \left(x^t - 1\right) \equiv 0 \bmod q \end{cases} \Rightarrow \begin{cases} x^t \equiv 1 \bmod p \\ x^t \equiv 1 \bmod q \end{cases}.$$

Εξαιτίας του τελευταίου συστήματος ισοδυναμιών θα ισχύει ότι

$$\begin{cases} x \equiv a \bmod p \\ x \equiv b \bmod q \end{cases} \Rightarrow \begin{cases} x^t \equiv a^t \bmod p \\ x^t \equiv b^t \bmod q \end{cases} \Rightarrow \begin{cases} a^t \equiv 1 \bmod p \\ b^t \equiv 1 \bmod q \end{cases}.$$

Επειδή $p \geq 3$ και $q \geq 3$ αφού τα p,q είναι περιττοί πρώτοι αριθμοί, $a \geq 2$ αφού $a \neq 1$, $b \geq 2$ αφού $b \neq 1$ και οι τάξεις των a ως προς p και b ως προς q είναι ίσες με p' και q' αντίστοιχα, το τελευταίο σύστημα ισοδυναμιών λόγω της Πρότασης 15.1 συνεπάγεται ότι

$$\begin{cases} t \equiv 0 \bmod p' \\ t \equiv 0 \bmod q' \end{cases}.$$

Οι p', q' είναι πρώτοι αριθμοί με $p' \neq q'$, άρα εξαιτίας της Πρότασης 6 το τελευταίο σύστημα ισοδυναμιών θα συνεπάγεται ότι

$$t \equiv 0 \bmod \left(p' \cdot q'\right).$$

Από την τελευταία ισοδυναμία προκύπτει πως $\exists d' \in \mathbb{Z}$ ώστε

$$t = p' \cdot q' \cdot d'.$$

Η (31) λόγω της τελευταίας σχέσης και του γεγονότος πως $p' \neq 0$ και $q' \neq 0$, συνεπάγεται ότι

$$p' \cdot q' = p' \cdot q' \cdot d' \cdot d \Rightarrow d' \cdot d = 1.$$

Επειδή $d, d' \in \mathbb{Z}$, από την τελευταία εξίσωση προκύπτει πως

$$\begin{cases} d = 1 \\ d' = 1 \end{cases} \text{ ή } \begin{cases} d = -1 \\ d' = -1 \end{cases}.$$

Όμως $p' > 0$, $q' > 0$ και $t > 0$, άρα από την (31) συνεπάγεται πως $d > 0$. Έτσι από την τελευταία διάζευξη των συστημάτων ισοδυναμιών, προκύπτει πως $d = 1$ και συνεπώς από την (31) συνεπάγεται πως

$$p' \cdot q' = t \cdot 1 \Rightarrow t = p' \cdot q'.$$

Επομένως τάξη t του x ως προς n είναι ίση με $p' \cdot q'$.

2.

Επειδή $a \in QR_p^*$ και $b \in QR_q^*$, $\exists x_1 \in \mathbb{Z}_p^*$ και $x_2 \in \mathbb{Z}_q^*$, ώστε

$$\begin{cases} a = {x_1}^2 \bmod p \\ b = {x_2}^2 \bmod q \end{cases} (32).$$

Επίσης σύμφωνα με την Πρόταση 12, για τα $x_1 \in \mathbb{Z}_p^*$ και $x_2 \in \mathbb{Z}_q^*$ $\exists y \in \mathbb{Z}_n^*$ μοναδικό στο $\mathbb{Z}_n^*$ ώστε

$$\begin{cases} x_1 \equiv y \bmod p \\ x_2 \equiv y \bmod q \end{cases}.$$

Από το τελευταίο σύστημα ισοδυναμιών συνεπάγεται πως

$$\begin{cases} {x_1}^2 \equiv y^2 \bmod p \\ {x_2}^2 \equiv y^2 \bmod q \end{cases} \xrightarrow{(32)} \begin{cases} a \equiv y^2 \bmod p \\ b \equiv y^2 \bmod q \end{cases} (33).$$

Επειδή

$$\begin{cases} x \equiv a \bmod p \\ x \equiv b \bmod q \end{cases},$$

τότε λόγω της (33) θα ισχύει

$$\begin{cases} x \equiv y^2 \bmod p \\ x \equiv y^2 \bmod q \end{cases} \Rightarrow \begin{cases} \left(x - y^2\right) \equiv \bmod p \\ \left(x - y^2\right) \equiv \bmod q \end{cases}.$$

Επειδή οι p, q είναι πρώτοι αριθμοί με $p \neq q$, τότε λόγω της Πρότασης 6 το τελευταίο σύστημα ισοδυναμιών συνεπάγεται ότι

$$\left(x - y^2\right) \equiv 0 \bmod \left(p \cdot q\right) \Rightarrow \left(x - y^2\right) \equiv 0 \bmod n \Rightarrow x \equiv y^2 \bmod n.$$

Έτσι για το $x \in \mathbb{Z}_n^*$ $\exists y \in \mathbb{Z}_n^*$ ώστε να ισχύει η τελευταία ισοδυναμία και συνεπώς το x είναι τετραγωνικό υπόλοιπο modulo n.

3.

Θα δειχτεί αρχικά πως $QR_n^* \neq \varnothing$. Ισχύει $1 \in \mathbb{Z}_n^*$ και επίσης

$$1 = 1^2 \bmod n,$$

αφού $n \geq 9 > 1$. Δηλαδή για το $1 \in \mathbb{Z}_n^*$ $\exists x' \in \mathbb{Z}_n^*$ ώστε

$$1 = x'^2 \bmod n.$$

Στη συγκεκριμένη περίπτωση είναι $x' = 1$. Συνεπώς το 1 είναι τετραγωνικό υπόλοιπο modulo n. Αυτό σημαίνει πως το QR_n^* έχει τουλάχιστον ένα στοιχείο και άρα $QR_n^* \neq \varnothing$.

Έστω $c \in QR_n^*$ και

$$\begin{cases} c_1 = c \bmod p \\ c_2 = c \bmod q \end{cases} \quad (34).$$

Θα δειχτεί πως $c_1 \in QR_p^*$ και $c_2 \in QR_q^*$. Επειδή $c \in QR_n^*$, τότε $\exists z \in \mathbb{Z}_n^*$ ώστε

$$c = z^2 \bmod n.$$

Από την τελευταία εξίσωση προκύπτει ότι

$$c \equiv z^2 \bmod \left(p \cdot q\right) \Rightarrow \left(c - z^2\right) \equiv 0 \bmod \left(p \cdot q\right) \Rightarrow \begin{cases} \left(c - z^2\right) \equiv 0 \bmod p \\ \left(c - z^2\right) \equiv 0 \bmod q \end{cases} \Rightarrow$$

$$\begin{cases} c \equiv z^2 \bmod p \\ c \equiv z^2 \bmod q \end{cases} \quad (35).$$

Έστω

$$\begin{cases} v_1 = z \bmod p \\ v_2 = z \bmod q \end{cases} \quad (36).$$

Τότε θα ισχύει

$$v_1 \in \{0, .., p-1\} \text{ και } v_2 \in \{0, .., q-1\}.$$

Επειδή $z \in \mathbb{Z}_n^*$, τότε οι z, n είναι πρώτοι μεταξύ τους και εφόσον το n είναι το γινόμενο των p, q, λόγω της Πρότασης 5.1 το z είναι επίσης πρώτο με καθένα από τα p, q. Από την (36) προκύπτει ότι

$$\begin{cases} v_1 \equiv z \bmod p \\ v_2 \equiv z \bmod q \end{cases}$$

και εφόσον τα z, p είναι πρώτοι μεταξύ τους όπως και τα z, q, τότε λόγω της Πρότασης 11 και του τελευταίου συστήματος ισοδυναμιών συνεπάγεται πως τα v_1, p είναι πρώτοι μεταξύ τους όπως και τα v_2, q. Δηλαδή

$$v_1 \in \mathbb{Z}_p^* \text{ και } v_2 \in \mathbb{Z}_q^*,$$

αφού $v_1 \in \{0,..,p-1\}$ και $v_2 \in \{0,..,q-1\}$. Από το τελευταίο σύστημα ισοδυναμιών προκύπτει πως

$$\begin{cases} v_1^2 \equiv z^2 \bmod p \\ v_2^2 \equiv z^2 \bmod q \end{cases} \xrightarrow{(35)} \begin{cases} v_1^2 \equiv c \bmod p \\ v_2^2 \equiv c \bmod q \end{cases} \quad (37).$$

Επειδή $c \in QR_n^*$, τότε $c \in \mathbb{Z}_n^*$. Όπως αποδείχτηκε πριν στην περίπτωση του $z \in \mathbb{Z}_n^*$ και των εξισώσεων της (36), ότι $v_1 \in \mathbb{Z}_p^*$ και $v_2 \in \mathbb{Z}_q^*$, έτσι και στην περίπτωση του $c \in \mathbb{Z}_n^*$ και των παρόμοιων εξισώσεων της (34), αποδεικνύεται με παρόμοιο τρόπο πως

$$c_1 \in \mathbb{Z}_p^* \text{ και } c_2 \in \mathbb{Z}_q^*.$$

Από τις (34), (37) συνεπάγεται πως

$$\begin{cases} c_1 = v_1^2 \bmod p \\ c_2 = v_2^2 \bmod q \end{cases}.$$

Λόγω του τελευταίου συστήματος των εξισώσεων και του γεγονότος πως $v_1, c_1 \in \mathbb{Z}_p^*$, $v_2, c_2 \in \mathbb{Z}_q^*$, συμπεραίνεται ότι

$$c_1 \in QR_p^* \text{ και } c_2 \in QR_q^*.$$

Εφόσον τα p, p', q, q' είναι περιττοί πρώτοι αριθμοί με

$$p = 2 \cdot p' + 1,\ q = 2 \cdot q' + 1,$$

τότε σύμφωνα με την Πρόταση 17 καθένα από τα QR_p^*, QR_q^* παράγεται από όλα τα στοιχεία του εκτός του 1. Έτσι, αφού για τα $a \in QR_p^*$, $b \in QR_q^*$ ισχύει $a \neq 1$, $b \neq 1$, τότε αυτά αποτελούν γεννήτορες των QR_p^*, QR_q^* αντίστοιχα. Επομένως για τα $c_1 \in QR_p^*$, $c_2 \in QR_q^*$ $\exists m, k \in \mathbb{N}^*$ ώστε

$$\begin{cases} c_1 = a^m \bmod p \\ c_2 = b^k \bmod q \end{cases}.$$

Από το τελευταίο σύστημα ισοδυναμιών και την (34) συνεπάγεται ότι

$$\begin{cases} c \equiv a^m \bmod p \\ c \equiv b^k \bmod q \end{cases} \quad (38).$$

Επειδή τα p', q' είναι πρώτοι αριθμοί με $p' \neq q'$, τότε λόγω της Πρότασης 2 θα είναι πρώτοι μεταξύ τους. Οπότε σύμφωνα με το Κινέζικο θεώρημα των υπολοίπων $\exists l \in \{0,.., p' \cdot q' - 1\}$ μοναδικό στο σύνολο $\{0,.., p' \cdot q' - 1\}$, έτσι ώστε

$$\begin{cases} l \equiv m \bmod p' \\ l \equiv k \bmod q' \end{cases}.$$

Το τελευταίο σύστημα ισοδυναμιών συνεπάγεται ότι

$$\begin{cases}(l-m)\equiv \bmod p'\\ (l-k)\equiv \bmod q'\end{cases}$$

και επομένως $\exists d_1, d_2 \in \mathbb{Z}$ ώστε

$$\begin{cases}l-m=p'\cdot d_1\\ l-k=q'\cdot d_2\end{cases}\Rightarrow\begin{cases}l=p'\cdot d_1+m\\ l=q'\cdot d_2+k\end{cases} \quad (39).$$

Επειδή

$$\begin{cases}x\equiv a \bmod p\\ x\equiv b \bmod q\end{cases},$$

τότε λόγω της (39) θα ισχύει

$$\begin{cases}x^l\equiv a^l \bmod p\\ x^l\equiv b^l \bmod q\end{cases}\Rightarrow\begin{cases}x^l\equiv a^{p'\cdot d_1+m} \bmod p\\ x^l\equiv b^{q'\cdot d_2+k} \bmod q\end{cases}\Rightarrow\begin{cases}x^l\equiv\left(a^{p'\cdot d_1}\cdot a^m\right)\bmod p\\ x^l\equiv\left(b^{q'\cdot d_2}\cdot b^k\right)\bmod q\end{cases}\Rightarrow$$

$$\begin{cases}x^l\equiv\left(\left(a^{p'\cdot d_1} \bmod p\right)\cdot\left(a^m \bmod p\right)\right)\bmod p\\ x^l\equiv\left(\left(b^{q'\cdot d_2} \bmod q\right)\cdot\left(b^k \bmod q\right)\right)\bmod q\end{cases} \quad (40).$$

Επειδή οι τάξεις των a ως προς p και b ως προς q είναι ίσες με p' και q' αντίστοιχα, θα ισχύει

$$\begin{cases}a^{p'}\equiv 1 \bmod p\\ b^{q'}\equiv 1 \bmod q\end{cases}\Rightarrow\begin{cases}\left(a^{p'}\right)^{d_1}\equiv 1^{d_1} \bmod p\\ \left(b^{q'}\right)^{d_2}\equiv 1^{d_2} \bmod q\end{cases}\Rightarrow\begin{cases}a^{p'\cdot d_1}\equiv 1 \bmod p=1\\ b^{q'\cdot d_2}\equiv 1 \bmod q=1\end{cases}.$$

Από την (40) συνεπάγεται λόγω του τελευταίου συστήματος ισοδυναμιών ότι

$$\begin{cases}x^l\equiv\left(1\cdot\left(a^m \bmod p\right)\right)\bmod p\\ x^l\equiv\left(1\cdot\left(b^k \bmod q\right)\right)\bmod q\end{cases}\Rightarrow\begin{cases}x^l\equiv\left(a^m \bmod p\right)\bmod p\\ x^l\equiv\left(b^k \bmod q\right)\bmod q\end{cases}\Rightarrow$$

$$\begin{cases}x^l\equiv a^m \bmod p\\ x^l\equiv b^k \bmod q\end{cases}\xrightarrow{(38)}\begin{cases}x^l\equiv c \bmod p\\ x^l\equiv c \bmod q\end{cases}\Rightarrow\begin{cases}\left(x^l-c\right)\equiv 0 \bmod p\\ \left(x^l-c\right)\equiv 0 \bmod q\end{cases}\Rightarrow$$

$$\left(x^l-c\right)\equiv 0 \bmod\left(p\cdot q\right)\Rightarrow c\equiv x^l \bmod n\Rightarrow c=x^l \bmod n \quad (41),$$

αφού $c\in\mathbb{Z}_n^*$, οπότε $c<n$. Συμπεραίνεται λοιπόν πως για το $c\in QR_n^*$ $\exists l\in\{0,..,p'\cdot q'-1\}$, ώστε να ισχύει η (41). Στην περίπτωση που $l=0$, τότε προκύπτει από αυτήν πως

$$c=x^0 \bmod n\Rightarrow c=1 \bmod n\Rightarrow c=x^{p'\cdot q'} \bmod n,$$

αφού σύμφωνα με την Πρόταση 18.1 η τάξη του x ως προς n είναι ίση με $p'\cdot q'$. Επομένως μπορεί να εξαχθεί το συμπέρασμα πως για το $c\in QR_n^*$ $\exists l\in\{1,..,p'\cdot q'\}$ ώστε να ισχύει η (41). Έτσι

$$\forall c\in QR_n^*\ \exists l\in\{1,..,p'\cdot q'\}\subset\mathbb{N}^*\ \text{ώστε}\ c=x^l \bmod n,$$

ενώ $x\in QR_n^*$ και $x\neq 1$, όπως αποδείχτηκε στις αποδείξεις των Προτάσεων 18.2 και 18.1 αντίστοιχα. Συνεπώς το x είναι γεννήτορας του QR_n^*.

4.

Σύμφωνα με την Πρόταση 18.1, η τάξη του x ως προς n είναι ίση με $p'\cdot q'$. Επειδή p', q' περιττοί πρώτοι αριθμοί, ισχύει $p'\geq 3$ και $q'\geq 3$. Συνεπώς

$$p'\cdot q'\geq 3\cdot 3\Rightarrow p'\cdot q'\geq 9>3\Rightarrow p'\cdot q'>3.$$

Άρα η τάξη του x ως προς n είναι μεγαλύτερη από 3 και για αυτό λόγω της Πρότασης 15.3 θα ισχύει ότι $\forall m,k\in\{1,..,p'\cdot q'-1\}$ με $m\neq k$, είναι

$$x^m \bmod n\neq x^k \bmod n.$$

Δηλαδή οι $p'\cdot q'-1$ το πλήθος αριθμοί

$$x^1 \bmod n, x^2 \bmod n,.., x^{p'\cdot q'-1} \bmod n$$

είναι διαφορετικοί μεταξύ τους. Επειδή $p'\cdot q'$ είναι η τάξη του x ως προς n, το $p'\cdot q'$ είναι ο ελάχιστος μη μηδενικός φυσικός αριθμός r για τον οποίο

$x^r\equiv 1 \bmod n$, δηλαδή $x^r \bmod n=1$

μια και $n\geq 9>1$. Αυτό σημαίνει πως αφού $\forall m\in\{1,..,p'\cdot q'-1\}$ είναι $m<p'\cdot q'$, θα ισχύει

$$x^m \bmod n\neq 1.$$

Άρα και με βάση το προηγούμενο συμπέρασμα ότι τα

$$x^1 \bmod n, x^2 \bmod n,.., x^{p'\cdot q'-1} \bmod n$$

είναι διαφορετικά μεταξύ τους, οι

$$p'\cdot q'-1+1=p'\cdot q'$$

το πλήθος αριθμοί

$$x^1 \bmod n, x^2 \bmod n,.., x^{p'\cdot q'-1} \bmod n, x^{p'\cdot q'} \bmod n$$

θα είναι και αυτοί διαφορετικοί μεταξύ τους.

Όπως αποδείχτηκε στο τέλος της απόδειξης της Πρότασης 18.3, $\forall c\in QR_n^*$ $\exists l\in\{1,..,p'\cdot q'\}$ ώστε

$$c=x^l \bmod n$$

και επομένως

$$QR_n^*\subseteq\{x^1 \bmod n,..,x^{p'\cdot q'} \bmod n\} \quad (42).$$

Έστω

$$z\in\{x^1 \bmod n,..,x^{p'\cdot q'} \bmod n\},$$

τότε $\exists l\in\{1,..,p'\cdot q'\}$ ώστε

$$z=x^l \bmod n \quad (43).$$

Θα δειχτεί ότι $z\in QR_n^*$. Σύμφωνα με την Πρόταση 18.2 $x\in QR_n^*$, οπότε $\exists y\in\mathbb{Z}_n^*$ ώστε

$$x=y^2 \bmod n$$

και άρα θα συνεπάγεται ότι

$$x\equiv y^2 \bmod n\Rightarrow x^l\equiv\left(y^2\right)^l \bmod n=y^{2\cdot l} \bmod n\Rightarrow x^l\equiv\left(y^l\right)^2 \bmod n\xrightarrow{(43)}$$

$$z=\left(y^l\right)^2 \bmod n \quad (44).$$

Από την (43) προκύπτει πως

$$z\in\{0,..,n-1\}.$$

Θα δειχτεί ότι $z \in \mathbb{Z}_n^*$. Επειδή $x \in \mathbb{Z}_n^*$, το x είναι πρώτος με το n που είναι το γινόμενο των p, q, οπότε σύμφωνα με την Πρόταση 5.1 το x θα είναι και πρώτος με καθένα από τα p, q. Συνεπώς, μια και $l \in \mathbb{N}^*$, λόγω της Πρότασης 5.2 το x^l είναι πρώτος με καθένα από τα p, q και εξαιτίας της Πρότασης 5.1 το x^l θα είναι και πρώτος με το γινόμενό τους n. Λόγω της (43) ισχύει

$$z \equiv x^l \bmod n,$$

οπότε σύμφωνα με την Πρόταση 11 το z είναι πρώτος με το n και επειδή $z \in \{0,..,n-1\}$, τότε το z θα ανήκει συγκεκριμένα στο

$$\{1,..,n-1\} = \mathbb{Z}_n^*.$$

Αν

$$h = y^l \bmod n,$$

τότε όπως αποδείχτηκε προηγουμένως ότι $z \in \mathbb{Z}_n^*$, έτσι αποδεικνύεται παρόμοια πως $h \in \mathbb{Z}_n^*$, μια και $y \in \mathbb{Z}_n^*$. Ισχύει

$$h = y^l \bmod n \Rightarrow h^2 \equiv \left(y^l\right)^2 \bmod n \xrightarrow{(44)} z = h^2 \bmod n.$$

Έτσι για το $z \in \mathbb{Z}_n^*$, $\exists h \in \mathbb{Z}_n^*$ ώστε να ισχύει η τελευταία εξίσωση και επομένως το z είναι τετραγωνικό υπόλοιπο modulo n, δηλαδή $z \in QR_n^*$. Συνεπώς

$$\left\{x^1 \bmod n,.., x^{p' \cdot q'} \bmod n\right\} \subseteq QR_n^*$$

και έτσι λόγω της (42) θα ισχύει

$$QR_n^* = \left\{x^1 \bmod n,.., x^{p' \cdot q'} \bmod n\right\}.$$

Επειδή το πλήθος του συνόλου $\left\{x^1 \bmod n,.., x^{p' \cdot q'} \bmod n\right\}$ είναι ίσο με $p' \cdot q'$, τότε και το πλήθος του QR_n^* είναι ίσο με $p' \cdot q'$.

5.

Σύμφωνα με την Πρόταση 18.4 είναι

$$QR_n^* = \left\{x^1 \bmod n,.., x^{p' \cdot q'} \bmod n\right\}.$$

Έστω

$$A = \left\{x^{1 \cdot p'} \bmod n, x^{2 \cdot p'} \bmod n,.., x^{(q'-1) \cdot p'} \bmod n\right\}.$$

Τότε το A είναι υποσύνολο του QR_n^* και περιέχει $q'-1$ στοιχεία. Εφόσον

$$\left(x^{p' \cdot q'} \bmod n\right) \notin A \text{ και } x^{p' \cdot q'} \bmod n = 1,$$

τότε $1 \notin A$. Έστω $c \in QR_n^*$ με $c \in A$. Επειδή $1 \notin A$ θα είναι $c \neq 1$ και άρα $c \geq 2$. Επίσης $\exists l \in \{1,..,q'-1\}$ ώστε

$$c = x^{l \cdot p'} \bmod n.$$

Αυτή η εξίσωση συνεπάγεται

$$c^{q'} \equiv \left(x^{l \cdot p'}\right)^{q'} \bmod n = x^{l \cdot p' \cdot q'} \bmod n \Rightarrow c^{q'} \equiv \left(x^{p' \cdot q'}\right)^l \bmod n \quad (45).$$

Σύμφωνα με την Πρόταση 18.1, η τάξη του x ως προς n είναι ίση με $p' \cdot q'$ και άρα ισχύει

$$x^{p' \cdot q'} \equiv 1 \bmod n \Rightarrow \left(x^{p' \cdot q'}\right)^l \equiv 1^l \bmod n \Rightarrow \left(x^{p' \cdot q'}\right)^l \equiv 1 \bmod n \xrightarrow{(45)} c^{q'} \equiv 1 \bmod n \quad (46).$$

Έστω t η τάξη του c ως προς n. Επειδή $n > 3$ και $c \geq 2$, σύμφωνα με την Πρόταση 15.1 η (46) συνεπάγεται ότι

$$q' \equiv 0 \bmod t,$$

δηλαδή $\exists d \in \mathbb{Z}$ ώστε

$$q' = t \cdot d.$$

Από την τελευταία εξίσωση προκύπτει ότι το t είναι διαιρέτης του q' το οποίο ως πρώτος αριθμός έχει δύο μη αρνητικούς διαιρέτες, τα $1, q'$. Επειδή $n > 3$ και $c \geq 2$, τότε σύμφωνα με την Πρόταση 14 θα είναι $t \geq 2 > 1$. Έτσι $t \neq 1$ και επειδή το t είναι μη αρνητικός διαιρέτης του q' θα ισχύει $t = q'$. Επομένως η τάξη κάθε στοιχείου του A είναι ίση με q'.

Έστω

$$B = \left\{ x^{1 \cdot q'} \bmod n, x^{2 \cdot q'} \bmod n, .., x^{(p'-1) \cdot q'} \bmod n \right\}.$$

Τότε το B είναι υποσύνολο του QR_n^* και περιέχει $p'-1$ στοιχεία. Εφόσον

$$\left(x^{p' \cdot q'} \bmod n \right) \notin B \text{ και } x^{p' \cdot q'} \bmod n = 1,$$

τότε $1 \notin B$. Έστω $c \in QR_n^*$ με $c \in B$. Επειδή $1 \notin B$ θα είναι $c \neq 1$ και άρα $c \geq 2$. Επίσης $\exists l \in \{1, .., p'-1\}$ ώστε

$$c = x^{l \cdot q'} \bmod n.$$

Αυτή η εξίσωση συνεπάγεται

$$c^{p'} \equiv \left(x^{l \cdot q'} \right)^{p'} \bmod n = x^{l \cdot q' \cdot p'} \bmod n \Rightarrow c^{p'} \equiv \left(x^{q' \cdot p'} \right)^{l} \bmod n \ (47).$$

Ισχύει επίσης

$$x^{p' \cdot q'} \equiv 1 \bmod n \Rightarrow \left(x^{p' \cdot q'} \right)^{l} \equiv 1^{l} \bmod n \Rightarrow \left(x^{q' \cdot p'} \right)^{l} \equiv 1 \bmod n \xrightarrow{(47)} c^{p'} \equiv 1 \bmod n \ (48).$$

Έστω t η τάξη του c ως προς n. Επειδή $n > 3$ και $c \geq 2$, σύμφωνα με την Πρόταση 15.1 η (48) συνεπάγεται ότι

$$p' \equiv 0 \bmod t,$$

δηλαδή $\exists d' \in \mathbb{Z}$ ώστε

$$p' = t \cdot d'.$$

Από την τελευταία εξίσωση προκύπτει ότι το t είναι διαιρέτης του p' το οποίο ως πρώτος αριθμός έχει δύο μη αρνητικούς διαιρέτες, τα $1, p'$. Επειδή $n > 3$ και $c \geq 2$, τότε σύμφωνα με την Πρόταση 14 θα είναι $t \geq 2 > 1$. Έτσι $t \neq 1$ και επειδή το t είναι μη αρνητικός διαιρέτης του p' θα ισχύει $t = p'$. Επομένως η τάξη κάθε στοιχείου του B είναι ίση με p'.

Έστω

$$C = QR_n^* - A - B - \{1\}.$$

Τότε το C είναι υποσύνολο του QR_n^* και το πλήθος των στοιχείων του είναι ίσο με

$$p' \cdot q' - (q'-1) - (p'-1) - 1 = p' \cdot q' - q' - p' + 1 = (p'-1) \cdot (q'-1) \neq 0$$

και άρα $C \neq \varnothing$. Έστω $c \in QR_n^*$ με $c \in C$. Επειδή $1 \notin C$ θα είναι $c \neq 1$ και άρα $c \geq 2$. Επειδή $c \in QR_n^*$ με $c \neq 1$ $\exists l \in \{1, .., p' \cdot q' - 1\}$ ώστε

$$c = x^{l} \bmod n \ (49).$$

Αυτή η εξίσωση συνεπάγεται

$$c^{p' \cdot q'} \equiv \left(x^{l} \right)^{p' \cdot q'} \bmod n = x^{l \cdot p' \cdot q'} \bmod n \Rightarrow c^{p' \cdot q'} \equiv \left(x^{p' \cdot q'} \right)^{l} \bmod n \ (50).$$

Ισχύει επίσης

$$x^{p' \cdot q'} \equiv 1 \bmod n \Rightarrow \left(x^{p' \cdot q'} \right)^{l} \equiv 1^{l} \bmod n \Rightarrow \left(x^{p' \cdot q'} \right)^{l} \equiv 1 \bmod n \xrightarrow{(50)} c^{p' \cdot q'} \equiv 1 \bmod n \ (51).$$

Έστω t η τάξη του c ως προς n. Επειδή $n>3$ και $c\geq 2$, σύμφωνα με την Πρόταση 15.1 η (51) συνεπάγεται ότι

$$p'\cdot q'\equiv 0 \bmod t,$$

δηλαδή $\exists d''\in\mathbb{Z}$ ώστε

$$p'\cdot q' = t\cdot d''.$$

Από την τελευταία εξίσωση προκύπτει ότι το t είναι διαιρέτης του $p'\cdot q'$ το οποίο ως γινόμενο των δύο πρώτων αριθμών p', q', έχει ως μη αρνητικούς διαιρέτες του τα $1, p', q', p'\cdot q'$. Επειδή $n>3$ και $c\geq 2$, τότε σύμφωνα με την Πρόταση 14 θα είναι $t\geq 2>1$. Έτσι $t\neq 1$ και επειδή το t είναι μη αρνητικός διαιρέτης του $p'\cdot q'$ θα είναι ίσο με p' ή q' ή $p'\cdot q'$. Εφόσον το t είναι η τάξη του c ως προς n θα ισχύει

$$c^t\equiv 1 \bmod n \quad (52).$$

Η (49) λόγω και του ότι το $p'\cdot q'$ είναι η τάξη του x ως προς n συνεπάγεται ότι

$$c^t\equiv \left(x^l\right)^t \bmod n \xrightarrow{(52)} x^{l\cdot t}\equiv 1 \bmod n \Rightarrow (l\cdot t)\equiv 0 \bmod (p'\cdot q').$$

Δηλαδή $\exists d_1\in\mathbb{Z}$ ώστε

$$l\cdot t = p'\cdot q'\cdot d_1 \quad (53).$$

Έστω $t=p'$. Τότε η (53) συνεπάγεται ότι

$$l\cdot t = p'\cdot q'\cdot d_1 \Rightarrow l\cdot p' = p'\cdot q'\cdot d_1 \Rightarrow l = q'\cdot d_1 \quad (54).$$

Επίσης $l\in\{1,..,p'\cdot q'-1\}$, όποτε λόγω της (54) θα ισχύει

$$1\leq q'\cdot d_1\leq p'\cdot q'-1< p'\cdot q' \Rightarrow q'\cdot d_1< p'\cdot q' \Rightarrow d_1< p'.$$

Επειδή $d_1\in\mathbb{Z}$, από την τελευταία ανισότητα συνεπάγεται ότι

$$d_1\leq p'-1 \quad (55).$$

Επίσης επειδή $l>0$ και $q'>0$ θα είναι λόγω της (54) και $d_1>0$ και άρα $d_1\geq 1$. Λόγω της τελευταίας ανισότητας και της (55) θα ισχύει

$$1\leq d_1\leq p'-1$$

και επομένως από την (54) προκύπτει πως το l είναι ένα από τα πρώτα $p'-1$ θετικά πολλαπλάσια του q'. Έτσι αφού λόγω της (49) είναι $c=x^l \bmod n$, τότε $c\in B$. Το τελευταίο συμπέρασμα καταλήγει σε άτοπο γιατί

$$c\in C \text{ και } C\cap B=\varnothing,$$

αφού $C=QR_n^*-A-B-\{1\}$. Επομένως είναι $t\neq p'$.

Έστω $t=q'$. Τότε η (53) συνεπάγεται ότι

$$l\cdot t = p'\cdot q'\cdot d_1 \Rightarrow l\cdot q' = p'\cdot q'\cdot d_1 \Rightarrow l = p'\cdot d_1 \quad (56).$$

Επίσης $l\in\{1,..,p'\cdot q'-1\}$, όποτε λόγω της (56) θα ισχύει

$$1\leq p'\cdot d_1\leq p'\cdot q'-1< p'\cdot q' \Rightarrow p'\cdot d_1< p'\cdot q' \Rightarrow d_1< q'.$$

Επειδή $d_1\in\mathbb{Z}$, από την τελευταία ανισότητα συνεπάγεται ότι

$$d_1\leq q'-1 \quad (57).$$

Επίσης επειδή $l>0$ και $p'>0$ θα είναι λόγω της (56) και $d_1>0$ και άρα $d_1\geq 1$. Λόγω της τελευταίας ανισότητας και της (57) θα ισχύει

$$1\leq d_1\leq q'-1$$

και επομένως από την (56) προκύπτει πως το l είναι ένα από τα πρώτα $q'-1$ θετικά πολλαπλάσια του p'. Έτσι αφού λόγω της (49) είναι $c=x^l \bmod n$, τότε $c\in A$. Το τελευταίο συμπέρασμα καταλήγει σε άτοπο γιατί

$$c \in C \text{ και } C \cap A = \varnothing,$$

αφού $C = QR_n^* - A - B - \{1\}$. Επομένως είναι και $t \neq q'$. Άρα $t = p' \cdot q'$. Έτσι η τάξη ως προς n κάθε στοιχείου του C είναι ίση με $p' \cdot q'$.

Από τα παραπάνω συμπεραίνεται πως $\forall c \in QR_n^*$ με $c \neq 1$, η τάξη του c ως προς n είναι ίση με p' ή q' ή $p' \cdot q'$.

6.

Έστω $c \in QR_n^*$ με $c \neq 1$. Τότε σύμφωνα με την Πρόταση 18.5 η τάξη του c ως προς ως προς n είναι ίση με p' ή q' ή $p' \cdot q'$.

Αν είναι ίση με p', τότε ισχύει

$$c^{p'} \equiv 1 \bmod n \Rightarrow \left(c^{p'}\right)^{q'} \equiv 1^{q'} \bmod n \Rightarrow c^{p' \cdot q'} \equiv 1 \bmod n.$$

Αν είναι ίση με q', τότε ισχύει

$$c^{q'} \equiv 1 \bmod n \Rightarrow \left(c^{q'}\right)^{p'} \equiv 1^{p'} \bmod n \Rightarrow c^{p' \cdot q'} \equiv 1 \bmod n.$$

Αν είναι ίση με $p' \cdot q'$, τότε ισχύει

$$c^{p' \cdot q'} \equiv 1 \bmod n.$$

Τέλος, αν $c = 1$ θα ισχύει

$$c^{p' \cdot q'} \bmod n = 1^{p' \cdot q'} \bmod n = 1 \bmod n \Rightarrow c^{p' \cdot q'} \equiv 1 \bmod n.$$

Επομένως $\forall c \in QR_n^*$ ισχύει

$$c^{p' \cdot q'} \equiv 1 \bmod n.$$

<u>Πρόταση 19</u>

Αν $n \in \mathbb{N}^*$ με $n \geq 2$ και $a \in QR_n^*$, τότε $a^{-1} \in QR_n^*$.

<u>Απόδειξη</u>

Επειδή $a \in QR_n^*$ θα είναι και $a \in \mathbb{Z}_n^*$, οπότε σύμφωνα με την Πρόταση 9 $\exists a^{-1} \in \mathbb{Z}_n^*$. Επίσης $\exists x \in \mathbb{Z}_n^*$ ώστε

$$a = x^2 \bmod n.$$

Επειδή $x \in \mathbb{Z}_n^*$ $\exists x^{-1} \in \mathbb{Z}_n^*$. Εφόσον $x^{-1} \in \mathbb{Z}_n^*$, το n είναι πρώτος με το x^{-1} και άρα λόγω της Πρότασης 5.2 θα είναι πρώτος και με το $\left(x^{-1}\right)^2$. Έστω

$$b = \left(x^{-1}\right)^2 \bmod n \text{ (58).}$$

Τότε αφού

$$b \equiv \left(x^{-1}\right)^2 \bmod n,$$

λόγω της Πρότασης 11 το b θα είναι πρώτος με το n. Εξαιτίας της (58) ισχύει

$$b \in \{0, .., n-1\}$$

και άρα $b \in \mathbb{Z}_n^*$. Από τις δύο παραπάνω εξισώσεις συνεπάγεται ότι

$$(a \cdot b) \equiv \left(x^2 \cdot \left(x^{-1}\right)^2\right) \bmod n \Rightarrow (a \cdot b) \equiv \left(x \cdot x^{-1}\right)^2 \bmod n \text{ (59).}$$

Είναι

$$\left(x \cdot x^{-1}\right) \bmod n = 1,$$

οπότε ισχύει ότι

$$\left(x \cdot x^{-1}\right)^2 \equiv 1 \bmod n \xrightarrow{(59)} (a \cdot b) \equiv 1 \bmod n \Rightarrow (a \cdot b) \bmod n = 1,$$

αφού $n \geq 2 > 1$. Έτσι λόγω της τελευταίας εξίσωσης το $b \in \mathbb{Z}_n^*$ είναι ο αντίστροφος του a, δηλαδή

$$a^{-1} = b.$$

Επομένως η (58) γίνεται

$$a^{-1} = \left(x^{-1}\right)^2 \bmod n.$$

Δηλαδή για το $a^{-1} \in \mathbb{Z}_n^*$ υπάρχει στοιχείο του $\mathbb{Z}_n^*$, το x^{-1}, έτσι ώστε να ισχύει η τελευταία εξίσωση. Επομένως $a^{-1} \in QR_n^*$.

Πρόταση 20

Έστω $n \in \mathbb{N}^*$ με $n \geq 2$, $m \in \mathbb{N}^*$ με $m \geq 2$ και $r \in \mathbb{Z}^*$. Τότε ισχύουν τα εξής:

1. Αν $\forall i \in \{1,..,m\}$ $a_i \in QR_n^*$, τότε $\left(\left(\prod_{i=1}^{m} a_i\right) \bmod n\right) \in QR_n^*$.
2. Αν $a \in QR_n^*$, τότε $\left(a^r \bmod n\right) \in QR_n^*$.
3. Αν $\forall i \in \{1,..,m\}$ $a_i \in QR_n^*$ και $r_i \in \mathbb{Z}^*$, τότε $\left(\left(\prod_{i=1}^{m} a_i^{r_i}\right) \bmod n\right) \in QR_n^*$.

Απόδειξη

1.

Ισχύει $m \in \mathbb{N}^*$ με $m \geq 2$, οπότε για $m = 2$ $a_1, a_2 \in QR_n^*$. Έτσι $\exists x_1, x_2 \in \mathbb{Z}_n^*$ ώστε

$$\begin{cases} a_1 = x_1^{\,2} \bmod n \\ a_2 = x_2^{\,2} \bmod n \end{cases}.$$

Από αυτό το σύστημα εξισώσεων προκύπτει πως

$$\left(a_1 \cdot a_2\right) \equiv \left(x_1^{\,2} \cdot x_2^{\,2}\right) \bmod n \Rightarrow \left(a_1 \cdot a_2\right) \equiv \left(x_1 \cdot x_2\right)^2 \bmod n \ (60).$$

Εφόσον $x_1, x_2 \in \mathbb{Z}_n^*$, το n είναι πρώτος με καθένα από τα x_1, x_2, άρα σύμφωνα με την Πρόταση 5.1 θα είναι πρώτος και με το γινόμενό τους $x_1 \cdot x_2$. Έστω

$$y = \left(x_1 \cdot x_2\right) \bmod n.$$

Τότε ισχύει

$$y \in \{0,..,n-1\} \text{ και } y \equiv \left(x_1 \cdot x_2\right) \bmod n \ (61).$$

Αφού τα $x_1 \cdot x_2, n$ είναι πρώτοι μεταξύ τους, σύμφωνα με την Πρόταση 11 από την (61) προκύπτει πως το y είναι πρώτος με το n και επειδή $y \in \{0,..,n-1\}$, τότε το y θα ανήκει συγκεκριμένα στο $\mathbb{Z}_n^*$. Η (61) συνεπάγεται ότι

$$y^2 \equiv \left(x_1 \cdot x_2\right)^2 \bmod n \xrightarrow{(60)} \left(a_1 \cdot a_2\right) \equiv y^2 \bmod n \Rightarrow \left(a_1 \cdot a_2\right) \bmod n = y^2 \bmod n \ (62).$$

Έστω

$$z = \left(a_1 \cdot a_2\right) \bmod n.$$

Τότε ισχύει

$$z \in \{0,..,n-1\} \text{ και } z \equiv \left(a_1 \cdot a_2\right) \bmod n \ (63).$$

Αφού $a_1, a_2 \in QR_n^*$ θα ισχύει $a_1, a_2 \in \mathbb{Z}_n^*$. Έτσι το n είναι πρώτος με καθένα από τα a_1, a_2, άρα σύμφωνα με την Πρόταση 5.1 θα είναι πρώτος και με το γινόμενό τους $a_1 \cdot a_2$. Επομένως σύμφωνα με την Πρόταση 11 από την (63) προκύπτει πως το z

είναι πρώτος με το n και επειδή $z \in \{0,..,n-1\}$, τότε το z θα ανήκει συγκεκριμένα στο $\mathbb{Z}_n^*$. Άρα

$$\left((a_1 \cdot a_2) \bmod n\right) \in \mathbb{Z}_n^*$$

λόγω της (63). Δηλαδή για το $\left((a_1 \cdot a_2) \bmod n\right) \in \mathbb{Z}_n^*$ υπάρχει στοιχείο του $\mathbb{Z}_n^*$, το y, έτσι ώστε να ισχύει η (62). Αυτό σημαίνει πως

$$\left((a_1 \cdot a_2) \bmod n\right) \in QR_n^*.$$

Έστω $m \geq 3$, τότε θα δειχτεί με τέλεια επαγωγή ότι $\forall k \in \{2,..,m\}$

$$\left(\left(\prod_{i=1}^{k} a_i\right) \bmod n\right) \in QR_n^*.$$

Για $k = 2$ η απόδειξη είναι η ίδια όπως και προηγουμένως. Έστω ότι για κάποιο $k \in \{2,..,m-1\}$

$$\left(\left(\prod_{i=1}^{k} a_i\right) \bmod n\right) \in QR_n^*.$$

Θα δειχτεί ότι και

$$\left(\left(\prod_{i=1}^{k+1} a_i\right) \bmod n\right) \in QR_n^*.$$

Λόγω της παραπάνω υπόθεσης είναι $a_{k+1} \in QR_n^*$, οπότε αποδεικνύεται παρόμοια όπως και προηγουμένως ότι το

$$\left(a_{k+1} \cdot \left(\left(\prod_{i=1}^{k} a_i\right) \bmod n\right)\right) \bmod n$$

ανήκει στο QR_n^*. Επειδή $a_{k+1} \in QR_n^*$ θα είναι και $a_{k+1} \in \mathbb{Z}_n^*$, δηλαδή $a_{k+1} < n$ και άρα

$$a_{k+1} \bmod n = a_{k+1}.$$

Λόγω της τελευταίας εξίσωσης και της Πρότασης 8.6 θα ισχύει ότι

$$\left(\prod_{i=1}^{k+1} a_i\right) \bmod n = \left(a_{k+1} \cdot \prod_{i=1}^{k} a_i\right) \bmod n = \left(\left(a_{k+1} \bmod n\right) \cdot \left(\left(\prod_{i=1}^{k} a_i\right) \bmod n\right)\right) \bmod n \Rightarrow$$

$$\left(\prod_{i=1}^{k+1} a_i\right) \bmod n = \left(a_{k+1} \cdot \left(\left(\prod_{i=1}^{k} a_i\right) \bmod n\right)\right) \bmod n.$$

Όπως προαναφέρθηκε το

$$\left(a_{k+1} \cdot \left(\left(\prod_{i=1}^{k} a_i\right) \bmod n\right)\right) \bmod n$$

ανήκει στο QR_n^*, οπότε λόγω της τελευταίας ισότητας

$$\left(\left(\prod_{i=1}^{k+1} a_i\right) \bmod n\right) \in QR_n^*.$$

Άρα $\forall k \in \{2,..,m\}$,

$$\left(\left(\prod_{i=1}^{k} a_i\right) \bmod n\right) \in QR_n^*$$

και επομένως για $k = m$

$$\left(\left(\prod_{i=1}^{m} a_i\right) \bmod n\right) \in QR_n^*.$$

2.

Έστω $r \in \mathbb{Z}_+^*$. Τότε αν $r = 1$ θα ισχύει

$$a^r \bmod n = a^1 \bmod n = a \bmod n \Rightarrow a^r \bmod n = a,$$

αφού $a \in QR_n^*$ και άρα $a \in \mathbb{Z}_n^*$, οπότε $a < n$. Εφόσον $a \in QR_n^*$, τότε από την τελευταία εξίσωση προκύπτει ότι

$$\left(a^r \bmod n\right) \in QR_n^*.$$

Έστω $r \geq 2$. Αν τεθούν $m = r$ και $\forall i \in \{1,..,m\}$ $a_i = a$, τότε $\forall i \in \{1,..,m\}$ $a_i \in QR_n^*$ και έτσι σύμφωνα με την Πρόταση 20.1

$$\left(\left(\prod_{i=1}^{m} a_i\right) \bmod n\right) \in QR_n^*.$$

Ισχύει ότι

$$\left(\prod_{i=1}^{m} a_i\right) \bmod n = \left(\prod_{i=1}^{m} a\right) \bmod n = a^m \bmod n = a^r \bmod n \Rightarrow \left(\prod_{i=1}^{m} a_i\right) \bmod n = a^r \bmod n$$

και άρα

$$\left(a^r \bmod n\right) \in QR_n^*.$$

Έστω $r \in \mathbb{Z}_-^*$. Τότε σύμφωνα με τον Ορισμό 5 ισχύει

$$a^r \bmod n = \left(a^{-1}\right)^{-r} \bmod n.$$

Εφόσον $n \in \mathbb{N}^*$ με $n \geq 2$ και $a \in QR_n^*$, τότε λόγω της Πρότασης 19 θα ισχύει $a^{-1} \in QR_n^*$. Επομένως αφού $(-r) \in \mathbb{Z}_+^*$, τότε σύμφωνα με την προηγούμενη απόδειξη θα ισχύει ότι

$$\left(\left(a^{-1}\right)^{-r} \bmod n\right) \in QR_n^*$$

και άρα λόγω της τελευταίας εξίσωσης

$$\left(a^r \bmod n\right) \in QR_n^*.$$

3.

Έστω ότι $\forall i \in \{1,..,m\}$ είναι

$$b_i = a_i^{r_i} \bmod n.$$

Τότε εφόσον $a_i \in QR_n^*$ και $r_i \in \mathbb{Z}^*$, σύμφωνα με την Πρόταση 20.2 θα ισχύει ότι

$$\left(a_i^{r_i} \bmod n\right) \in QR_n^*$$

και άρα $b_i \in QR_n^*$. Ισχύει

$$\begin{cases} b_1 = a_1^{r_1} \bmod n \\ .. \\ b_m = a_m^{r_m} \bmod n \end{cases} \Rightarrow \left(\prod_{i=1}^{m} b_i\right) \equiv \left(\prod_{i=1}^{m} a_i^{r_i}\right) \bmod n \Rightarrow \left(\prod_{i=1}^{m} b_i\right) \bmod n = \left(\prod_{i=1}^{m} a_i^{r_i}\right) \bmod n.$$

Επειδή $\forall i \in \{1,..,m\}$ $b_i \in QR_n^*$, τότε σύμφωνα με την Πρόταση 20.1 θα ισχύει

$$\left(\left(\prod_{i=1}^{m} b_i\right) \bmod n\right) \in QR_n^*$$

και συνεπώς λόγω της τελευταίας εξίσωσης θα είναι

$$\left(\left(\prod_{i=1}^{m} a_i^{r_i}\right) \bmod n\right) \in QR_n^* .$$

Ισχυρισμός Παραγοντοποίησης σε Πρώτους Αριθμούς [3]

Αν p, p', q, q' είναι περιττοί πρώτοι αριθμοί με $p \neq q$, $p' \neq q'$,

$$p = 2 \cdot p' + 1,\ q = 2 \cdot q' + 1,\ n = p \cdot q$$

και οι δυαδικές αναπαραστάσεις των p, q έχουν το ίδιο πλήθος από bits, τότε το πρόβλημα της παραγοντοποίησης του n στους πρώτους παράγοντές του p, q θεωρείται ότι είναι πάρα πολύ δύσκολο να λυθεί.

Πρώτος Ισχυρισμός Διακριτού Λογαρίθμου [5]

Αν $n, h, g \in \mathbb{N}^*$ με $n \geq 2$ και

$$g \bmod n \neq 1,$$

τότε θεωρείται ότι είναι πάρα πολύ δύσκολο ή και αδύνατο να λυθεί το πρόβλημα εύρεσης διακριτού λογαρίθμου $x \in \mathbb{Z}^*$ του h ως προς τη βάση g, όπου

$$h \equiv g^x \bmod n .$$

Η αδυναμία επίλυσης εντοπίζεται στην περίπτωση που δεν υπάρχει $x \in \mathbb{Z}^*$ που να ικανοποιεί αυτήν την ισοδυναμία, διαφορετικά αν υπάρχει τουλάχιστο ένα τότε είναι πάρα πολύ δύσκολο να βρεθεί.

Δεύτερος Ισχυρισμός Διακριτού Λογαρίθμου [5]

Αν $n, h, k \in \mathbb{N}^*$ με $n \geq 2$, $k \geq 2$ και $\forall i \in \{1,..,k\}$ $g_i \in \mathbb{N}^*$ με

$$g_i \bmod n \neq 1,$$

τότε θεωρείται ότι είναι πάρα πολύ δύσκολο ή και αδύνατο να λυθεί το πρόβλημα εύρεσης k διακριτών λογαρίθμων $x_i \in \mathbb{Z}$ του h ως προς τις k βάσεις g_i, όπου

$$i \in \{1,..,k\},\ (x_1,..,x_k) \neq (0,..,0) \text{ και } h \equiv \left(\prod_{i=1}^{k} g_i^{x_i}\right) \bmod n .$$

Η αδυναμία επίλυσης εντοπίζεται στην περίπτωση που δεν υπάρχουν πλειάδες

$$(x_1,..,x_k) \in \mathbb{Z}^k \text{ με } (x_1,..,x_k) \neq (0,..,0)$$

που να ικανοποιούν αυτήν την ισοδυναμία, διαφορετικά αν υπάρχει τουλάχιστο μία τέτοια τότε είναι πάρα πολύ δύσκολο να βρεθούν τα k στοιχεία της.

Τρίτος Ισχυρισμός Διακριτού Λογαρίθμου [5]

Αν $n, k \in \mathbb{N}^*$ $n \geq 2$, με $k \geq 2$ και $\forall i \in \{1,..,k\}$ $g_i \in \mathbb{N}^*$ με

$$g_i \bmod n \neq 1,$$

τότε θεωρείται ότι είναι πάρα πολύ δύσκολο ή και αδύνατο να λυθεί το πρόβλημα εύρεσης k διακριτών λογαρίθμων $x_i \in \mathbb{Z}$ του 1 ως προς τις k βάσεις g_i, όπου

$$i \in \{1,..,k\},\ (x_1,..,x_k) \neq (0,..,0) \text{ και } 1 = \left(\prod_{i=1}^{k} g_i^{x_i}\right) \bmod n .$$

Η αδυναμία επίλυσης εντοπίζεται στην περίπτωση που δεν υπάρχουν πλειάδες

$$(x_1,..,x_k) \in \mathbb{Z}^k \text{ με } (x_1,..,x_k) \neq (0,..,0)$$

που να ικανοποιούν αυτήν την εξίσωση, διαφορετικά αν υπάρχει τουλάχιστο μία τέτοια τότε είναι πάρα πολύ δύσκολο να βρεθούν τα k στοιχεία της.

Πρόταση 21

Αν p, p', q, q' είναι περιττοί πρώτοι αριθμοί με $p \neq q$, $p' \neq q'$,

$$p = 2 \cdot p' + 1,\ q = 2 \cdot q' + 1,\ n = p \cdot q,$$

$k \in \mathbb{N}^*$ με $k \geq 2$, $\forall i \in \{1,..,k\}$ $g_i \in QR_n^* - \{1\}$ και είναι γνωστά τα p', q', τότε είναι εφικτή η λύση του προβλήματος εύρεσης k διακριτών λογαρίθμων $x_i \in \mathbb{Z}$ του 1 ως προς τις k βάσεις g_i, όπου

$$i \in \{1,..,k\},\ (x_1,..,x_k) \neq (0,..,0) \text{ και } 1 = \left(\prod_{i=1}^{k} g_i^{x_i} \right) \bmod n.$$

Αν τα p', q' είναι άγνωστα, τότε είναι πάρα πολύ δύσκολο να λυθεί το συγκεκριμένο πρόβλημα.

Απόδειξη

Έστω ότι είναι γνωστά τα p', q'. Τότε θα μπορούσε να υπολογιστεί το γινόμενο $p' \cdot q'$. Σύμφωνα με την Πρόταση 18.5 η τάξη ως προς n κάθε στοιχείου, διαφορετικού του 1, του QR_n^* είναι ίση με p' ή q' ή $p' \cdot q'$. Επειδή $\forall i \in \{1,..,k\}$ ισχύει $g_i \in QR_n^* - \{1\}$, το g_i είναι στοιχείο του QR_n^* διαφορετικό του 1 και άρα η τάξη του ως προς n, έστω t_i, θα είναι ίση με p' ή q' ή $p' \cdot q'$. Εφόσον

$$g_i^{t_i} \bmod n = 1,$$

τότε από τη στιγμή που τα $p', q', p' \cdot q'$ είναι γνωστά, είναι δυνατό να υπολογιστούν τα

$$g_i^{p'} \bmod n, g_i^{q'} \bmod n, g_i^{p' \cdot q'} \bmod n$$

και να εξεταστεί ποιο από τα τρία τελευταία είναι ίσο με 1, βρίσκοντας την τάξη t_i του g_i. Ισχύει λόγω της Πρότασης 8.7.3 ότι

$$\begin{cases} g_1^{t_1} \equiv 1 \bmod n \\ .. \\ g_k^{t_k} \equiv 1 \bmod n \end{cases} \Rightarrow \left(\prod_{i=1}^{k} g_i^{t_i} \right) \equiv 1 \bmod n \Rightarrow \left(\prod_{i=1}^{k} g_i^{t_i} \right) \bmod n = 1.$$

Επειδή $\forall i \in \{1,..,k\}$ είναι $t_i \neq 0$, αφού το t_i είναι ίσο με ένα από τα $p', q', p' \cdot q'$, τότε από την τελευταία εξίσωση συμπεραίνεται πως βρίσκοντας τις τάξεις $t_1,..,t_k$ των $g_1,..,g_k$ αντίστοιχα, βρίσκεται ταυτόχρονα μια πλειάδα $(x_1,..,x_k) \in \mathbb{Z}^k$ k διακριτών λογαρίθμων του 1 ως προς τις k βάσεις g_i, όπου

$$(x_1,..,x_k) \neq (0,..,0).$$

Έτσι το πρόβλημα που αναφέρεται στην παρούσα Πρόταση είναι εφικτό να λυθεί.
Η διαδικασία επίλυσής του βασίζεται στη γνώση των p', q', οπότε σε περίπτωση που αυτά είναι άγνωστα αυτή η διαδικασία δεν μπορεί να λάβει χώρα και επομένως λόγω του Τρίτου Ισχυρισμού Διακριτού Λογαρίθμου το συγκεκριμένο πρόβλημα είναι πάρα πολύ δύσκολο να λυθεί.

4. Σχήμα CL Ψηφιακών Υπογραφών

Στην ενότητα αυτή παρουσιάζεται το σχήμα των CL ψηφιακών υπογραφών που εφαρμόζεται σε ψηφιακά πιστοποιητικά από την Αρχή που τα εκδίδει. Η υλοποίηση του σχήματος χωρίζεται σε τέσσερις φάσεις, αυτές της δημιουργίας παραμέτρων, της κωδικοποίησης, της υπογραφής και της επιβεβαίωσης.

4.1. Φάση Δημιουργίας Παραμέτρων

Η φάση αυτή προηγείται από τις άλλες τρεις και κατά τη διάρκειά της η Αρχή δημιουργεί παραμέτρους του ιδιωτικού και δημοσίου κλειδιού της, καθώς και άλλες που θα χρησιμοποιηθούν κατά την εκτέλεση zkp πρωτοκόλλων στα πλαίσια ηλεκτρονικών συναλλαγών που θα έχουν με φορείς νόμιμοι κάτοχοι πιστοποιητικών, τα οποία θα είναι υπογεγραμμένα από την εκδότρια Αρχή σύμφωνα με το σχήμα των CL ψηφιακών υπογραφών. Συγκεκριμένα δημιουργείται ένα μέρος των παραμέτρων που απαρτίζουν το ιδιωτικό της κλειδί, που θα χρησιμοποιεί για να υπογράφει, αλλά και όλες οι παράμετροι που συνθέτουν το δημόσιο κλειδί της το οποίο θα χρησιμοποιηθεί από τους μελλοντικούς νόμιμους κατόχους των πιστοποιητικών που θα εκδόσει η Αρχή, για να επιβεβαιώσουν τις CL ψηφιακές υπογραφές της σε αυτά. Το τμήμα του ιδιωτικού κλειδιού που δημιουργείται στην παρούσα φάση αποτελείται από σταθερές παραμέτρους που θα συμμετέχουν κάθε φορά που η Αρχή θα υπογράφει ένα πιστοποιητικό. Επίσης το δημόσιο κλειδί απαρτίζεται μόνο από σταθερές παραμέτρους που θα συμμετέχουν στην επιβεβαίωση της υπογραφής της Αρχής στο κάθε πιστοποιητικό που θα εκδίδει.

Συγκεκριμένα η Αρχή [6] επιλέγει δύο περιττούς πρώτους αριθμούς p', q' με $p' \neq q'$, έτσι ώστε οι αριθμοί p, q με

$$p = 2 \cdot p' + 1 \text{ και } q = 2 \cdot q' + 1$$

να είναι επίσης πρώτοι και οι δυαδικές τους αναπαραστάσεις να έχουν το ίδιο πλήθος από bits, έστω $l_{p,q}$. Από τις δύο αυτές σχέσεις προκύπτει πως οι p, q είναι περιττοί με $p \neq q$, εφόσον $p' \neq q'$. Η Αρχή υπολογίζει τα γινόμενα

$$n = p \cdot q, p' \cdot q'$$

και κρατάει μυστικά τα

$$p, q, p', q', p' \cdot q' .$$

Η δυαδική αναπαράσταση του n έχει πλήθος από bits ίσο με l_n, όπου

$$l_n = 2 \cdot l_{p,q},$$

αφού το πλήθος των bits της δυαδικής αναπαράστασης του γινομένου δύο αριθμών είναι ίσο με το άθροισμα των bits των δυαδικών τους αναπαραστάσεων. Για τα p, p', q, q', n τηρούνται οι προϋποθέσεις του Ισχυρισμού Παραγοντοποίησης σε Πρώτους Αριθμούς και για αυτό είναι πάρα πολύ δύσκολο να υπολογιστούν οι πρώτοι παράγοντες p, q του n. Το τελευταίο είναι εξαιρετικά μεγάλο και [7] μια ενδεικτική τιμή για το l_n είναι το 1024, οπότε μπορεί να είναι

$$2^{l_n - 1} \leq n < 2^{l_n} \Rightarrow 2^{1023} \leq n < 2^{1024} .$$

Έτσι το διάστημα $\left[2^{1023}, 2^{1024}\right)$ περιέχει ενδεικτικές τιμές για το n.

Ύστερα επιλέγει τυχαία έναν αριθμό S_1 από το σύνολο $\mathbb{Z}_p^*$ και έναν S_2 από το $\mathbb{Z}_q^*$, έτσι ώστε $S_1 \in QR_p^*$ με $S_1 \neq 1$ και $S_2 \in QR_q^*$ με $S_2 \neq 1$. Σύμφωνα με τις Προτάσεις 7 και 13, τα πλήθη των $\mathbb{Z}_p^*, \mathbb{Z}_q^*, QR_p^*, QR_q^*$ είναι $p-1, q-1, p', q'$ αντίστοιχα. Δηλαδή τα

QR_p^*, QR_q^* περιέχουν τα μισά στοιχεία από τα $\mathbb{Z}_p^*, \mathbb{Z}_q^*$ αντίστοιχα. Αυτό σημαίνει πως είναι εύκολο να βρεθούν από τυχαία επιλογή ανάμεσα στους αριθμούς των $\mathbb{Z}_p^*, \mathbb{Z}_q^*$ τα S_1, S_2 αντίστοιχα. Μετά υπολογίζει με βάση το Κινέζικο θεώρημα των υπολοίπων τον μοναδικό, σύμφωνα με την Πρόταση 12, αριθμό $S \in \mathbb{Z}_n^*$ όπου

$$\begin{cases} S \equiv S_1 \bmod p \\ S \equiv S_2 \bmod q \end{cases}.$$

Τότε σύμφωνα με την Πρόταση 18.1 η τάξη του S ως προς n είναι ίση $p' \cdot q'$ και σύμφωνα με την Πρόταση 18.2 $S \in QR_n^*$. Όπως αποδείχτηκε στην απόδειξη της Πρότασης 18.1, θα ισχύει επιπλέον $S \neq 1$. [6] Κατόπιν επιλέγει τυχαία τους αριθμούς l_{R_1}, l_{R_2}, l_S από το σύνολο $\{2,.., p' \cdot q' - 1\}$ και υπολογίζει τα

$$\begin{cases} R_1 = S^{l_{R_1}} \bmod n \\ R_2 = S^{l_{R_2}} \bmod n \\ Z = S^{l_S} \bmod n \end{cases}.$$

Σύμφωνα με την Πρόταση 18.4 θα ισχύει

$$R_1, R_2, Z \in QR_n^*.$$

Επιπλέον, επειδή τα l_{R_1}, l_{R_2}, l_S είναι διάφορα των $1, p' \cdot q'$, τότε τα R_1, R_2, Z είναι διάφορα των

$$S^1 \bmod n = S \text{ και } S^{p' \cdot q'} \bmod n = 1,$$

μια που $S \in QR_n^*$ και άρα $S \in \mathbb{Z}_n^*$, οπότε $S < n$ και $p' \cdot q'$ είναι η τάξη του S ως προς n. Η Αρχή κρατάει μυστικά τα l_{R_1}, l_{R_2}, l_S. Οι p, q είναι περιττοί πρώτοι αριθμοί με $p \neq q$ και ισχύει $n = p \cdot q$. Άρα θα είναι

$$\begin{cases} p \geq 3 \\ q \geq 3 \end{cases}$$

και συνεπώς

$$n = p \cdot q \geq 3 \cdot 3 = 9 > 2.$$

Επίσης $S, R_1, R_2, Z \in QR_n^*$ και έτσι τηρούνται οι προϋποθέσεις της Πρότασης 19, οπότε για τους αντίστροφους $S^{-1}, R_1^{-1}, R_2^{-1}, Z^{-1}$ των S, R_1, R_2, Z αντίστοιχα θα ισχύει

$$S^{-1}, R_1^{-1}, R_2^{-1}, Z^{-1} \in QR_n^*.$$

Αυτοί υπολογίζονται από την Αρχή μέσω του επεκτεινόμενου Ευκλείδειου αλγορίθμου.
Τα

$$n, S^{-1}, R_1^{-1}, R_2^{-1}, Z$$

είναι οι σταθερές παράμετροι του ιδιωτικού κλειδιού το οποίο αποτελείται και από μία μεταβλητή παράμετρο που η Αρχή θα υπολογίζει κάθε φορά που θα υπογράφει ένα πιστοποιητικό. Αυτό σημαίνει πως το ιδιωτικό της κλειδί δεν είναι σταθερό αλλά μπορεί να μεταβάλλεται σε κάθε νέα υπογραφή της. Αντίθετα, όπως προαναφέρθηκε το δημόσιο κλειδί αποτελείται μόνο από σταθερές παραμέτρους οι οποίες είναι οι n, S, R_1, R_2, Z. Η Αρχή δημοσιοποιεί το δημόσιο κλειδί της

$$(n, S, R_1, R_2, Z).$$

Εφόσον γίνονται γνωστά τα S, R_1, R_2, οποιοσδήποτε μπορεί να υπολογίσει και να μάθει τους αντίστροφούς τους $S^{-1}, R_1^{-1}, R_2^{-1}$. Έτσι ξέροντας τα $n, S^{-1}, R_1^{-1}, R_2^{-1}, Z$ ξέρει και μέρος του ιδιωτικού κλειδιού. Αυτό όμως δεν επηρεάζει την εμπιστευτικότητα που πρέπει να διέπει το ιδιωτικό κλειδί της Αρχής, καθώς αυτή εξασφαλίζεται από την εμπιστευτικότητα της μεταβλητής παραμέτρου που θα υπολογίζεται στα πλαίσια κάθε νέας υπογραφής. Έτσι από τη στιγμή που οποιοσδήποτε άλλος εκτός της Αρχής δε θα ξέρει όλες τις παραμέτρους του ιδιωτικού της κλειδιού, αυτό θα παραμένει άγνωστο σε αυτόν. Η δημιουργία της μεταβλητής παραμέτρου περιγράφεται την υποενότητα 4.3.

Εκτός όμως από παραμέτρους των κλειδιών της, η Αρχή δημιουργεί και παραμέτρους που είναι απαραίτητες για τη διεξαγωγή zkp πρωτοκόλλων στα πλαίσια ηλεκτρονικών συναλλαγών που θα έχουν με φορείς νόμιμοι κάτοχοι πιστοποιητικών, τα οποία θα είναι υπογεγραμμένα από την ίδια. Συγκεκριμένα δημιουργεί την παράμετρο g με τον ίδιο τρόπο που δημιούργησε και το $S \in QR_n^*$, οπότε θα ισχύει $g \in QR_n^* - \{1\}$ και η τάξη του g ως προς n θα είναι ίση με $p' \cdot q'$. Θα πρέπει όμως $g \neq S$. Κατόπιν επιλέγει τυχαία τον αριθμό $l_{g'}$ από το σύνολο $\{2,.., p' \cdot q' - 1\}$ και υπολογίζει το

$$g' = g^{l_{g'}} \bmod n \quad (64).$$

Έτσι θα ισχύει $g' \in QR_n^*$ με $g' \neq g$ και $g' \neq 1$. Η Αρχή κρατάει μυστικό το $l_{g'}$ και δημοσιοποιεί τα g, g'.

Αν υποτεθεί πως t είναι ο αριθμός των πεδίων σε κάθε πιστοποιητικό και k οι διαφορετικές δυνατές τιμές που μπορεί να πάρει κάθε ένα από αυτά, τότε η Αρχή βρίσκει τους πρώτους $t \cdot k$ περιττούς πρώτους αριθμούς. Αν $v_{\max}$ είναι ο μέγιστος αυτών των αριθμών, η Αρχή επιλέγει ύστερα έναν περιττό πρώτο αριθμό P', έτσι ώστε να ισχύει

$$P' > v_{\max} + 1$$

και ο αριθμός P με

$$P = 2 \cdot P' + 1$$

να είναι επίσης πρώτος. Από τη σχέση αυτή προκύπτει πως ο P είναι και αυτός περιττός. Θα πρέπει καθένα από τα P, P' να είναι διαφορετικό από τα p', q', p, q. Ύστερα επιλέγει τυχαία και εύκολα έναν αριθμό f από το σύνολο $\mathbb{Z}_P^*$, έτσι ώστε $f \in QR_P^*$ με $f \neq 1$. Τότε σύμφωνα με την Πρόταση 16 η τάξη του f ως προς P είναι ίση με P' και σύμφωνα με την Πρόταση 17 το f είναι γεννήτορας του QR_P^*. Συγκεκριμένα όπως αναφέρεται στο τέλος της απόδειξης της Πρότασης 17, θα ισχύει

$$QR_P^* = \left\{ f^1 \bmod P,\ f^2 \bmod P,..,\ f^{P'-1} \bmod P,\ f^{P'} \bmod P \right\}.$$

Κατόπιν η Αρχή επιλέγει τυχαία τον αριθμό $l_{f'}$ από το σύνολο $\{2,.., P' - 1\}$ και υπολογίζει το

$$f' = f^{l_{f'}} \bmod P \quad (65).$$

Σύμφωνα με την παραπάνω αναπαράσταση του QR_P^* θα ισχύει $f' \in QR_P^*$. Επιπλέον, επειδή το $l_{f'}$ είναι διάφορο των $1, P'$, τότε το f' είναι διάφορο των

$$f^1 \bmod P = f \quad \text{και} \quad f^{P'} \bmod P = 1,$$

μια που $f \in QR_P^*$ και άρα $f \in \mathbb{Z}_P^*$, οπότε $f < P$ και P' είναι η τάξη του f ως προς P. Η Αρχή κρατάει μυστικό το $l_{f'}$ και δημοσιοποιεί τα P, P', f, f'.

4.2. Φάση Κωδικοποίησης

Στη φάση αυτή λαμβάνει χώρα η κωδικοποίηση των πληροφοριών που πρόκειται να υπογραφούν. Αμέσως μετά το τέλος της προηγούμενης φάσης, [6] η εκδότρια Αρχή αντιστοιχίζει την καθεμία από όλες τις τιμές που μπορούν να λάβουν όλα τα πεδία ενός πιστοποιητικού, σε έναν διαφορετικό πρώτο αριθμό. Όπως αναφέρθηκε στην προηγούμενη υποενότητα, ο αριθμός των πεδίων κάθε πιστοποιητικού είναι ίσος με t και οι διαφορετικές δυνατές τιμές που μπορεί να πάρει κάθε ένα από αυτά είναι k. Τότε το πλήθος όλων των τιμών που μπορούν να λάβουν όλα τα πεδία είναι ίσο με $t \cdot k$. Η Αρχή κωδικοποιεί καθεμία από αυτές τις $t \cdot k$ τιμές σε έναν από τους πρώτους $t \cdot k$ περιττούς πρώτους αριθμούς που βρήκε κατά τη φάση δημιουργίας παραμέτρων. Κάθε τιμή κωδικοποιείται σε έναν διαφορετικό πρώτο αριθμό. Ο μέγιστος πρώτος αριθμός στον οποίο μπορεί να είναι κωδικοποιημένη μία τιμή είναι ο $v_{\max}$, σύμφωνα με το τέλος της προηγούμενης υποενότητας. Η Αρχή κατηγοριοποιεί τους $t \cdot k$ πρώτους αριθμούς σε t ομάδες των k αριθμών την καθεμία και αντιστοιχίζει ένα πεδίο σε μια τέτοια ομάδα και κάθε τιμή του αυτού του πεδίου σε έναν διαφορετικό αριθμό αυτής της ομάδας. Δηλαδή αν $i \in \{1,..,t\}$, η iοστή ομάδα περιέχει τους πρώτους αριθμούς στους οποίους κωδικοποιούνται οι k τιμές που μπορεί να πάρει το iοστό πεδίο. Η μεταβλητή i είναι ο δείκτης ενός πεδίου και για αυτό παίρνει τιμές από το σύνολο $\{1,..,t\}$. Αν a_i είναι η μεταβλητή που αποτελεί τον δείκτη της τιμής που παίρνει το iοστό πεδίο, τότε $a_i \in \{1,..,k\}$. Δηλαδή η a_iοστή τιμή του iοστού πεδίου αντιστοιχεί στον a_iοστό πρώτο αριθμό της iοστής ομάδας. Αν $e_1, e_2, .., e_{t \cdot k}$ οι $t \cdot k$ πρώτοι αριθμοί, τότε θεωρείται πως οι

$$e_{(i-1)\cdot k+1}, e_{(i-1)\cdot k+2}, .., e_{(i-1)\cdot k+k}$$

είναι οι k αριθμοί της iοστής ομάδας. Έτσι το $e_{(i-1)\cdot k+a_i}$ είναι ο πρώτος αριθμός στον οποίο κωδικοποιείται η a_iοστή τιμή του iοστού πεδίου και αποτελεί τον κώδικά της. Οι κώδικες όλων των τιμών που μπορούν να λάβουν όλα τα πεδία ενός πιστοποιητικού, καταγράφονται από την Αρχή σε μια λίστα με τέτοιο τρόπο ώστε μαζί με τον κάθε κωδικό σε πλήρη αντιστοίχιση να είναι καταγεγραμμένη και η τιμή στην οποία αντιστοιχεί. Η λίστα αυτή των κωδικών των τιμών των πεδίων δημοσιοποιείται από την Αρχή.

Όταν η τελευταία εκδίδει ένα πιστοποιητικό, το κωδικοποιεί, ως ηλεκτρονικό έγγραφο που είναι, μέσω των ASCII κωδικών των χαρακτήρων του σε έναν μη μηδενικό φυσικό αριθμό m. Θεωρείται πως το πιστοποιητικό ως ψηφιακό έγγραφο είναι τέτοιο ώστε ο αριθμός στον οποίο κωδικοποιείται να ανήκει σε ένα συγκεκριμένο εύρος τιμών. Συγκεκριμένα [6] η δυαδική αναπαράσταση του αριθμού m έχει σταθερό πλήθος από bits ίσο με l_m. Αυτό σημαίνει πως το m παίρνει τιμές από το σύνολο $\{1,..,2^{l_m}-1\}$. Ύστερα η Αρχή υπολογίζει το γινόμενο των πρώτων αριθμών στους οποίους αντιστοιχούν οι τιμές που έχουν τα πεδία του πιστοποιητικού, δηλαδή το

$$\prod_{i=1}^{t} e_{(i-1)\cdot k+a_i} .$$

Θεωρείται πως η δυαδική αναπαράσταση καθενός από όλους τους $t \cdot k$ πρώτους αριθμούς έχει σταθερό πλήθος από bits ίσο με $\frac{l_m}{t}$ και επομένως αυτοί ανήκουν στο διάστημα $\left(2, 2^{\frac{l_m}{t}} - 1\right]$. Επειδή το πλήθος των bits της δυαδικής αναπαράστασης του γινομένου δύο αριθμών είναι ίσο με το άθροισμα των bits των δυαδικών τους αναπαραστάσεων, τότε η δυαδική αναπαράσταση του $\prod_{i=1}^{t} e_{(i-1)\cdot k + a_i}$ θα έχει πλήθος από bits ίσο με

$$t \cdot \frac{l_m}{t} = l_m,$$

όσο δηλαδή έχει και η δυαδική αναπαράσταση του m στο οποίο αντιστοιχίζεται το πιστοποιητικό. Αυτό σημαίνει πως και το $\prod_{i=1}^{t} e_{(i-1)\cdot k + a_i}$ παίρνει τιμές από το σύνολο $\left\{1, .., 2^{l_m} - 1\right\}$.

4.3. Φάση Υπογραφής

Στη συγκεκριμένη φάση δημιουργείται το υπόλοιπο μέρος του ιδιωτικού κλειδιού που αποτελείται από μία μεταβλητή παραμέτρο η οποία μπορεί να έχει και διαφορετική τιμή κάθε φορά που υπογράφεται ένα νέο πιστοποιητικό. Επίσης πραγματοποιείται η υπογραφή των πληροφοριών, συγκεκριμένα του αριθμού στον οποίο είναι κωδικοποιημένο το πιστοποιητικό, αλλά και του γινομένου των πρώτων αριθμών στους οποίους είναι κωδικοποιημένες οι τιμές που έχουν τα πεδία του πιστοποιητικού.

[6] Η εκδότρια Αρχή επιλέγει τυχαία έναν έναν αριθμό $v \in \mathbb{N}^*$ του οποίου η δυαδική αναπαράσταση έχει πλήθος από bits ίσο με l_v, όπου

$$l_v = l_n + l_m + l$$

με $l \in \mathbb{N}^*$. Επίσης επιλέγει τυχαία έναν πρώτο αριθμό e έτσι ώστε $e \neq p'$, $e \neq q'$ και $e < p' \cdot q'$. Θεωρείται πως η δυαδική του αναπαράσταση του e έχει πλήθος από bits ίσο με l_e, όπου

$$l_e > l_m + 2 \text{ και ισχύει } e \in \left(2^{l_e - 1}, 2^{l_e}\right).$$

Επειδή οι e, p', q' είναι πρώτοι αριθμοί με $e \neq p'$ και $e \neq q'$, τότε σύμφωνα με την Πρόταση 2 ο e είναι πρώτος με καθέναν από τους p', q' και συνεπώς λόγω της Πρότασης 5.1, ο e είναι πρώτος και με το γινόμενο $p' \cdot q'$. Αυτό σημαίνει πως $e \in \mathbb{Z}^*_{p' \cdot q'}$, από τη στιγμή που $e < p' \cdot q'$. Επίσης οι p', q' είναι περιττοί πρώτοι αριθμοί, άρα

$$\begin{cases} p' \geq 3 \\ q' \geq 3 \end{cases}$$

και συνεπώς

$$p' \cdot q' \geq 3 \cdot 3 = 9 > 2.$$

Έτσι [6] τηρούνται οι προϋποθέσεις της Πρότασης 9 και για αυτό υπάρχει ο αντίστροφος $e^{-1} \in \mathbb{Z}^*_{p' \cdot q'}$ του e, που είναι μοναδικός και για τον οποίο ισχύει

$$\left(e\cdot e^{-1}\right)\bmod\left(p'\cdot q'\right)=1.$$

Η Αρχή τον υπολογίζει χρησιμοποιώντας τον επεκτεινόμενο Ευκλείδειο αλγόριθμο. Αν $d=e^{-1}$ τότε $d\in\mathbb{Z}^*_{p'\cdot q'}$, δηλαδή το d είναι πρώτος με το $p'\cdot q'$ και ισχύει

$$\left(e\cdot d\right)\bmod\left(p'\cdot q'\right)=1 \text{ (66).}$$

Από την τελευταία σχέση προκύπτει πως $\exists k\in\mathbb{N}^*$ ώστε

$$e\cdot d=p'\cdot q'\cdot k+1 \text{ (67).}$$

Το d κρατείται μυστικό από την Αρχή και αποτελεί την μεταβλητή παράμετρο του ιδιωτικού κλειδιού, το οποίο στην ολοκληρωμένη του μορφή είναι η εξάδα

$$\left(n,S^{-1},R_1^{-1},R_2^{-1},Z,d\right).$$

Επειδή κάθε φορά που υπογράφεται ένα πιστοποιητικό το e επιλέγεται τυχαία, η τιμή του μπορεί να είναι διαφορετική σε κάθε φάση υπογραφής με αποτέλεσμα το d που υπολογίζεται από την (66), να έχει και αυτό μεταβαλλόμενη τιμή και έτσι να μην αποτελεί μία σταθερή παράμετρο. Επίσης όπως αναφέρθηκε στην υποενότητα 4.1, το d είναι η μόνη παράμετρος του ιδιωτικού κλειδιού που κρατείται μυστική και για αυτόν τον λόγο η εμπιστευτικότητά του είναι αυτή που εξασφαλίζει την εμπιστευτικότητα του ιδιωτικού κλειδιού.

Αν m_1 η κωδικοποίηση του πιστοποιητικού και

$$m_2=\prod_{i=1}^{t}e_{(i-1)\cdot k+a_i},$$

τότε $m_1,m_2\in\mathbb{N}^*$. Η Αρχή υπολογίζει το A, όπου

$$A=\left(\left(R_1^{-1}\right)^{m_1}\cdot\left(R_2^{-1}\right)^{m_2}\cdot\left(S^{-1}\right)^{v}\cdot Z\right)^{d}\bmod n \text{ (68).}$$

Από την τελευταία σχέση φαίνεται με ποιον τρόπο το ιδιωτικό κλειδί εφαρμόζεται στις πληροφορίες $m_1,m_2\in\mathbb{N}^*$ που πρόκειται να υπογραφούν, προκειμένου να παραχθεί ένα μέρος της ψηφιακής υπογραφής, το A. Η πλήρης υπογραφή των πληροφοριών m_1,m_2, είναι η τριάδα $\left(A,e,v\right)$. Η Αρχή αποστέλλει το πιστοποιητικό στον νόμιμο ιδιοκτήτη του, μαζί με το m_2 και την υπογραφή $\left(A,e,v\right)$.

Η (68) συνεπάγεται λόγω των Προτάσεων 10.3 και 10.4 ότι

$$A=\left(\left(R_1^{-1}\right)^{m_1\cdot d}\cdot\left(R_2^{-1}\right)^{m_2\cdot d}\cdot\left(S^{-1}\right)^{v\cdot d}\cdot Z^{d}\right)\bmod n.$$

Εφόσον $S^{-1},R_1^{-1},R_2^{-1},Z\in QR_n^*$ και $m_1,m_2,d,v\in\mathbb{N}^*$, τότε λόγω της τελευταίας εξίσωσης και της Πρότασης 20.3 θα ισχύει $A\in QR_n^*$. Λόγω της (68), του Ορισμού 5 και των Προτάσεων 10.1, 10.4 και 10.3 θα ισχύει, μια και $m_1,m_2,v\in\mathbb{N}^*$, ότι

$$A=\left(R_1^{-m_1}\cdot R_2^{-m_2}\cdot S^{-v}\cdot Z\right)^{d}\bmod n\Rightarrow A^e\equiv\left(\left(R_1^{-m_1}\cdot R_2^{-m_2}\cdot S^{-v}\cdot Z\right)^{d}\right)^{e}\bmod n=$$

$$\left(R_1^{-m_1}\cdot R_2^{-m_2}\cdot S^{-v}\cdot Z\right)^{d\cdot e}\bmod n\xrightarrow{(67)}A^e\equiv\left(R_1^{-m_1}\cdot R_2^{-m_2}\cdot S^{-v}\cdot Z\right)^{p'\cdot q'\cdot k+1}\bmod n\Rightarrow$$

$$A^e\equiv\left(R_1^{-m_1\cdot(p'\cdot q'\cdot k+1)}\cdot R_2^{-m_2\cdot(p'\cdot q'\cdot k+1)}\cdot S^{-v\cdot(p'\cdot q'\cdot k+1)}\cdot Z^{\,p'\cdot q'\cdot k+1}\right)\bmod n \text{ (69).}$$

Επειδή $S^{-1},R_1^{-1},R_2^{-1},Z\in QR_n^*$, τότε σύμφωνα με την Πρόταση 18.6 θα ισχύει

$$\begin{cases} \left(R_1^{-1}\right)^{p'\cdot q'} \equiv 1 \bmod n \\ \left(R_2^{-1}\right)^{p'\cdot q'} \equiv 1 \bmod n \\ \left(S^{-1}\right)^{p'\cdot q'} \equiv 1 \bmod n \\ Z^{p'\cdot q'} \equiv 1 \bmod n \end{cases}.$$

Λόγω του Ορισμού 5 και των Προτάσεων 10.1, 10.4, 8.7.2, συνεπάγεται από το τελευταίο σύστημα ισοδυναμιών ότι

$$\begin{cases} R_1^{-p'\cdot q'} \equiv 1 \bmod n \\ R_2^{-p'\cdot q'} \equiv 1 \bmod n \\ S^{-p'\cdot q'} \equiv 1 \bmod n \\ Z^{p'\cdot q'} \equiv 1 \bmod n \end{cases} \Rightarrow \begin{cases} \left(R_1^{-p'\cdot q'}\right)^k \equiv 1^k \bmod n \\ \left(R_2^{-p'\cdot q'}\right)^k \equiv 1^k \bmod n \\ \left(S^{-p'\cdot q'}\right)^k \equiv 1^k \bmod n \\ \left(Z^{p'\cdot q'}\right)^k \equiv 1^k \bmod n \end{cases} \Rightarrow \begin{cases} R_1^{-p'\cdot q'\cdot k} \equiv 1 \bmod n \\ R_2^{-p'\cdot q'\cdot k} \equiv 1 \bmod n \\ S^{-p'\cdot q'\cdot k} \equiv 1 \bmod n \\ Z^{p'\cdot q'\cdot k} \equiv 1 \bmod n \end{cases} \Rightarrow$$

$$\begin{cases} R_1^{-p'\cdot q'\cdot k-1} \equiv R_1^{-1} \bmod n \\ R_2^{-p'\cdot q'\cdot k-1} \equiv R_2^{-1} \bmod n \\ S^{-p'\cdot q'\cdot k-1} \equiv S^{-1} \bmod n \\ Z^{p'\cdot q'\cdot k+1} \equiv Z \bmod n \end{cases} \Rightarrow \begin{cases} \left(R_1^{-p'\cdot q'\cdot k-1}\right)^{m_1} \equiv \left(R_1^{-1}\right)^{m_1} \bmod n \\ \left(R_2^{-p'\cdot q'\cdot k-1}\right)^{m_2} \equiv \left(R_2^{-1}\right)^{m_2} \bmod n \\ \left(S^{-p'\cdot q'\cdot k-1}\right)^{v} \equiv \left(S^{-1}\right)^{v} \bmod n \\ Z^{p'\cdot q'\cdot k+1} \equiv Z \bmod n \end{cases} \Rightarrow$$

$$\begin{cases} R_1^{-m_1\cdot(p'\cdot q'\cdot k+1)} \equiv \left(R_1^{-1}\right)^{m_1} \bmod n \\ R_2^{-m_2\cdot(p'\cdot q'\cdot k+1)} \equiv \left(R_2^{-1}\right)^{m_2} \bmod n \\ S^{-v\cdot(p'\cdot q'\cdot k+1)} \equiv \left(S^{-1}\right)^{v} \bmod n \\ Z^{p'\cdot q'\cdot k+1} \equiv Z \bmod n \end{cases}.$$

Λόγω της Πρότασης 8.7.3, το τελευταίο σύστημα ισοδυναμιών συνεπάγεται ότι

$$\left(R_1^{-m_1\cdot(p'\cdot q'\cdot k+1)} \cdot R_2^{-m_2\cdot(p'\cdot q'\cdot k+1)} \cdot S^{-v\cdot(p'\cdot q'\cdot k+1)} \cdot Z^{p'\cdot q'\cdot k+1}\right) \equiv \left(R_1^{-m_1} \cdot R_2^{-m_2} \cdot S^{-v} \cdot Z\right) \bmod n \xrightarrow{(69)}$$

$$A^e \equiv \left(R_1^{-m_1} \cdot R_2^{-m_2} \cdot S^{-v} \cdot Z\right) \bmod n.$$

Λόγω της Πρότασης 10.5, η τελευταία ισοδυναμία συνεπάγεται ότι

$$Z \equiv \left(A^e \cdot R_1^{m_1} \cdot R_2^{m_2} \cdot S^v\right) \bmod n \quad (70).$$

Επειδή $Z \in QR_n^*$ θα είναι και $Z \in \mathbb{Z}_n^*$, οπότε $Z < n$. Αυτό σημαίνει πως η (70) γίνεται

$$Z = \left(A^e \cdot R_1^{m_1} \cdot R_2^{m_2} \cdot S^v\right) \bmod n \quad (71).$$

4.4. Φάση Επιβεβαίωσης

Στη συγκεκριμένη φάση λαμβάνει χώρα η διαδικασία της επιβεβαίωσης της γνησιότητας της CL ψηφιακής υπογραφής από τον υποψήφιο νόμιμο ιδιοκτήτη του πιστοποιητικού. Συγκεκριμένα ο τελευταίος αφού παραλάβει το πιστοποιητικό, το m_2 και την υπογραφή (A, e, v), κωδικοποιεί το πιστοποιητικό μέσω των ASCII κωδικών των χαρακτήρων του στον αντίστοιχο μη μηδενικό φυσικό αριθμό m_1. Ύστερα ελέγχει αν ισχύει η (71). Σε περίπτωση που αποβεί θετικός ο έλεγχος τότε

αποφαίνεται πως το πιστοποιητικό, το m_2 και η υπογραφή (A,e,v) δημιουργήθηκαν και στάλθηκαν από την εκδότρια Αρχή με αποτέλεσμα να αποδεχτεί το πιστοποιητικό ως έγκυρο. Διαφορετικά αν δεν ισχύει η (71) δεν πείθεται ότι ο δημιουργός και αποστολέας των τριών παραπάνω είναι η ίδια η Αρχή και έτσι απορρίπτει το πιστοποιητικό.

Στην περίπτωση που επαληθευτεί η (71) ο παραλήπτης συμπεραίνει πως το πιστοποιητικό είναι γνήσιο, γιατί κανείς άλλος εκτός της Αρχής δε θα μπορούσε να δημιουργήσει και να αποστείλει το συγκεκριμένο μαζί με το m_2 και την υπογραφή (A,e,v). Κάποιος που θα επιχειρήσει να το κάνει θα δημιουργήσει αρχικά ένα πιστοποιητικό και θα υπολογίσει τα αντίστοιχα m_1, m_2. Μετά για αυτά θα προσπαθήσει να βρει τέτοια A,e,v ώστε να ισχύσει η (71).

Έστω πως αρχικά διαλέγει τυχαία τιμές για τα v,e. Το δεύτερο θα πρέπει να είναι πρώτος αριθμός και μάλιστα να ισχύει $e \neq p'$ και $e \neq q'$ όπως αναφέρθηκε στην προηγούμενη υποενότητα. Στην περίπτωση που η τυχαία επιλογή του e πληρεί αυτά τα κριτήρια, τότε θα πρέπει μετά να υπολογίσει έναν αριθμό d από την εξίσωση

$$(e \cdot d) \bmod (p' \cdot q') = 1 \quad (66)$$

ώστε μετά να τον χρησιμοποιήσει για τον υπολογισμό του A από τη σχέση

$$A = \left(\left(R_1^{-1}\right)^{m_1} \cdot \left(R_2^{-1}\right)^{m_2} \cdot \left(S^{-1}\right)^{v} \cdot Z \right)^{d} \bmod n \quad (68).$$

Προκειμένου όμως να λύσει την (66) ως προς d είναι απαραίτητη η γνώση του $p' \cdot q'$ την οποία δεν έχει, αφού όπως αναφέρθηκε στην υποενότητα 4.1 αυτό κρατείται μυστικό από την Αρχή. Επίσης δεν μπορεί ούτε να το υπολογίσει καθώς αφενός δε γνωρίζει τους παράγοντές του p', q' ώστε να τους πολλαπλασιάσει και αφετέρου δεν ξέρει τα p,q από τα οποία θα μπορούσε να βρει τα p', q' χρησιμοποιώντας τις εξισώσεις

$$p = 2 \cdot p' + 1, \; q = 2 \cdot q' + 1$$

αντίστοιχα. Η έλλειψη γνώσης των p, q, p', q' οφείλεται στο γεγονός πως και αυτά κρατούνται μυστικά από την Αρχή. Επίσης όπως αναφέρθηκε στην υποενότητα 4.1, είναι πάρα πολύ δύσκολο να υπολογιστούν οι πρώτοι παράγοντες p,q του

$$n = p \cdot q .$$

Έτσι από τη στιγμή που δε γνωρίζει και δεν μπορεί να υπολογίσει το γινόμενο $p' \cdot q'$ αδυνατεί να λύσει την (66) ως προς d και άρα να υπολογίσει το A από την (68).

Έστω πως δεν επιλέγει εκείνος το e αλλά μαθαίνει κάποιο από τα e που έχει επιλέξει τυχαία η Αρχή σε κάποια φάση υπογραφής και σκοπός του είναι να πληροφορηθεί και το αντίστοιχο $d = e^{-1}$ που έχει υπολογίσει η Αρχή στην ίδια φάση, έτσι ώστε αυτός να μπορέσει να υπολογίσει το A από την (68). Επειδή σε κάθε φάση υπογραφής η Αρχή κρατάει μυστικό το d που υπολογίζει, είναι αδύνατο για εκείνον να το μάθει.

Έστω πως διαλέγει τυχαία τιμές για τα v,d. Το δεύτερο θα πρέπει να είναι πρώτος με το $p' \cdot q'$ όπως αναφέρθηκε στην προηγούμενη υποενότητα. Αυτός θα μπορέσει να υπολογίσει από την (68) το A, όμως στην περίπτωση που τύχει το d να είναι πρώτος δε θα μπορέσει να χρησιμοποιήσει την (66) για να υπολογίσει το e ώστε να θέσει το τελευταίο στην τριάδα της υπογραφής (A,e,v) που θα αποστείλει μετά και να μπορέσει ο παραλήπτης να επαληθεύσει την (71). Ο υπολογισμός του e είναι

ανέφικτος εξαιτίας του γεγονότος ότι το $p' \cdot q'$ είναι άγνωστο και δεν μπορεί να υπολογιστεί.
Έστω τέλος πως διαλέγει τυχαία μια τιμή για την παράμετρο A. Τότε λόγω του Δεύτερου Ισχυρισμού Διακριτού Λογαρίθμου θα είναι πάρα πολύ δύσκολο ή και αδύνατο να μπορέσει να βρει από την (71) κάποια e, v που αποτελούν λογαρίθμους του Z ως προς τα A, S αντίστοιχα. Αν επιλέξει μια τυχαία τιμή για το v, τότε σύμφωνα με τον Πρώτο Ισχυρισμό Διακριτού Λογαρίθμου θα είναι πάρα πολύ δύσκολο ή και αδύνατο να μπορέσει να βρει από την (68) κάποιο d που αποτελεί λογάριθμο του A ως προς τη βάση

$$\left(R_1^{-1}\right)^{m_1} \cdot \left(R_2^{-1}\right)^{m_2} \cdot \left(S^{-1}\right)^{v} \cdot Z,$$

ώστε μετά να το χρησιμοποιήσει για να υπολογίσει το e από την (66). Ακόμα και αν καταφέρει να βρει κάποιο d, τότε είναι αδύνατο να υπολογίσει μετά το e από την (66) εφόσον δε γνωρίζει το $p' \cdot q'$.

[7], [6] Οι ίδιοι οι Camenisch Lysyanskaya που δημιούργησαν το CL σχήμα υπογραφών αναφέρουν πως εκτός από την ισχύ της (71) θα πρέπει επίσης να ελεγχθεί αν

$$m_1, m_2 \in \left\{1, .., 2^{l_m} - 1\right\} \text{ και } e \in \left(2^{l_e - 1}, 2^{l_e}\right)$$

προκειμένου να αποφανθεί ο παραλήπτης πως η ψηφιακή υπογραφή είναι γνήσια, όπου m_1 ο μη μηδενικός φυσικός αριθμός στον οποίο ο παραλήπτης κωδικοποιεί το πιστοποιητικό. Όπως όμως αποδείχτηκε παραπάνω, η επαλήθευση της (71) αποτελεί από μόνη της απόδειξη πως η υπογραφή (A, e, v) είναι της Αρχής. Για αυτόν τον λόγο προσωπικά θεωρώ περιττούς τους δύο επιπλέον ελέγχους που προτείνουν οι δημιουργοί του CL σχήματος υπογραφών. Από τη στιγμή που η επαλήθευση της (71) αποδεικνύει ότι το πιστοποιητικό, το m_2 και η υπογραφή (A, e, v) δημιουργήθηκαν και στάλθηκαν από την εκδότρια Αρχή και με δεδομένο ότι σε κάθε φάση υπογραφής αυτή επιλέγει να είναι $m_1, m_2 \in \left\{1, .., 2^{l_m} - 1\right\}$ και $e \in \left(2^{l_e - 1}, 2^{l_e}\right)$, τότε για τα m_2, e που παραλαμβάνει ο παραλήπτης και το m_1 που υπολογίζει θα ισχύουν οι δύο επιπλέον συνθήκες.

5. Αποδεικτικά Πρωτόκολλα Μηδενικής Γνώσης

Στην ενότητα αυτή μελετάται η χρήση zkp πρωτοκόλλων σε διάφορες ηλεκτρονικές συναλλαγές που έχουν με φορείς νόμιμοι κάτοχοι ψηφιακών πιστοποιητικών, τα οποία εκδόθηκαν και υπογράφτηκαν από την εκδότρια Αρχή σύμφωνα με το σχήμα των CL ψηφιακών υπογραφών. Όπως αναφέρθηκε στην ενότητα 2, τέτοιες συναλλαγές αφορούν την πρόσβαση σε υπηρεσίες ή την παροχή δικαιωμάτων που επιτυγχάνονται με την ικανοποίηση κριτηρίων από τις τιμές συγκεκριμένων από τα πεδία του πιστοποιητικού. Ο έλεγχος που διενεργείται από τον φορέα προκειμένου να διαπιστωθεί η εγκυρότητα του πιστοποιητικού και εάν ικανοποιούνται τα κριτήρια αυτά, πραγματοποιείται με την χρήση zkp πρωτοκόλλων ώστε να διασφαλίζεται η ιδιωτικότητα των τιμών των πεδίων του πιστοποιητικού.

[8] Σε ένα αποδεικτικό πρωτόκολλο μηδενικής γνώσης συμμετέχουν δύο οντότητες, ο *Prover* που διατυπώνει μία πρόταση η οποία μπορεί να είναι αληθής ή ψευδής και ο *Verifier* που δε γνωρίζει την τιμή αληθείας της. Σκοπός του Prover είναι να πείσει για το αληθές της πρότασης τον Verifier χρησιμοποιώντας το zkp πρωτόκολλο, το οποίο

είναι μια σειρά βημάτων καθένα από τα οποία εκτελείται είτε από τον έναν είτε από τον άλλον. Αν η πρόταση ισχύει και τηρήσουν και οι δύο το πρωτόκολλο, τότε μετά την εκτέλεσή του ο Verifier θα πειστεί σχεδόν κατά 100%, ενώ αν δεν τηρηθεί τότε δε θα πειστεί σχεδόν κατά 100%. Αν η πρόταση δεν ισχύει, τότε ανεξάρτητα αν το πρωτόκολλο τηρηθεί ή όχι, ο Verifier δε θα πειστεί σχεδόν κατά 100%.
Η πρόταση που διατυπώνει ο Prover σχετίζεται πάντα με ορισμένες πληροφορίες. Κατά τη διάρκεια και μετά το τέλος του πρωτοκόλλου ο Verifier δεν μπορεί να μάθει άμεσα ή να εξάγει έμμεσα από μόνος του αυτές τις πληροφορίες. Για αυτό και τέτοιου είδους πρωτόκολλα απόδειξης χαρακτηρίζονται από την μηδενική γνώση που παρέχουν άμεσα ή έμμεσα για τέτοιες πληροφορίες, δηλαδή την μηδενική πληροφόρηση για λόγους ασφάλειας. Έτσι αυτά είναι κατάλληλα όταν χρειάζεται να αποδειχτεί ένας ισχυρισμός, χωρίς όμως παράλληλη αποκάλυψη ευαίσθητων και προσωπικών δεδομένων που σχετίζονται με αυτόν.

Μια τέτοια περίπτωση ισχυρισμού είναι ότι τα προαναφερθέντα κριτήρια ικανοποιούνται από τις τιμές των προαναφερθέντων συγκεκριμένων πεδίων ενός πιστοποιητικού. Ο νόμιμος κάτοχός του πρέπει να αποδείξει στον φορέα αυτόν τον ισχυρισμό, χωρίς όμως την άμεση ή έμμεση πληροφόρηση των παραπάνω τιμών που σχετίζονται με τον συγκεκριμένο ισχυρισμό. Αυτές αποτελούν προσωπικά αλλά μπορεί και ευαίσθητα δεδομένα. Στο προτελευταίο παράδειγμα της ενότητας 2 ο ισχυρισμός είναι ο εξής: '*ο αριθμός των τέκνων είναι μεγαλύτερος ή ίσος του* 3'. Τα προσωπικά δεδομένα που σχετίζονται με αυτήν την πρόταση είναι ο αριθμός των τέκνων. Ο νόμιμος κάτοχος αποδεικνύει την εγκυρότητα του πιστοποιητικού του και την ισχύ αυτής της πρότασης στον φορέα μέσω των αντίστοιχων zkp πρωτοκόλλων, δίχως όμως ο τελευταίος να μάθει τον αριθμό των τέκνων. Παράλληλα εξασφαλίζεται η εμπιστευτικότητα των τιμών και των άλλων πεδίων, αφού αφενός η εκτέλεση των zkp πρωτοκόλλων δεν εμπλέκει καμιά από αυτές ώστε να υπήρχε η παραμικρή πιθανότητα μέσα από την χρήση τους να αποκαλυφθούν κάποιες από αυτές και αφετέρου το πιστοποιητικό δεν είναι προσβάσιμο στον φορέα.
Όπως αναφέρθηκε στην ενότητα 2, τα κριτήρια ελέγχου μπορεί να απαιτούν από κάποια πεδία να έχουν κάποιες δεδομένες τιμές. Τότε ο ισχυρισμός που ο νόμιμος κάτοχος του πιστοποιητικού καλείται να αποδείξει στον φορέα είναι ότι αυτά τα πεδία έχουν αυτές τις δεδομένες τιμές. Μετά την εκτέλεση των αντίστοιχων zkp πρωτοκόλλων, ο νόμιμος κάτοχος θα έχει πείσει τον φορέα για την εγκυρότητα του πιστοποιητικού του και το αληθές του ισχυρισμού και έτσι ο τελευταίος θα πληροφορηθεί τις τιμές αυτών των πεδίων. Οι συγκεκριμένες τιμές είναι πληροφορίες που σχετίζονται με τον ισχυρισμό και όπως αναφέρθηκε παραπάνω δεν πρέπει να αποκαλύπτονται άμεσα ή έμμεσα στον Verifier, που εν προκειμένω είναι ο φορέας. Εφόσον αποκαλύπτονται, το αντίστοιχο zkp πρωτόκολλο που χρησιμοποιείται σε αυτήν την περίπτωση χάνει το χαρακτηριστικό της μηδενικής γνώσης. Στο τελευταίο παράδειγμα της ενότητας 2 ο ισχυρισμός είναι ο εξής: '*το πεδίο του επιπέδου μόρφωσης έχει την τιμή 'Πανεπιστήμιο''*. Αυτή η τιμή είναι προσωπικό δεδομένο και σχετίζεται με τον συγκεκριμένο ισχυρισμό. Όταν το αληθές του τελευταίου αποδειχτεί από τον νόμιμο κάτοχο στον φορέα μέσω του αντίστοιχου zkp πρωτοκόλλου, τότε η τιμή '*Πανεπιστήμιο*' γίνεται γνωστή στον φορέα με αποτέλεσμα να παραβιαστεί η ιδιωτικότητά της σε αντίθεση με ό,τι συμβαίνει με την ιδιωτικότητα των τιμών των υπολοίπων πεδίων.

Στη συγκεκριμένη ενότητα αναλύονται τέσσερα zkp πρωτόκολλα που χρησιμοποιούνται σε ηλεκτρονικές συναλλαγές που έχουν με φορείς νόμιμοι κάτοχοι ψηφιακών πιστοποιητικών τα οποία είναι υπογεγραμμένα σύμφωνα με το σχήμα των

CL ψηφιακών υπογραφών. Ένα από αυτά παρουσιάζεται σε δύο διαφορετικές εκδόσεις, ενώ σε δύο παρατίθενται επεκτάσεις τους. Το πρώτο πρωτόκολλο που εξετάζεται χρησιμοποιείται από έναν κάτοχο όπως οι παραπάνω προκειμένου να αποδείξει στον φορέα πως έχει ένα έγκυρο πιστοποιητικό. Σε μια ηλεκτρονική συναλλαγή η πρώτη πληροφορία που πρέπει να ξέρει ένας φορέας είναι εάν το πιστοποιητικό της οντότητας που ξεκινάει μαζί του τη συναλλαγή είναι έγκυρο. Για αυτό και το συγκεκριμένο πρωτόκολλο εκτελείται χρονικά πάντα πρώτο πριν οποιοδήποτε άλλο από τα υπόλοιπα τρία. Το δεύτερο ανήκει στην κατηγορία των zkp πρωτοκόλλων που αποδεικνύουν πως κάποια από τα πεδία του πιστοποιητικού έχουν κάποιες δεδομένες τιμές. Τα τέσσερα αυτά πρωτόκολλα είναι σύνθετα γιατί κάνουν και χρήση τεσσάρων άλλων, τα τρία από τα οποία αναλύονται πρώτα στις τρεις πρώτες υποενότητες που ακολουθούν. Το πρωτόκολλο που δεν αναλύεται είναι αυτό της ισότητας διακριτών λογαρίθμων διαφορετικών modulo. Τα τέσσερα πρωτόκολλα των ηλεκτρονικών συναλλαγών αναλύονται στις μετέπειτα υποενότητες.

5.1. Zkp Πρωτόκολλο Γνώσης Διακριτών Λογαρίθμων

[5] Στην υποενότητα αυτή παρουσιάζεται και αναλύεται ένα zkp πρωτόκολλο το οποίο χρησιμοποιεί ο Prover για να πείσει τον Verifier ότι γνωρίζει $k \in \mathbb{N}^* - \{1\}$ διακριτούς λογαρίθμους $a_i \in \mathbb{Z}^*$ του $h \in \mathbb{N}^*$ ως προς τις k βάσεις $g_i \in QR_n^* - \{1\}$, όπου $i \in \{1,..,k\}$ και $n \in \mathbb{N}^*$. Δηλαδή ισχύει

$$h \equiv \left(\prod_{i=1}^{k} g_i^{a_i} \right) \bmod n \quad (72).$$

Συγκεκριμένα

$$n = p \cdot q,$$

όπου p, p', q, q' είναι περιττοί πρώτοι αριθμοί με $p \neq q$, $p' \neq q'$,

$$p = 2 \cdot p' + 1 \text{ και } q = 2 \cdot q' + 1.$$

Στην περίπτωση που υπάρχουν πλειάδες $(a_1,..,a_k) \in (\mathbb{Z}^*)^k$ οι οποίες ικανοποιούν την (72) και ο Prover ξέρει κάποια από αυτές, τότε χρησιμοποιεί το συγκεκριμένο πρωτόκολλο προκειμένου να πείσει τον Verifier για αυτήν τη γνώση του, ενώ παράλληλα η πλειάδα που γνωρίζει αποτελεί την πληροφορία που πρέπει κατά τη διάρκεια και μετά το τέλος της εκτέλεσης του πρωτοκόλλου να μην αποκαλυφθεί άμεσα ή έμμεσα στον Verifier. Το πρωτόκολλο αυτό είναι κατάλληλο για την απόδειξη γνώσης διακριτών λογαρίθμων στην περίπτωση που οι τέσσερις παραπάνω περιττοί πρώτοι αριθμοί καθώς και το γινόμενο $p' \cdot q'$ είναι άγνωστα στους Prover και Verifier. Αυτό συμβαίνει γιατί όπως φαίνεται παρακάτω σε κανένα βήμα αυτού του πρωτοκόλλου δεν απαιτείται η χρήση και άρα η γνώση των πέντε αυτών παραμέτρων από τους δύο συμμετέχοντες. Επομένως το συγκεκριμένο zkp πρωτόκολλο είναι κατάλληλο να χρησιμοποιηθεί στην περίπτωση όπου οι συγκεκριμένες παράμετροι είναι εκείνες τις οποίες δημιουργεί και υπολογίζει, κατά τη φάση δημιουργίας παραμέτρων, η Αρχή που εκδίδει και υπογράφει ψηφιακά πιστοποιητικά σύμφωνα με το σχήμα των CL ψηφιακών υπογραφών, καθώς όπως αναφέρθηκε στην υποενότητα 4.1 κρατάει μυστικές αυτές τις παραμέτρους. Συνεπώς το παρών πρωτόκολλο μπορεί να χρησιμοποιηθεί σε ηλεκτρονικές συναλλαγές που έχουν με φορείς νόμιμοι κάτοχοι πιστοποιητικών όπως τα παραπάνω. Το πρωτόκολλο και η απόδειξη ότι πετυχαίνει τον σκοπό του έχουν ως εξής:

- Prover
  - Στέλνει στον Verifier τα h,k,n και $g_i \ \ \forall i \in \{1,..,k\}$.
  - $\forall i \in \{1,..,k\}$ επιλέγει τυχαία $v_i \in \{1,..,n\}$.
  - Υπολογίζει $z = \left(\prod_{i=1}^{k} g_i^{v_i} \right) \bmod n$ (73).
  - Στέλνει στον Verifier το z.
- Verifier
  - Επιλέγει τυχαία $c \in \{1,..,n\}$.
  - Στέλνει στον Prover το c.
- Prover
  - $\forall i \in \{1,..,k\}$ υπολογίζει $r_i = v_i + c \cdot a_i$ (74).
  - $\forall i \in \{1,..,k\}$ στέλνει στον Verifier το r_i.
- Verifier
  - Ελέγχει αν $\left(z \cdot h^c \right) \equiv \left(\prod_{i=1}^{k} g_i^{r_i} \right) \bmod n$.
  - Αν ισχύει η ισοδυναμία, τότε ο Prover γνωρίζει κάποια $a_i \in \mathbb{Z}^*$, όπου $i \in \{1,..,k\}$, έτσι ώστε να ισχύει $h \equiv \left(\prod_{i=1}^{k} g_i^{a_i} \right) \bmod n$.

<u>Απόδειξη</u>

Στην αρχή ο Prover στέλνει στον Verifier τα h,k,n και $g_i \ \ \forall i \in \{1,..,k\}$, προκειμένου ο τελευταίος να τα πληροφορηθεί.

1. <u>Ο Prover γνωρίζει λογαρίθμους και το πρωτόκολλο τηρείται</u>

Σε αυτήν την περίπτωση υπάρχουν πλειάδες $(a_1,..,a_k) \in (\mathbb{Z}^*)^k$ που ικανοποιούν την (72) και ο Prover γνωρίζει κάποια από αυτές. Τότε από την (72) συνεπάγεται ότι:

$$h^c \equiv \left(g_1^{a_1} \cdot .. \cdot g_k^{a_k} \right)^c \bmod n = \left(\left(g_1^{a_1} \right)^c \cdot .. \cdot \left(g_k^{a_k} \right)^c \right) \bmod n \Rightarrow$$

$$h^c \equiv \left(\prod_{i=1}^{k} g_i^{a_i \cdot c} \right) \bmod n \xrightarrow{(73)} \left(z \cdot h^c \right) \equiv \left(\left(\prod_{i=1}^{k} g_i^{v_i} \right) \cdot \left(\prod_{i=1}^{k} g_i^{a_i \cdot c} \right) \right) \bmod n =$$

$$\left(\prod_{i=1}^{k} \left(g_i^{v_i} \cdot g_i^{a_i \cdot c} \right) \right) \bmod n = \left(\prod_{i=1}^{k} g_i^{v_i + a_i \cdot c} \right) \bmod n \xrightarrow{(74)} \left(z \cdot h^c \right) \equiv \left(\prod_{i=1}^{k} g_i^{r_i} \right) \bmod n .$$

Επομένως η ισοδυναμία που καλείται να ελέγξει ο Verifier ισχύει.

2. <u>Ο Prover δε γνωρίζει λογαρίθμους και το πρωτόκολλο τηρείται</u>

Σε αυτήν την περίπτωση ο Prover δε γνωρίζει κάποια πλειάδα διακριτών λογαρίθμων $(a_1,..,a_k) \in (\mathbb{Z}^*)^k$ που να ικανοποιούν την (72). Τότε σύμφωνα με το Δεύτερο Ισχυρισμό Διακριτού Λογαρίθμου είναι πάρα πολύ δύσκολο ή και αδύνατο να υπολογίσει τους άγνωστους λογαρίθμους. Εφόσον το πρωτόκολλο τηρηθεί και από τους δύο συμμετέχοντες, τότε για τον υπολογισμό των r_i, όπου $i \in \{1,..,k\}$, ο Prover

θα χρησιμοποιήσει τυχαίες τιμές αντί των λογαρίθμων που δε γνωρίζει. Έστω ότι $\forall i \in \{1,..,k\}$ $x_i \in \mathbb{Z}^*$ είναι η τιμή που επιλέγει τυχαία για τον υπολογισμό του r_i, δηλαδή

$$r_i = v_i + c \cdot x_i .$$

[8] Μετά την τυχαία επιλογή είναι πάρα πολύ δύσκολο ή και αδύνατο να ισχύει ότι

$$h \equiv \left(\prod_{i=1}^{k} g_i^{x_i} \right) \bmod n ,$$

λόγω του Δεύτερου Ισχυρισμού Διακριτού Λογαρίθμου. Επομένως σχεδόν κατά 100% θα είναι

$$h \bmod n \neq \left(\prod_{i=1}^{k} g_i^{x_i} \right) \bmod n .$$

Οι τυχαίες επιλογές των x_i από τον Prover και του c από τον Verifier μπορεί να είναι τέτοιες που να επιφέρουν την ισχύ της ισοδυναμίας

$$h^c \equiv \left(\prod_{i=1}^{k} g_i^{x_i} \right)^c \bmod n \ (75)^*.$$

Σε μια τέτοια περίπτωση θα συνεπάγεται από την (75) ότι

$$h^c \equiv \left(\prod_{i=1}^{k} \left(g_i^{x_i} \right)^c \right) \bmod n = \left(\prod_{i=1}^{k} g_i^{x_i \cdot c} \right) \bmod n \Rightarrow h^c \equiv \left(\prod_{i=1}^{k} \left(g_i^{c} \right)^{x_i} \right) \bmod n .$$

Δηλαδή οι Prover και Verifier επιλέγουν τυχαία τέτοια x_i και c αντίστοιχα, ώστε τα $x_1,..,x_k \in \mathbb{Z}^*$ να αποτελούν διακριτούς λογαρίθμους του h^c ως προς τις βάσεις $g_1^{\,c},..,g_k^{\,c}$. Αυτό το ενδεχόμενο είναι πάρα πολύ δύσκολο ή αδύνατο να συμβεί σύμφωνα με το Δεύτερο Ισχυρισμό Διακριτού Λογαρίθμου και επομένως η πιθανότητα να ισχύει η (75) είναι εξαιρετικά μικρή.

Θα δειχτεί ότι η ισοδυναμία που καλείται να ελέγξει ο Verifier δεν ισχύει σχεδόν κατά 100%. Έστω πως αυτή αληθεύει, δηλαδή

$$\left(z \cdot h^c \right) \equiv \left(\prod_{i=1}^{k} g_i^{r_i} \right) \bmod n \ (76).$$

Τίθεται

$$e = \left(\prod_{i=1}^{k} g_i^{x_i} \right) \bmod n \ (77).$$

$\forall i \in \{1,..,k\}$ είναι

$$r_i = v_i + c \cdot x_i \ (78),$$

ενώ από την (77) συνεπάγεται ότι

$$e^c \equiv \left(\prod_{i=1}^{k} g_i^{x_i} \right)^c \bmod n = \left(\prod_{i=1}^{k} \left(g_i^{x_i} \right)^c \right) \bmod n \Rightarrow e^c \equiv \left(\prod_{i=1}^{k} g_i^{x_i \cdot c} \right) \bmod n \xrightarrow{(73)}$$

$$\left(z \cdot e^c \right) \equiv \left(\left(\prod_{i=1}^{k} g_i^{x_i \cdot c} \right) \cdot \left(\prod_{i=1}^{k} g_i^{v_i} \right) \right) \bmod n = \left(\prod_{i=1}^{k} \left(g_i^{x_i \cdot c} \cdot g_i^{v_i} \right) \right) \bmod n =$$

---

*Για παράδειγμα $5 = 5 \bmod 13 \neq 8 \bmod 13 = 8$, αλλά $5^2 \equiv 8^2 \bmod 13 = 12$, αφού $25 \equiv 64 \bmod 13 = 12$.

$$\left(\prod_{i=1}^{k}\left(g_i^{x_i\cdot c+v_i}\right)\right)\bmod n \xrightarrow{(78)} \left(z\cdot e^c\right)\equiv\left(\prod_{i=1}^{k} g_i^{r_i}\right)\bmod n \xrightarrow{(76)}$$

$$\left(z\cdot h^c\right)\equiv\left(z\cdot e^c\right)\bmod n \Rightarrow \left(z\cdot h^c - z\cdot e^c\right)\equiv 0\bmod n \Rightarrow \left(z\cdot\left(h^c-e^c\right)\right)\equiv 0\bmod\left(p\cdot q\right).$$

Επειδή τα p,q είναι πρώτοι αριθμοί με $p\neq q$, τότε λόγω των Προτάσεων 6 και 4 η τελευταία ισοδυναμία συνεπάγεται ότι

$$\begin{cases}\left(z\cdot\left(h^c-e^c\right)\right)\equiv 0\bmod p\\ \left(z\cdot\left(h^c-e^c\right)\right)\equiv 0\bmod q\end{cases}\Rightarrow\begin{cases}z\equiv 0\bmod p\vee\left(h^c-e^c\right)\equiv 0\bmod p\\ z\equiv 0\bmod q\vee\left(h^c-e^c\right)\equiv 0\bmod q\end{cases}\quad(79).$$

Επειδή το n είναι γινόμενο δύο πρώτων αριθμών, των p,q, τότε θα ισχύει $n>2$. Επιπλέον $\forall i\in\{1,..,k\}\ \ g_i\in QR_n^*$, οπότε σύμφωνα με την Πρόταση 20.3 και τη σχέση

$$z=\left(\prod_{i=1}^{k} g_i^{v_i}\right)\bmod n,$$

θα ισχύει ότι $z\in QR_n^*$. Στην απόδειξη της Πρότασης 18.3 αποδείχτηκε πως $\forall c\in QR_n^*$

$$\left(c\bmod p\right)\in QR_p^*\ \text{ και }\ \left(c\bmod q\right)\in QR_q^*.$$

Έτσι και για το $z\in QR_n^*$ θα ισχύει

$$\left(z\bmod p\right)\in QR_p^*\ \text{ και }\ \left(z\bmod q\right)\in QR_q^*$$

και συνεπώς

$$\left(z\bmod p\right)\in\mathbb{Z}_p^*\ \text{ και }\ \left(z\bmod q\right)\in\mathbb{Z}_q^*.$$

Από την τελευταία σύζευξη συμπεραίνεται πως τα $z\bmod p, z\bmod q$ είναι πρώτα με τους πρώτους αριθμούς p,q αντίστοιχα. Επομένως σύμφωνα με την Πρόταση 1 τα $z\bmod p, z\bmod q$ δε διαιρούνται με τα p,q αντίστοιχα, δηλαδή

$$\begin{cases}\left(z\bmod p\right)\bmod p\neq 0\\ \left(z\bmod q\right)\bmod q\neq 0\end{cases}\Rightarrow\begin{cases}z\bmod p\neq 0\\ z\bmod q\neq 0\end{cases}.$$

Λόγω του τελευταίου συστήματος και της Πρότασης 6, η (79) συνεπάγεται ότι

$$\begin{cases}\left(h^c-e^c\right)\equiv 0\bmod p\\ \left(h^c-e^c\right)\equiv 0\bmod q\end{cases}\Rightarrow\left(h^c-e^c\right)\equiv 0\bmod\left(p\cdot q\right)\Rightarrow h^c\equiv e^c\bmod n\ \ (80).$$

Από την (77) συνεπάγεται ότι

$$e=\left(\prod_{i=1}^{k} g_i^{x_i}\right)\bmod n\Rightarrow e^c\equiv\left(\prod_{i=1}^{k} g_i^{x_i}\right)^c\bmod n\xrightarrow{(80)}h^c\equiv\left(\prod_{i=1}^{k} g_i^{x_i}\right)^c\bmod n\ \ (75).$$

Η πιθανότητα να ισχύει η (75) είναι εξαιρετικά μικρή όπως αποδείχτηκε προηγουμένως. Επίσης, επειδή η (75) προκύπτει ως συνεπαγωγή της υπόθεσης

$$\left(z\cdot h^c\right)\equiv\left(\prod_{i=1}^{k} g_i^{r_i}\right)\bmod n\ \ (76),$$

τότε η πιθανότητα να ισχύει η τελευταία ισοδυναμία είναι μικρότερη από την αντίστοιχη εξαιρετικά μικρή της (75).

<u>Ειδική περίπτωση</u>

Μία περίπτωση στην οποία η (76) ισχύει είναι όταν υπάρχουν πλειάδες $\left(a_1,..,a_k\right)\in\left(\mathbb{Z}^*\right)^k$ που ικανοποιούν την

$$h \equiv \left(\prod_{i=1}^{k} g_i^{a_i} \right) \bmod n \quad (72)$$

και το c τυχαία επιλέγεται από τον Verifier να είναι πολλαπλάσιο του $p' \cdot q'$. Αυτό αποδεικνύεται παρακάτω.

Έστω

$$h' = h \bmod n.$$

Τότε λόγω της (72) θα είναι

$$h' = \left(\prod_{i=1}^{k} g_i^{a_i} \right) \bmod n.$$

Επειδή $n > 2$ και $\forall i \in \{1,..,k\}$ $g_i \in QR_n^*$, τότε σύμφωνα με την τελευταία εξίσωση και την Πρόταση 20.3 θα ισχύει $h' \in QR_n^*$. Εφόσον το c, το οποίο επιλέγεται από το $\{1,..,n\}$, είναι πολλαπλάσιο του $p' \cdot q'$, τότε $\exists d \in \mathbb{Z}$ ώστε

$$c = p' \cdot q' \cdot d.$$

Επειδή $h' \in QR_n^*$, τότε σύμφωνα με την Πρόταση 18.6 θα είναι

$$h'^{p' \cdot q'} \equiv 1 \bmod n.$$

Εφόσον $h' = h \bmod n$, τότε θα ισχύει και λόγω της τελευταίας ισοδυναμίας ότι

$$h'^{p' \cdot q'} \equiv h^{p' \cdot q'} \bmod n \Rightarrow h^{p' \cdot q'} \equiv 1 \bmod n \Rightarrow \left(h^{p' \cdot q'} \right)^d \equiv 1^d \bmod n \Rightarrow h^{p' \cdot q' \cdot d} \equiv 1 \bmod n \Rightarrow$$

$$h^c \equiv 1 \bmod n \Rightarrow z \cdot h^c \equiv z \bmod n \ (81).$$

Επίσης αφού $\forall i \in \{1,..,k\}$ $g_i \in QR_n^*$, τότε θα ισχύει ότι

$$g_i^{p' \cdot q'} \equiv 1 \bmod n \Rightarrow \left(g_i^{p' \cdot q'} \right)^d \equiv 1^d \bmod n \Rightarrow g_i^{p' \cdot q' \cdot d} \equiv 1 \bmod n \Rightarrow g_i^c \equiv 1 \bmod n \Rightarrow$$

$$\left(g_i^c \right)^{a_i} \equiv 1^{a_i} \bmod n \Rightarrow g_i^{c \cdot a_i} \equiv 1 \bmod n \Rightarrow g_i^{v_i} \cdot g_i^{c \cdot a_i} \equiv g_i^{v_i} \bmod n \Rightarrow$$

$$g_i^{v_i + c \cdot a_i} \equiv g_i^{v_i} \bmod n \xrightarrow{(74)} g_i^{r_i} \equiv g_i^{v_i} \bmod n \Rightarrow \left(\prod_{i=1}^{k} g_i^{r_i} \right) \equiv \left(\prod_{i=1}^{k} g_i^{v_i} \right) \bmod n \xrightarrow{(73)}$$

$$\left(\prod_{i=1}^{k} g_i^{r_i} \right) \equiv z \bmod n \xrightarrow{(81)} z \cdot h^c \equiv \left(\prod_{i=1}^{k} g_i^{r_i} \right) \bmod n \ (76).$$

Επομένως στη συγκεκριμένη ειδική περίπτωση η (76) ισχύει. Επίσης

$$n = p \cdot q = (2 \cdot p' + 1) \cdot (2 \cdot q' + 1) \Rightarrow n = 4 \cdot p' \cdot q' + 2 \cdot p' + 2 \cdot q' + 1 \ (82).$$

Επειδή τα p', q' είναι περιττοί πρώτοι αριθμοί, θα ισχύει

$$\begin{cases} p' \geq 3 \\ q' \geq 3 \end{cases} \Rightarrow \begin{cases} \frac{1}{p'} \leq \frac{1}{3} \\ \frac{1}{q'} \leq \frac{1}{3} \\ p' \cdot q' \geq 9 \end{cases} \Rightarrow \begin{cases} \frac{2}{p'} \leq \frac{2}{3} \\ \frac{2}{q'} \leq \frac{2}{3} \\ \frac{1}{p' \cdot q'} \leq \frac{1}{9} \end{cases} \Rightarrow \frac{2}{p'} + \frac{2}{q'} + \frac{1}{p' \cdot q'} \leq \frac{2}{3} + \frac{2}{3} + \frac{1}{9} = \frac{13}{9} < \frac{18}{9} = 2 \Rightarrow$$

$$\frac{2 \cdot p' + 2 \cdot q' + 1}{p' \cdot q'} < 2 \Rightarrow 2 \cdot p' + 2 \cdot q' + 1 < 2 \cdot p' \cdot q' \Rightarrow$$

$$4 \cdot p' \cdot q' + 2 \cdot p' + 2 \cdot q' + 1 < 4 \cdot p' \cdot q' + 2 \cdot p' \cdot q' \xrightarrow{(82)} n < 6 \cdot p' \cdot q'.$$

Από την τελευταία ανισότητα προκύπτει πως το πλήθος των πολλαπλασίων του $p' \cdot q'$ στο σύνολο $\{1,..,n\}$ είναι μικρότερο από 6. Εφόσον επομένως το c επιλέγεται

από το $\{1,..,n\}$ και είναι πολλαπλάσιο του $p' \cdot q'$, θα μπορεί να λάβει το πολύ 5 διαφορετικές τιμές. Έτσι με δεδομένο ότι n είναι οι δυνατές τιμές που μπορεί να λάβει το c από το $\{1,..,n\}$, τότε η πιθανότητα αυτό να είναι πολλαπλάσιο του $p' \cdot q'$ είναι το πολύ ίση με $\frac{5}{n}$. Όπως αναφέρθηκε στην υποενότητα 4.1, το διάστημα $\left[2^{1023}, 2^{1024}\right)$ περιέχει ενδεικτικές τιμές για το n, οπότε αν $n \in \left[2^{1023}, 2^{1024}\right)$ θα ισχύει ότι

$$2^{1023} \le n \Rightarrow \frac{1}{n} \le \frac{1}{2^{1023}} \Rightarrow \frac{5}{n} \le \frac{5}{2^{1023}} < \frac{5}{2^{1000}} = \frac{5}{\left(2^{10}\right)^{100}} = \frac{5}{1024^{100}} < \frac{5}{1000^{100}} = \frac{5}{\left(10^3\right)^{100}} =$$

$$\frac{5}{10^{300}} = \frac{5}{10^{300}} \cdot 100\% \Rightarrow \frac{5}{n} < \frac{5}{10^{298}}\% .$$

Δηλαδή είναι εξαιρετικά πολύ μικρή η πιθανότητα να επιλέξει ο Verifier τυχαία το c από το $\{1,..,n\}$ και αυτό να είναι πολλαπλάσιο του $p' \cdot q'$. Αυτό το συμπέρασμα σε συνδυασμό με το ότι θα πρέπει ταυτόχρονα να υπάρχουν και πλειάδες $(a_1,..,a_k) \in \left(\mathbb{Z}^*\right)^k$ που να ικανοποιούν την (72) ώστε να ισχύσει η ισοδυναμία

$$\left(z \cdot h^c\right) \equiv \left(\prod_{i=1}^{k} g_i^{r_i}\right) \bmod n ,$$

καθιστά πάρα πολύ δύσκολη την ύπαρξη της συγκεκριμένης ειδικής περίπτωσης.
Ξέχωρα από αυτήν, όπως προαναφέρθηκε η πιθανότητα να ισχύει η ισοδυναμία

$$\left(z \cdot h^c\right) \equiv \left(\prod_{i=1}^{k} g_i^{r_i}\right) \bmod n$$

που καλείται να ελέγξει ο Verifier, είναι μικρότερη από την αντίστοιχη εξαιρετικά μικρή της (75). Έτσι στην περίπτωση που Prover δε γνωρίζει κάποια πλειάδα διακριτών λογαρίθμων $(a_1,..,a_k) \in \left(\mathbb{Z}^*\right)^k$ που να ικανοποιούν την (72) και το πρωτόκολλο τηρηθεί, η ισοδυναμία που καλείται να ελέγξει ο Verifier δε θα ισχύει σχεδόν κατά 100%.

3. <u>Ο Prover δε γνωρίζει λογαρίθμους και επιλέγει να μην τηρήσει το πρωτόκολλο</u>

[8] Σε αυτήν την περίπτωση ο Prover δε γνωρίζει κάποια πλειάδα διακριτών λογαρίθμων $(a_1,..,a_k) \in \left(\mathbb{Z}^*\right)^k$ που να ικανοποιούν την (72) και ενεργεί έτσι προκειμένου να ξεγελάσει τον Verifier ώστε να τον πείσει για τον ψευδή ισχυρισμό του. Το ζητούμενο για τον Prover είναι να καταφέρει να ισχύσει η ισοδυναμία που ελέγχει ο Verifier ώστε ο τελευταίος να πειστεί.
Μία δυνατότητα που έχει είναι να υπολογίσει κανονικά σύμφωνα με το πρωτόκολλο το z ή να το επιλέξει τυχαία, να το στείλει στον Verifier και αφού λάβει το c να προσπαθήσει να επιλύσει ως προς r_i, όπου $i \in \{1,..,k\}$, την ισοδυναμία

$$\left(z \cdot h^c\right) \equiv \left(\prod_{i=1}^{k} g_i^{r_i}\right) \bmod n ,$$

ώστε αυτή μετά και την αποστολή των λύσεων r_i να επαληθευτεί από τον Verifier. Όμως σύμφωνα με το Δεύτερο Ισχυρισμό Διακριτού Λογαρίθμου είναι πάρα πολύ δύσκολο ή και αδύνατο να βρει r_i που ικανοποιούν την προηγούμενη ισοδυναμία, αφού αυτά αποτελούν k διακριτούς λογαρίθμους του $z \cdot h^c$ ως προς τις βάσεις g_i.

Εδώ να επισημανθεί το γεγονός πως αν δεν υπάρχουν k διακριτοί λογάριθμοι r_i που να ικανοποιούν αυτήν την ισοδυναμία, τότε δεν υπάρχουν και k διακριτοί λογάριθμοι a_i που να ικανοποιούν την ισοδυναμία

$$h \equiv \left(\prod_{i=1}^{k} g_i^{a_i} \right) \bmod n .$$

Εφόσον στην περίπτωση 1 της παρούσας απόδειξης δείχτηκε πως η ύπαρξη των λογαρίθμων a_i συνεπάγεται την ισχύ της ισοδυναμίας

$$\left(z \cdot h^c \right) \equiv \left(\prod_{i=1}^{k} g_i^{r_i} \right) \bmod n$$

και άρα την ύπαρξη των λογαρίθμων r_i, τότε εφαρμόζοντας σε αυτήν την συνεπαγωγή τον κανόνα της αντιθετοαντιστροφής λαμβάνεται η προηγούμενη επισήμανση.

[8] Από την άλλη, αν εξαρχής ο Prover επέλεγε τυχαία τα r_i, δε θα μπορούσε να υπολογίσει από την ισοδυναμία που ελέγχει ο Verifier το z και να το στείλει ώστε αυτή μετά να επαληθευτεί, εφόσον δε θα ήξερε ακόμα το c, αφού αυτό το λαμβάνει μετά τον υπολογισμό και την αποστολή του z.

Επομένως στην περίπτωση που ο Prover δε γνωρίζει κάποια πλειάδα διακριτών λογαρίθμων $(a_1,..,a_k) \in \left(\mathbb{Z}^*\right)^k$ που να ικανοποιούν την (72) και επιλέξει να μην τηρήσει το πρωτόκολλο, τότε η ισοδυναμία που καλείται να ελέγξει ο Verifier δε θα ισχύει σχεδόν κατά 100%.

Συνεπώς από την παρούσα απόδειξη προκύπτει πως μόνο όταν υπάρχουν πλειάδες $(a_1,..,a_k) \in \left(\mathbb{Z}^*\right)^k$ που ικανοποιούν την (72), ο Prover γνωρίζει κάποια από αυτές και το πρωτόκολλο τηρηθεί, η ισοδυναμία

$$\left(z \cdot h^c \right) \equiv \left(\prod_{i=1}^{k} g_i^{r_i} \right) \bmod n$$

που καλείται να ελέγξει ο Verifier θα ισχύει σίγουρα. Διαφορετικά η πιθανότητα να ισχύει είναι εξαιρετικά μικρή. Αυτό σημαίνει πως η ισχύς της αποτελεί σχεδόν κατά 100% απόδειξη ότι ο Prover γνωρίζει k διακριτούς λογαρίθμους του h ως προς τις k βάσεις $g_1,..,g_k$.

4. <u>Εμπιστευτικότητα πληροφορίας</u>

Στην περίπτωση που ξέρει k τέτοιους λογαρίθμους, αυτοί αποτελούν πληροφορία που δε θα αποκαλυφθεί άμεσα ή έμμεσα στον Verifier. Αυτό συμβαίνει γιατί για όσο εκτελείται το πρωτόκολλο ο Verifier δεν τους μαθαίνει άμεσα από τον Prover και από την άλλη του είναι σχεδόν αδύνατο να τους πληροφορηθεί έμμεσα προσπαθώντας να τους υπολογίσει. Πράγματι, λόγω του Δεύτερου Ισχυρισμού Διακριτού Λογαρίθμου είναι πάρα πολύ δύσκολο να τους βρει από την (72) ενώ από την άλλη, μετά την λήψη των r_i όπου $i \in \{1,..,k\}$, δεν μπορεί να τους πληροφορηθεί επιλύοντας τις k εξισώσεις

$$r_i = v_i + c \cdot a_i$$

ως προς a_i. Ο λόγος είναι ότι θα πρέπει πρώτα να υπολογίσει τους διακριτούς λογαρίθμους v_i του z ως προς τις βάσεις g_i από την εξίσωση

$$z = \left(\prod_{i=1}^{k} g_i^{v_i} \right) \bmod n,$$

κάτι που είναι πάρα πολύ δύσκολο σύμφωνα με το Δεύτερο Ισχυρισμό Διακριτού Λογαρίθμου.

5.2. Zkp Πρωτόκολλο Γνώσης Διακριτών Λογαρίθμων modulo Πρώτο Αριθμό

[8] Στην υποενότητα αυτή παρουσιάζεται και αναλύεται ένα zkp πρωτόκολλο το οποίο χρησιμοποιεί ο Prover για να πείσει τον Verifier ότι γνωρίζει $k \in \mathbb{N}^* - \{1\}$ διακριτούς λογαρίθμους $a_i \in \mathbb{Z}^*$ modulo P του $h \in \mathbb{N}^*$ ως προς τις k βάσεις $g_i \in QR_P^* - \{1\}$, όπου $i \in \{1,..,k\}$ και P είναι περιττός πρώτος αριθμός. Δηλαδή ισχύει

$$h \equiv \left(\prod_{i=1}^{k} g_i^{a_i} \right) \bmod P \quad (83).$$

Συγκεκριμένα

$$P = 2 \cdot P' + 1,$$

όπου P' είναι επίσης περιττός πρώτος αριθμός. Στην περίπτωση που υπάρχουν πλειάδες $(a_1,..,a_k) \in (\mathbb{Z}^*)^k$ οι οποίες ικανοποιούν την (83) και ο Prover ξέρει κάποια από αυτές, τότε χρησιμοποιεί το συγκεκριμένο πρωτόκολλο προκειμένου να πείσει τον Verifier για αυτήν τη γνώση του, ενώ παράλληλα η πλειάδα που γνωρίζει αποτελεί την πληροφορία που πρέπει κατά τη διάρκεια και μετά το τέλος της εκτέλεσης του πρωτοκόλλου να μην αποκαλυφθεί άμεσα ή έμμεσα στον Verifier. Το πρωτόκολλο και η απόδειξη ότι πετυχαίνει τον σκοπό του έχουν ως εξής:

- Prover
  - Στέλνει στον Verifier τα h, k, P, P' και $g_i \ \ \forall i \in \{1,..,k\}$.
  - $\forall i \in \{1,..,k\}$ επιλέγει τυχαία $v_i \in \{1,..,P'-1\}$.
  - Υπολογίζει $z = \left(\prod_{i=1}^{k} g_i^{v_i} \right) \bmod P$ (84).
  - Στέλνει στον Verifier το z.
- Verifier
  - Επιλέγει τυχαία $c \in \{1,..,P'-1\}$.
  - Στέλνει στον Prover το c.
- Prover
  - $\forall i \in \{1,..,k\}$ υπολογίζει $r_i = (v_i + c \cdot a_i) \bmod P'$ (85).
  - $\forall i \in \{1,..,k\}$ στέλνει στον Verifier το r_i.
- Verifier
  - Ελέγχει αν $(z \cdot h^c) \equiv \left(\prod_{i=1}^{k} g_i^{r_i} \right) \bmod P$.

- Αν ισχύει η ισοδυναμία, τότε ο Prover γνωρίζει κάποια $a_i \in \mathbb{Z}^*$, όπου $i \in \{1,..,k\}$, έτσι ώστε να ισχύει $h \equiv \left(\prod_{i=1}^{k} g_i^{a_i} \right) \bmod P$.

<u>Απόδειξη</u>

Στην αρχή ο Prover στέλνει στον Verifier τα h, k, P, P' και $g_i \quad \forall i \in \{1,..,k\}$, προκειμένου ο τελευταίος να τα πληροφορηθεί.

1. <u>Ο Prover γνωρίζει λογαρίθμους και το πρωτόκολλο τηρείται</u>

Σε αυτήν την περίπτωση υπάρχουν πλειάδες $(a_1,..,a_k) \in (\mathbb{Z}^*)^k$ που ικανοποιούν την (83) και ο Prover γνωρίζει κάποια από αυτές. Τότε από την (83) συνεπάγεται ότι:

$$h^c \equiv \left(g_1^{a_1} \cdot ... \cdot g_k^{a_k} \right)^c \bmod P = \left(\left(g_1^{a_1} \right)^c \cdot ... \cdot \left(g_k^{a_k} \right)^c \right) \bmod P \Rightarrow$$

$$h^c \equiv \left(\prod_{i=1}^{k} g_i^{a_i \cdot c} \right) \bmod P \xrightarrow{(84)} \left(z \cdot h^c \right) \equiv \left(\left(\prod_{i=1}^{k} g_i^{v_i} \right) \cdot \left(\prod_{i=1}^{k} g_i^{a_i \cdot c} \right) \right) \bmod P =$$

$$\left(\prod_{i=1}^{k} \left(g_i^{v_i} \cdot g_i^{a_i \cdot c} \right) \right) \bmod P \Rightarrow \left(z \cdot h^c \right) \equiv \left(\prod_{i=1}^{k} g_i^{v_i + a_i \cdot c} \right) \bmod P \quad (86).$$

Λόγω της (85), $\forall i \in \{1,..,k\} \quad \exists d_i \in \mathbb{Z}$ ώστε να ισχύει

$$v_i + c \cdot a_i = P' \cdot d_i + r_i$$

και άρα η (86) συνεπάγεται ότι

$$\left(z \cdot h^c \right) \equiv \left(\prod_{i=1}^{k} g_i^{P' \cdot d_i + r_i} \right) \bmod P \quad (87).$$

Επειδή τα P, P' είναι περιττοί πρώτοι αριθμοί με $P = 2 \cdot P' + 1$ και $\forall i \in \{1,..,k\}$ $g_i \in QR_P^* - \{1\}$, δηλαδή $g_i \in QR_P^*$ με $g_i \neq 1$, τότε σύμφωνα με την Πρόταση 16 η τάξη του g_i ως προς P είναι ίση με P'. Επομένως $\forall i \in \{1,..,k\}$ θα ισχύει

$$g_i^{P'} \equiv 1 \bmod P.$$

Από αυτήν την ισοδυναμία συνεπάγεται ότι

$$\left(g_i^{P'} \right)^{d_i} \equiv 1^{d_i} \bmod P \Rightarrow g_i^{P' \cdot d_i} \equiv 1 \bmod P \Rightarrow \left(g_i^{P' \cdot d_i} \cdot g_i^{r_i} \right) \equiv g_i^{r_i} \bmod P \Rightarrow$$

$$g_i^{P' \cdot d_i + r_i} \equiv g_i^{r_i} \bmod P \Rightarrow \left(\prod_{i=1}^{k} g_i^{P' \cdot d_i + r_i} \right) \equiv \left(\prod_{i=1}^{k} g_i^{r_i} \right) \bmod P \xrightarrow{(87)}$$

$$\left(z \cdot h^c \right) \equiv \left(\prod_{i=1}^{k} g_i^{r_i} \right) \bmod P.$$

Επομένως η ισοδυναμία που καλείται να ελέγξει ο Verifier ισχύει.

2. <u>Ο Prover δε γνωρίζει λογαρίθμους και το πρωτόκολλο τηρείται</u>

Σε αυτήν την περίπτωση ο Prover δε γνωρίζει κάποια πλειάδα διακριτών λογαρίθμων $(a_1,..,a_k) \in (\mathbb{Z}^*)^k$ που να ικανοποιούν την (83). Τότε σύμφωνα με το Δεύτερο Ισχυρισμό Διακριτού Λογαρίθμου είναι πάρα πολύ δύσκολο ή και αδύνατο να υπολογίσει τους άγνωστους λογαρίθμους. Εφόσον το πρωτόκολλο τηρείται και από τους δύο συμμετέχοντες, τότε για τον υπολογισμό των r_i, όπου $i \in \{1,..,k\}$, ο Prover θα χρησιμοποιήσει τυχαίες τιμές αντί των λογαρίθμων που δε γνωρίζει. Έστω ότι

$\forall i \in \{1,..,k\}$ $x_i \in \mathbb{Z}^*$ είναι η τιμή που επιλέγει τυχαία για τον υπολογισμό του r_i, δηλαδή

$$r_i = (v_i + c \cdot x_i) \bmod P'.$$

[8] Μετά την τυχαία επιλογή είναι πάρα πολύ δύσκολο ή και αδύνατο να ισχύει ότι

$$h \equiv \left(\prod_{i=1}^{k} g_i^{x_i} \right) \bmod P,$$

λόγω του Δεύτερου Ισχυρισμού Διακριτού Λογαρίθμου. Επομένως σχεδόν κατά 100% θα είναι

$$h \bmod P \neq \left(\prod_{i=1}^{k} g_i^{x_i} \right) \bmod P.$$

Οι τυχαίες επιλογές των x_i από τον Prover και του c από τον Verifier μπορεί να είναι τέτοιες που να επιφέρουν την ισχύ της ισοδυναμίας

$$h^c \equiv \left(\prod_{i=1}^{k} g_i^{x_i} \right)^c \bmod P \quad (88)^{**}.$$

Σε μια τέτοια περίπτωση θα συνεπάγεται από την (88) ότι

$$h^c \equiv \left(\prod_{i=1}^{k} \left(g_i^{x_i} \right)^c \right) \bmod P = \left(\prod_{i=1}^{k} g_i^{x_i \cdot c} \right) \bmod P \Rightarrow h^c \equiv \left(\prod_{i=1}^{k} \left(g_i^{c} \right)^{x_i} \right) \bmod P.$$

Δηλαδή οι Prover και Verifier επιλέγουν τυχαία τέτοια x_i και c αντίστοιχα, ώστε τα $x_1,..,x_k \in \mathbb{Z}^*$ να αποτελούν διακριτούς λογαρίθμους του h^c ως προς τις βάσεις $g_1^{\,c},..,g_k^{\,c}$. Αυτό το ενδεχόμενο είναι πάρα πολύ δύσκολο ή αδύνατο να συμβεί σύμφωνα με το Δεύτερο Ισχυρισμό Διακριτού Λογαρίθμου και επομένως η πιθανότητα να ισχύει η (88) είναι εξαιρετικά μικρή.

Θα δειχτεί ότι η ισοδυναμία που καλείται να ελέγξει ο Verifier δεν ισχύει σχεδόν κατά 100%. Έστω πως αυτή αληθεύει, δηλαδή

$$\left(z \cdot h^c \right) \equiv \left(\prod_{i=1}^{k} g_i^{r_i} \right) \bmod P \quad (89).$$

Τίθεται

$$e = \left(\prod_{i=1}^{k} g_i^{x_i} \right) \bmod P \quad (90).$$

$\forall i \in \{1,..,k\}$ είναι

$$r_i = (v_i + c \cdot x_i) \bmod P' \quad (91),$$

ενώ από την (90) συνεπάγεται ότι

$$e^c \equiv \left(\prod_{i=1}^{k} g_i^{x_i} \right)^c \bmod P = \left(\prod_{i=1}^{k} \left(g_i^{x_i} \right)^c \right) \bmod P \Rightarrow e^c \equiv \left(\prod_{i=1}^{k} g_i^{x_i \cdot c} \right) \bmod P \xrightarrow{(84)}$$

$$\left(z \cdot e^c \right) \equiv \left(\left(\prod_{i=1}^{k} g_i^{x_i \cdot c} \right) \cdot \left(\prod_{i=1}^{k} g_i^{v_i} \right) \right) \bmod P = \left(\prod_{i=1}^{k} \left(g_i^{x_i \cdot c} \cdot g_i^{v_i} \right) \right) \bmod P \Rightarrow$$

$$\left(z \cdot e^c \right) \equiv \left(\prod_{i=1}^{k} \left(g_i^{x_i \cdot c + v_i} \right) \right) \bmod P \quad (92).$$

**Αντίστοιχο παράδειγμα έχει αναφερθεί στην απόδειξη της υποενότητας 5.1.

Λόγω της (91), $\forall i \in \{1,..,k\}\ \ \exists d_i' \in \mathbb{Z}$ ώστε να ισχύει

$$v_i + c \cdot x_i = P' \cdot d_i' + r_i$$

και άρα η (92) συνεπάγεται ότι

$$\left(z \cdot e^c\right) \equiv \left(\prod_{i=1}^{k} \left(g_i^{P' \cdot d_i' + r_i}\right)\right) \bmod P \ \ (93).$$

Ισχύει ότι

$$g_i^{P'} \equiv 1 \bmod P \Rightarrow \left(g_i^{P'}\right)^{d_i'} \equiv 1^{d_i'} \bmod P \Rightarrow g_i^{P' \cdot d_i'} \equiv 1 \bmod P \Rightarrow \left(g_i^{P' \cdot d_i'} \cdot g_i^{r_i}\right) \equiv g_i^{r_i} \bmod P \Rightarrow$$

$$g_i^{P' \cdot d_i' + r_i} \equiv g_i^{r_i} \bmod P \Rightarrow \left(\prod_{i=1}^{k} g_i^{P' \cdot d_i' + r_i}\right) \equiv \left(\prod_{i=1}^{k} g_i^{r_i}\right) \bmod P \xrightarrow{(93)}$$

$$\left(z \cdot e^c\right) \equiv \left(\prod_{i=1}^{k} g_i^{r_i}\right) \bmod P \xrightarrow{(89)} \left(z \cdot h^c\right) \equiv \left(z \cdot e^c\right) \bmod P \Rightarrow$$

$$\left(z \cdot h^c - z \cdot e^c\right) \equiv 0 \bmod P \Rightarrow \left(z \cdot \left(h^c - e^c\right)\right) \equiv 0 \bmod P .$$

Επειδή το P είναι πρώτος αριθμός, τότε λόγω της Πρότασης 4 η τελευταία ισοδυναμία συνεπάγεται ότι

$$z \equiv 0 \bmod P \vee \left(h^c - e^c\right) \equiv 0 \bmod P \ \ (94).$$

Επειδή $\forall i \in \{1,..,k\}\ \ g_i \in QR_P^*$, τότε $g_i \in \mathbb{Z}_P^*$ και άρα το P θα είναι πρώτος με το g_i. Επομένως λόγω των Προτάσεων 5.2 και 5.1, το P θα είναι πρώτος με το $\prod_{i=1}^{k} g_i^{v_i}$ και έτσι εξαιτίας της Πρότασης 11 και της ισοδυναμίας

$$z \equiv \left(\prod_{i=1}^{k} g_i^{v_i}\right) \bmod P$$

που προκύπτει από την (84), το P θα είναι επίσης πρώτος με το z. Αυτό σημαίνει πως εφόσον το P είναι πρώτος αριθμός, λόγω της Πρότασης 1 δε θα διαιρεί το z, δηλαδή

$$z \bmod P \neq 0 .$$

Έτσι η (94) συνεπάγεται

$$\left(h^c - e^c\right) \equiv 0 \bmod P \Rightarrow h^c \equiv e^c \bmod P \ \ (95).$$

Από την (90) συνεπάγεται ότι

$$e = \left(\prod_{i=1}^{k} g_i^{x_i}\right) \bmod P \Rightarrow e^c \equiv \left(\prod_{i=1}^{k} g_i^{x_i}\right)^c \bmod P \xrightarrow{(95)} h^c \equiv \left(\prod_{i=1}^{k} g_i^{x_i}\right)^c \bmod P \ \ (88).$$

Η πιθανότητα να ισχύει η (88) είναι εξαιρετικά μικρή όπως αποδείχτηκε προηγουμένως. Επίσης, επειδή η (88) προκύπτει ως συνεπαγωγή της υπόθεσης

$$\left(z \cdot h^c\right) \equiv \left(\prod_{i=1}^{k} g_i^{r_i}\right) \bmod P \ \ (89),$$

τότε η πιθανότητα να ισχύει η τελευταία ισοδυναμία είναι μικρότερη από την αντίστοιχη εξαιρετικά μικρή της (88).

Άρα στην περίπτωση που Prover δε γνωρίζει κάποια πλειάδα διακριτών λογαρίθμων $\left(a_1,..,a_k\right) \in \left(\mathbb{Z}^*\right)^k$ που να ικανοποιούν την (83) και το πρωτόκολλο τηρηθεί, η ισοδυναμία που καλείται να ελέγξει ο Verifier δε θα ισχύει σχεδόν κατά 100% .

3. <u>Ο Prover δε γνωρίζει λογαρίθμους και επιλέγει να μην τηρήσει το πρωτόκολλο</u>

[8] Σε αυτήν την περίπτωση ο Prover δε γνωρίζει κάποια πλειάδα διακριτών λογαρίθμων $(a_1,..,a_k)\in(\mathbb{Z}^*)^k$ που να ικανοποιούν την (83) και ενεργεί έτσι προκειμένου να ξεγελάσει τον Verifier ώστε να τον πείσει για τον ψευδή ισχυρισμό του. Το ζητούμενο για τον Prover είναι να καταφέρει να ισχύσει η ισοδυναμία που ελέγχει ο Verifier ώστε ο τελευταίος να πειστεί.

Μία δυνατότητα που έχει είναι να υπολογίσει κανονικά σύμφωνα με το πρωτόκολλο το z ή να το επιλέξει τυχαία, να το στείλει στον Verifier και αφού λάβει το c να προσπαθήσει να επιλύσει ως προς r_i, όπου $i\in\{1,..,k\}$, την ισοδυναμία

$$\left(z\cdot h^c\right)\equiv\left(\prod_{i=1}^{k}g_i^{r_i}\right)\bmod P,$$

ώστε αυτή μετά και την αποστολή των λύσεων r_i να επαληθευτεί από τον Verifier. Όμως σύμφωνα με το Δεύτερο Ισχυρισμό Διακριτού Λογαρίθμου είναι πάρα πολύ δύσκολο ή και αδύνατο να βρει r_i που ικανοποιούν την προηγούμενη ισοδυναμία, αφού αυτά αποτελούν k διακριτούς λογαρίθμους του $z\cdot h^c$ ως προς τις βάσεις g_i. Εδώ να επισημανθεί το γεγονός πως αν δεν υπάρχουν k διακριτοί λογάριθμοι r_i που να ικανοποιούν αυτήν την ισοδυναμία, τότε δεν υπάρχουν και k διακριτοί λογάριθμοι a_i που να ικανοποιούν την ισοδυναμία

$$h\equiv\left(\prod_{i=1}^{k}g_i^{a_i}\right)\bmod P.$$

Εφόσον στην περίπτωση 1 της παρούσας απόδειξης δείχτηκε πως η ύπαρξη των λογαρίθμων a_i συνεπάγεται την ισχύ της ισοδυναμίας

$$\left(z\cdot h^c\right)\equiv\left(\prod_{i=1}^{k}g_i^{r_i}\right)\bmod P$$

και άρα την ύπαρξη των λογαρίθμων r_i, τότε εφαρμόζοντας σε αυτήν την συνεπαγωγή τον κανόνα της αντιθετοαντιστροφής λαμβάνεται η προηγούμενη επισήμανση.

[8] Από την άλλη, αν εξαρχής ο Prover επέλεγε τυχαία τα r_i, δε θα μπορούσε να υπολογίσει από την ισοδυναμία που ελέγχει ο Verifier το z και να το στείλει ώστε αυτή μετά να επαληθευτεί, εφόσον δε θα ήξερε ακόμα το c, αφού αυτό το λαμβάνει μετά τον υπολογισμό και την αποστολή του z.

Επομένως στην περίπτωση που ο Prover δε γνωρίζει κάποια πλειάδα διακριτών λογαρίθμων $(a_1,..,a_k)\in(\mathbb{Z}^*)^k$ που να ικανοποιούν την (83) και επιλέξει να μην τηρήσει το πρωτόκολλο, τότε η ισοδυναμία που καλείται να ελέγξει ο Verifier δε θα ισχύει σχεδόν κατά 100%.

Συνεπώς από την παρούσα απόδειξη προκύπτει πως μόνο όταν υπάρχουν πλειάδες $(a_1,..,a_k)\in(\mathbb{Z}^*)^k$ που ικανοποιούν την (83), ο Prover γνωρίζει κάποια από αυτές και το πρωτόκολλο τηρηθεί, η ισοδυναμία

$$\left(z\cdot h^c\right)\equiv\left(\prod_{i=1}^{k}g_i^{r_i}\right)\bmod P$$

που καλείται να ελέγξει ο Verifier θα ισχύει σίγουρα. Διαφορετικά η πιθανότητα να ισχύει είναι εξαιρετικά μικρή. Αυτό σημαίνει πως η ισχύς της αποτελεί σχεδόν κατά

100% απόδειξη ότι ο Prover γνωρίζει k διακριτούς λογαρίθμους modulo P του h ως προς τις k βάσεις $g_1,..,g_k$.

4. <u>Εμπιστευτικότητα πληροφορίας</u>

Στην περίπτωση που ξέρει k τέτοιους λογαρίθμους, αυτοί αποτελούν πληροφορία που δε θα αποκαλυφθεί άμεσα ή έμμεσα στον Verifier. Αυτό συμβαίνει γιατί για όσο εκτελείται το πρωτόκολλο ο Verifier δεν τους μαθαίνει άμεσα από τον Prover και από την άλλη του είναι σχεδόν αδύνατο να τους πληροφορηθεί έμμεσα προσπαθώντας να τους υπολογίσει. Πράγματι, λόγω του Δεύτερου Ισχυρισμού Διακριτού Λογαρίθμου είναι πάρα πολύ δύσκολο να τους βρει από την (83) ενώ από την άλλη, μετά την λήψη των r_i όπου $i \in \{1,..,k\}$, δεν μπορεί να τους πληροφορηθεί επιλύοντας τις k εξισώσεις

$$r_i = (v_i + c \cdot a_i) \bmod P'$$

ως προς a_i. Ο λόγος είναι ότι θα πρέπει πρώτα να υπολογίσει τους διακριτούς λογαρίθμους v_i του z ως προς τις βάσεις g_i από την εξίσωση

$$z = \left(\prod_{i=1}^{k} g_i^{v_i} \right) \bmod P,$$

κάτι που είναι πάρα πολύ δύσκολο σύμφωνα με το Δεύτερο Ισχυρισμό Διακριτού Λογαρίθμου.

5.3. Zkp Πρωτόκολλο Ισότητας Διακριτών Λογαρίθμων

Στην υποενότητα αυτή παρουσιάζεται και αναλύεται ένα zkp πρωτόκολλο το οποίο χρησιμοποιεί ο Prover για να πείσει τον Verifier ότι όταν τα $a,b \in \mathbb{N}^*$ αναπαρίστανται αντίστοιχα στις $m \in \mathbb{N}^* - \{1\}$ βάσεις $g_i \in QR_n^* - \{1\}$, όπου $i \in \{1,..,m\}$ και $l \in \mathbb{N}^* - \{1\}$ βάσεις $h_j \in QR_n^* - \{1\}$, όπου $j \in \{1,..,l\}$, υπάρχουν $k \in \mathbb{N}^*$ διακριτοί λογάριθμοι του a ως προς τα g_s, όπου $s \in \{1,..,k\}$, και k του b ως προς τα h_s που είναι ίσοι μεταξύ τους. Δηλαδή ισχύει

$$\begin{cases} a \equiv \left(g_1^{r_1} \cdot ... \cdot g_k^{r_k} \cdot g_{k+1}^{r_{k+1}} \cdot ... \cdot g_m^{r_m} \right) \bmod n \\ b \equiv \left(h_1^{r_1} \cdot ... \cdot h_k^{r_k} \cdot h_{k+1}^{r'_{k+1}} \cdot ... \cdot h_l^{r'_l} \right) \bmod n \end{cases} \quad (96),$$

Όπου

$$\begin{cases} k < m \\ k < l \end{cases},$$

$(r_1,..,r_k) \in (\mathbb{Z}^*)^k$ είναι κοινοί διακριτοί λογάριθμοι, $(r_{k+1},..,r_m) \in (\mathbb{Z}^*)^{m-k}$, $(r'_{k+1},..,r'_l) \in (\mathbb{Z}^*)^{l-k}$ και τα πλήθη των βάσεων m,l μπορεί να είναι ίσα ή διαφορετικά μεταξύ τους. Επίσης ισχύει

$$n = p \cdot q,$$

όπου p, p', q, q' είναι περιττοί πρώτοι αριθμοί με $p \neq q$, $p' \neq q'$,

$$p = 2 \cdot p' + 1 \text{ και } q = 2 \cdot q' + 1.$$

Στην περίπτωση που υπάρχουν πλειάδες κοινών λογαρίθμων $(r_1,..,r_k) \in (\mathbb{Z}^*)^k$ των a,b ως προς τις βάσεις $g_1,..,g_k$ και $h_1,..,h_k$ αντίστοιχα και ο Prover ξέρει κάποια από αυτές μαζί με λογαρίθμους ως προς τις υπόλοιπες βάσεις στις οποίες αναπαρίστανται

τα a, b, τότε χρησιμοποιεί το συγκεκριμένο πρωτόκολλο προκειμένου να πείσει τον Verifier ότι υπάρχουν κοινοί λογάριθμοι των a και b ως προς τις βάσεις $g_1,..,g_k$ και $h_1,..,h_k$ με αναπαραστάσεις στις βάσεις $g_1,..,g_m$ και $h_1,..,h_l$ αντίστοιχα. Η πλειάδα $(r_1,..,r_k)$ και οι λογάριθμοι ως προς τις υπόλοιπες βάσεις που γνωρίζει ο Prover αποτελούν την πληροφορία που πρέπει κατά τη διάρκεια και μετά το τέλος της εκτέλεσης του πρωτοκόλλου να μην αποκαλυφθεί άμεσα ή έμμεσα στον Verifier. Όπως το πρωτόκολλο της υποενότητας 5.1 έτσι και αυτό είναι κατάλληλο να χρησιμοποιηθεί στην περίπτωση που οι τέσσερις παραπάνω περιττοί πρώτοι αριθμοί καθώς και το γινόμενο $p' \cdot q'$ είναι άγνωστα στους Prover και Verifier, γιατί σε κανένα βήμα του δεν απαιτείται η χρήση και άρα η γνώση των πέντε αυτών παραμέτρων από τους δύο συμμετέχοντες. Επομένως το παρών zkp πρωτόκολλο είναι κατάλληλο να χρησιμοποιηθεί σε ηλεκτρονικές συναλλαγές που έχουν με φορείς νόμιμοι κάτοχοι πιστοποιητικών που εκδίδονται και υπογράφονται από την Αρχή σύμφωνα με το σχήμα των CL ψηφιακών υπογραφών. Το πρωτόκολλο και η απόδειξη ότι πετυχαίνει τον σκοπό του έχουν ως εξής:

- Prover
  - Στέλνει στον Verifier τα k και $g_i, h_i \ \ \forall i \in \{1,..,k\}$.
  - Εκτελεί με τον Verifier το πρωτόκολλο γνώσης διακριτών λογαρίθμων του a ως προς τις βάσεις $g_1,..,g_m$. Αν δεν αποδειχτεί ότι ο Prover γνωρίζει κάποιους διακριτούς λογαρίθμους, τότε το παρών πρωτόκολλο διακόπτεται.
  - Εκτελεί με τον Verifier το πρωτόκολλο γνώσης διακριτών λογαρίθμων του b ως προς τις βάσεις $h_1,..,h_l$. Αν δεν αποδειχτεί ότι ο Prover γνωρίζει κάποιους διακριτούς λογαρίθμους, τότε το παρών πρωτόκολλο διακόπτεται.
- Verifier
  - Υπολογίζει $a \cdot b$ και $g_i \cdot h_i \ \ \forall i \in \{1,..,k\}$.
  - Στέλνει στον Prover τα $a \cdot b$ και $g_i \cdot h_i \ \ \forall i \in \{1,..,k\}$.
- Prover
  - Εκτελεί με τον Verifier το πρωτόκολλο γνώσης διακριτών λογαρίθμων του $a \cdot b$ ως προς τις βάσεις $g_1 \cdot h_1,..,g_k \cdot h_k, g_{k+1},..,g_m, h_{k+1},..,h_l$.
- Verifier
  - Αν αποδειχτεί ότι ο Prover γνωρίζει διακριτούς λογαρίθμους του $a \cdot b$ ως προς τις βάσεις $g_1 \cdot h_1,..,g_k \cdot h_k, g_{k+1},..,g_m, h_{k+1},..,h_l$, τότε υπάρχουν κοινοί λογάριθμοι των a και b ως προς τις βάσεις $g_1,..,g_k$ και $h_1,..,h_k$ με αναπαραστάσεις στις βάσεις $g_1,..,g_m$ και $h_1,..,h_l$ αντίστοιχα.

Απόδειξη

Στην αρχή ο Prover στέλνει στον Verifier τα k και $g_i, h_i \ \ \forall i \in \{1,..,k\}$, προκειμένου ο τελευταίος να τα πληροφορηθεί.

1. <u>Υπάρχουν κοινοί λογάριθμοι και το πρωτόκολλο τηρείται</u>

Σε αυτήν την περίπτωση υπάρχουν πλειάδες κοινών λογαρίθμων $(r_1,..,r_k)\in(\mathbb{Z}^*)^k$ των a,b ως προς τις βάσεις $g_1,..,g_k$ και $h_1,..,h_k$ αντίστοιχα και ο Prover γνωρίζει κάποια από αυτές μαζί με λογαρίθμους ως προς τις υπόλοιπες βάσεις στις οποίες αναπαρίστανται τα a,b. Τότε εφόσον ο Prover γνωρίζει διακριτούς λογαρίθμους των a και b ως προς τα $g_1,..,g_m$ και $h_1,..,h_l$ αντίστοιχα, θα εκτελέσει με επιτυχία τα δύο πρώτα πρωτόκολλα γνώσης διακριτών λογαρίθμων. Σε αυτήν την περίπτωση η (96) λόγω της Πρότασης 8.7.3 συνεπάγεται ότι

$$(a\cdot b)\equiv\left(g_1^{r_1}\cdot..\cdot g_k^{r_k}\cdot g_{k+1}^{r_{k+1}}\cdot..\cdot g_m^{r_m}\cdot h_1^{r_1}\cdot..\cdot h_k^{r_k}\cdot h_{k+1}^{r'_{k+1}}\cdot..\cdot h_l^{r_l'}\right)\bmod n=$$

$$\left(\left(g_1^{r_1}\cdot h_1^{r_1}\right)\cdot..\cdot\left(g_k^{r_k}\cdot h_k^{r_k}\right)\cdot g_{k+1}^{r_{k+1}}\cdot..\cdot g_m^{r_m}\cdot h_{k+1}^{r'_{k+1}}\cdot..\cdot h_l^{r_l'}\right)\bmod n\Rightarrow$$

$$(a\cdot b)\equiv\left((g_1\cdot h_1)^{r_1}\cdot..\cdot(g_k\cdot h_k)^{r_k}\cdot g_{k+1}^{r_{k+1}}\cdot..\cdot g_m^{r_m}\cdot h_{k+1}^{r'_{k+1}}\cdot..\cdot h_l^{r_l'}\right)\bmod n\,.$$

Από τη στιγμή που ο Prover γνωρίζει όλους τους λογαρίθμους στην τελευταία ισοδυναμία, τότε γνωρίζει διακριτούς λογαρίθμους του $a\cdot b$ ως προς τις βάσεις

$$g_1\cdot h_1,..,g_k\cdot h_k,g_{k+1},..,g_m,h_{k+1},..,h_l$$

και επομένως θα εκτελέσει επιτυχώς και το τρίτο πρωτόκολλο γνώσης διακριτών λογαρίθμων.

2. <u>Δεν υπάρχουν κοινοί λογάριθμοι και το πρωτόκολλο τηρείται</u>

Σε αυτήν την περίπτωση δεν υπάρχουν πλειάδες κοινών λογαρίθμων $(r_1,..,r_k)\in(\mathbb{Z}^*)^k$ των a,b ως προς τις βάσεις $g_1,..,g_k$ και $h_1,..,h_k$ αντίστοιχα. Τότε ο Prover δε θα μπορέσει να ακολουθήσει την προηγούμενη διαδικασία προκειμένου να πληροφορηθεί διακριτούς λογαρίθμους του $a\cdot b$ ως προς τα

$$g_1\cdot h_1,..,g_k\cdot h_k,g_{k+1},..,g_m,h_{k+1},..,h_l\,.$$

Θα δειχτεί ότι σχεδόν κατά 100% δε γνωρίζει τέτοιους λογαρίθμους. Τίθεται ο ισχυρισμός πως γνωρίζει κάποιους. Αν ξέρει λογαρίθμους των a και b ως προς τις βάσεις $g_1,..,g_m$ και $h_1,..,h_l$ αντίστοιχα, θα εκτελέσει με επιτυχία τα δύο πρώτα πρωτόκολλα. Σε αντίθετη περίπτωση θα αποτύχει σε ένα από τα δύο και έτσι το παρών πρωτόκολλο θα διακοπεί με αποτέλεσμα ο Verifier να μην μπορέσει στο τέλος να διαπιστώσει εάν ο ισχυρισμός του Prover είναι αληθής. Στην πρώτη περίπτωση αν $\{r_1,..,r_m\},\{r'_1,..,r'_l\}$ είναι αντίστοιχα οι διακριτοί λογάριθμοι του a ως προς τις βάσεις $g_1,..,g_m$ και του b ως προς τις βάσεις $h_1,..,h_l$ τους οποίους ξέρει ο Prover, τότε θα ισχύει ότι

$$\begin{cases}a\equiv\left(g_1^{r_1}\cdot..\cdot g_k^{r_k}\cdot g_{k+1}^{r_{k+1}}\cdot..\cdot g_m^{r_m}\right)\bmod n\\ b\equiv\left(h_1^{r'_1}\cdot..\cdot h_k^{r'_k}\cdot h_{k+1}^{r'_{k+1}}\cdot..\cdot h_l^{r_l'}\right)\bmod n\end{cases}\quad(97).$$

Εφόσον δεν υπάρχουν κοινοί λογάριθμοι των a,b ως προς τα $g_1,..,g_k$ και $h_1,..,h_k$ αντίστοιχα, θα ισχύει επιπλέον ότι $r_i\neq r'_i$ για ένα τουλάχιστο $i\in\{1,..,k\}$. Οι λογάριθμοι του $a\cdot b$ ως προς τις βάσεις

$$g_1\cdot h_1,..,g_k\cdot h_k,g_{k+1},..,g_m,h_{k+1},..,h_l$$

που σύμφωνα με τον προηγούμενο ισχυρισμό γνωρίζει ο Prover, δε θα έγιναν γνωστοί σε αυτόν προσπαθώντας ο ίδιος να λύσει την ισοδυναμία

$$(a\cdot b)\equiv\left(\left(g_1\cdot h_1\right)^{x_1}\cdot..\cdot\left(g_k\cdot h_k\right)^{x_k}\cdot g_{k+1}{}^{x_{k+1}}\cdot..\cdot g_m{}^{x_m}\cdot h_{k+1}{}^{x'_{k+1}}\cdot..\cdot h_l{}^{x'_l}\right)\bmod n \quad (98)$$

ως προς

$$x_1,..,x_k,x_{k+1},..,x_m,x'_{k+1},..,x'_l\in\mathbb{Z}^*,$$

καθώς κάτι τέτοιο θα ήταν πάρα πολύ δύσκολο σύμφωνα με το Δεύτερο Ισχυρισμό Διακριτού Λογαρίθμου.

Λαμβάνοντας υπόψη του ότι ισχύει η (97), μια δεύτερη εναλλακτική οδός που πιθανόν θα τον οδηγούσε στη γνώση αυτών των λογαρίθμων θα ήταν να ακολουθούσε τις παρακάτω συνεπαγωγές προκειμένου να συμπεράνει τη συνθήκη που θα έπρεπε αυτοί να τηρούν. Από την (97) προκύπτει πως

$$(a\cdot b)\equiv\left(g_1{}^{r_1}\cdot..\cdot g_k{}^{r_k}\cdot g_{k+1}{}^{r_{k+1}}\cdot..\cdot g_m{}^{r_m}\cdot h_1{}^{r'_1}\cdot..\cdot h_k{}^{r'_k}\cdot h_{k+1}{}^{r'_{k+1}}\cdot..\cdot h_l{}^{r'_l}\right)\bmod n \quad (99).$$

Από την (98) συνεπάγεται ότι

$$(a\cdot b)\equiv\left(\left(g_1{}^{x_1}\cdot h_1{}^{x_1}\right)\cdot..\cdot\left(g_k{}^{x_k}\cdot h_k{}^{x_k}\right)\cdot g_{k+1}{}^{x_{k+1}}\cdot..\cdot g_m{}^{x_m}\cdot h_{k+1}{}^{x'_{k+1}}\cdot..\cdot h_l{}^{x'_l}\right)\bmod n\Rightarrow$$

$$(a\cdot b)\equiv\left(g_1{}^{x_1}\cdot..\cdot g_k{}^{x_k}\cdot g_{k+1}{}^{x_{k+1}}\cdot..\cdot g_m{}^{x_m}\cdot h_1{}^{x_1}\cdot..\cdot h_k{}^{x_k}\cdot h_{k+1}{}^{x'_{k+1}}\cdot..\cdot h_l{}^{x'_l}\right)\bmod n\xrightarrow{(99)}$$

$$\left(g_1{}^{r_1}\cdot..\cdot g_k{}^{r_k}\cdot g_{k+1}{}^{r_{k+1}}\cdot..\cdot g_m{}^{r_m}\cdot h_1{}^{r'_1}\cdot..\cdot h_k{}^{r'_k}\cdot h_{k+1}{}^{r'_{k+1}}\cdot..\cdot h_l{}^{r'_l}\right)\equiv$$

$$\left(g_1{}^{x_1}\cdot..\cdot g_k{}^{x_k}\cdot g_{k+1}{}^{x_{k+1}}\cdot..\cdot g_m{}^{x_m}\cdot h_1{}^{x_1}\cdot..\cdot h_k{}^{x_k}\cdot h_{k+1}{}^{x'_{k+1}}\cdot..\cdot h_l{}^{x'_l}\right)\bmod n\Rightarrow$$

$$\left(g_1{}^{r_1-x_1}\cdot..\cdot g_k{}^{r_k-x_k}\cdot g_{k+1}{}^{r_{k+1}-x_{k+1}}\cdot..\cdot g_m{}^{r_m-x_m}\cdot h_1{}^{r'_1-x_1}\cdot..\cdot h_k{}^{r'_k-x_k}\cdot h_{k+1}{}^{r'_{k+1}-x'_{k+1}}\cdot..\cdot h_l{}^{r'_l-x'_l}\right)\equiv 1\bmod n.$$

Από την τελευταία ισοδυναμία προκύπτει πως η συνθήκη που θα πρέπει να ικανοποιούν τα

$$x_1,..,x_k,x_{k+1},..,x_m,x'_{k+1},..,x'_l$$

είναι ότι τα

$$r_1-x_1,..,r_k-x_k,r_{k+1}-x_{k+1},..,r_m-x_m,r'_1-x_1,..,r'_k-x_k,r'_{k+1}-x'_{k+1},..,r'_l-x'_l$$

θα πρέπει να αποτελούν διακριτούς λογαρίθμους του 1 ως προς τις βάσεις

$$g_1,..,g_k,g_{k+1},..,g_m,h_1,..,h_k,h_{k+1},..,h_l\in QR_n^*-\{1\}$$

αντίστοιχα. Επειδή ο Prover δε γνωρίζει τα p',q', αφού αυτά κρατούνται μυστικά από την εκδότρια Αρχή όπως αναφέρθηκε στην υποενότητα 4.1, τότε σύμφωνα με την Πρόταση 21 θα ήταν πάρα πολύ δύσκολο να βρει μια μη μηδενική πλειάδα διακριτών λογαρίθμων του 1 ως προς τις βάσεις

$$g_1,..,g_k,g_{k+1},..,g_m,h_1,..,h_k,h_{k+1},..,h_l,$$

ώστε αρχικά να τη δοκιμάσει εάν θα μπορούσε να αποτελέσει τιμή της πλειάδας

$$\left(r_1-x_1,..,r_k-x_k,r_{k+1}-x_{k+1},..,r_m-x_m,r'_1-x_1,..,r'_k-x_k,r'_{k+1}-x'_{k+1},..,r'_l-x'_l\right)$$

και αν ναι μετά να δοκιμάσει αν τα

$$x_1,..,x_k,x_{k+1},..,x_m,x'_{k+1},..,x'_l$$

που θα είχε υπολογίσει ικανοποιούσαν την (98). Από την άλλη αν επέλεγε να δοκιμάσει την ίδια την μηδενική πλειάδα $\left(\underset{m+l}{0,..,0}\right)$, θα διαπίστωνε πως δε θα μπορούσε να αποτελέσει τιμή της

$$\left(r_1-x_1,..,r_k-x_k,r_{k+1}-x_{k+1},..,r_m-x_m,r'_1-x_1,..,r'_k-x_k,r'_{k+1}-x'_{k+1},..,r'_l-x'_l\right),$$

καθώς θα ήταν αδύνατο να ισχύσει

$$\begin{cases} r_1 - x_1 = 0 \\ .. \\ r_k - x_k = 0 \\ r_{k+1} - x_{k+1} = 0 \\ .. \\ r_m - x_m = 0 \\ r'_1 - x_1 = 0 \\ .. \\ r'_k - x_k = 0 \\ r'_{k+1} - x'_{k+1} = 0 \\ .. \\ r'_l - x'_l = 0 \end{cases}$$

και άρα

$$\begin{cases} x_1 = r_1 = r'_1 \\ .. \\ x_k = r_k = r'_k \end{cases},$$

αφού όπως προαναφέρθηκε ισχύει $r_i \neq r'_i$ για ένα τουλάχιστο $i \in \{1,..,k\}$. Επομένως ο Prover δε θα μπορούσε να υπολογίσει κάποια

$$x_1,..,x_k,x_{k+1},..,x_m,x'_{k+1},..,x'_l$$

που να τηρούσαν την παραπάνω συνθήκη ώστε μετά να δοκιμάσει αν αυτά ικανοποιούσαν την (98). Έτσι αν ακολουθούσε τη δεύτερη εναλλακτική οδό, σχεδόν κατά 100% δε θα μπορούσε να λάβει γνώση κάποιων διακριτών λογαρίθμων του $a \cdot b$ ως προς τις βάσεις

$$g_1 \cdot h_1,..,g_k \cdot h_k,g_{k+1},..,g_m,h_{k+1},..,h_l .$$

Συνεπώς σχεδόν σίγουρα με κανέναν τρόπο δε θα μπορούσε ο Prover να πληροφορηθεί τέτοιους διακριτούς λογαρίθμους και έτσι ο παραπάνω ισχυρισμός που τέθηκε δεν αληθεύει σχεδόν κατά 100%. Επομένως όταν δεν υπάρχουν πλειάδες κοινών λογαρίθμων $(r_1,..,r_k) \in (\mathbb{Z}^*)^k$ των a,b ως προς τις βάσεις $g_1,..,g_k$ και $h_1,..,h_k$ αντίστοιχα και το πρωτόκολλο τηρείται, ο Prover σχεδόν σίγουρα δε γνωρίζει διακριτούς λογαρίθμους του $a \cdot b$ ως προς τις βάσεις

$$g_1 \cdot h_1,..,g_k \cdot h_k,g_{k+1},..,g_m,h_{k+1},..,h_l .$$

Εφόσον σύμφωνα με την υπόθεση τηρείται το παρών πρωτόκολλο, ο Prover θα εκτελέσει κανονικά όπως προβλέπεται με τον Verifier το τελευταίο πρωτόκολλο γνώσης διακριτών λογαρίθμων και το αποτέλεσμα θα είναι σχεδόν 100% ανεπιτυχές για τον ίδιο.

3. <u>Δεν υπάρχουν κοινοί λογάριθμοι και ο Prover επιλέγει να μην τηρήσει το πρωτόκολλο</u>

Σε αυτήν την περίπτωση δεν υπάρχουν πλειάδες κοινών λογαρίθμων $(r_1,..,r_k) \in (\mathbb{Z}^*)^k$ των a,b ως προς τις βάσεις $g_1,..,g_k$ και $h_1,..,h_k$ αντίστοιχα και ο Prover ενεργεί έτσι προκειμένου να ξεγελάσει τον Verifier ώστε να τον πείσει για τον ψευδή ισχυρισμό του. Η μόνη δυνατότητα που έχει για να λειτουργήσει αντικανονικά είναι να μην

εκτελέσει όπως προβλέπεται το τελευταίο πρωτόκολλο γνώσης διακριτών λογαρίθμων, αφού προηγουμένως έχει τηρήσει όλα τα βήματα. Αν το εκτελούσε κανονικά, τότε όπως αναφέρθηκε προηγούμενα το αποτέλεσμα θα ήταν για τον ίδιο ανεπιτυχές αφού δεν υπάρχουν πλειάδες κοινών λογαρίθμων $(r_1,..,r_k)\in(\mathbb{Z}^*)^k$ των a,b ως προς τις βάσεις $g_1,..,g_k$ και $h_1,..,h_k$ αντίστοιχα. Θα μπορούσε επομένως να αλλοιώσει κάποια από τα

$$a\cdot b, g_1\cdot h_1,..,g_k\cdot h_k, g_{k+1},..,g_m, h_{k+1},..,h_l$$

ώστε να εκτελέσει αυτό το πρωτόκολλο με διαφορετικές παραμέτρους που θα του εξασφάλιζαν το επιτυχές για αυτόν αποτέλεσμα. Όμως όλες οι προηγούμενες παράμετροι είναι γνωστές στον Verifier, τα $a\cdot b, g_1\cdot h_1,..,g_k\cdot h_k$ τα υπολόγισε ο ίδιος και τα $g_{k+1},..,g_m$ και $h_{k+1},..,h_l$ είναι γνωστά από το πρώτο και δεύτερο αντίστοιχα πρωτόκολλο γνώσης διακριτών λογαρίθμων, όπου ως βάσεις που είναι ο Prover του τα κοινοποίησε στην αρχή των εκτελέσεών τους. Έτσι όταν πληροφορηθεί τις αλλοιωμένες παραμέτρους από τον Prover στην αρχή της εκτέλεσης του τρίτου πρωτοκόλλου γνώσης διακριτών λογαρίθμων, αυτός θα τις εντοπίσει, θα καταλάβει ότι αυτό δεν τηρείται από τον Prover και θα διακόψει τη συμμετοχή του σε αυτό μην μπορώντας στο τέλος να διαπιστώσει εάν ο ισχυρισμός του Prover είναι αληθής.
Έτσι στην περίπτωση που δεν υπάρχουν πλειάδες κοινών λογαρίθμων $(r_1,..,r_k)\in(\mathbb{Z}^*)^k$ των a,b ως προς τις βάσεις $g_1,..,g_k$ και $h_1,..,h_k$ αντίστοιχα και ο Prover επιλέξει να μην τηρήσει το πρωτόκολλο που εξετάζεται στην παρούσα υποενότητα, δε θα καταφέρει να εκτελέσει επιτυχώς το πρωτόκολλο γνώσης διακριτών λογαρίθμων του $a\cdot b$ ως προς τις βάσεις

$$g_1\cdot h_1,..,g_k\cdot h_k, g_{k+1},..,g_m, h_{k+1},..,h_l .$$

Συνεπώς από την παρούσα απόδειξη προκύπτει πως μόνο όταν υπάρχουν πλειάδες κοινών λογαρίθμων $(r_1,..,r_k)\in(\mathbb{Z}^*)^k$ των a,b ως προς τις βάσεις $g_1,..,g_k$ και $h_1,..,h_k$ αντίστοιχα, ο Prover γνωρίζει κάποια από αυτές μαζί με λογαρίθμους ως προς τις υπόλοιπες βάσεις στις οποίες αναπαρίστανται τα a,b και το πρωτόκολλο τηρηθεί, αυτός μπορεί να πείσει σίγουρα τον Verifier ότι γνωρίζει διακριτούς λογαρίθμους του $a\cdot b$ ως προς τα

$$g_1\cdot h_1,..,g_k\cdot h_k, g_{k+1},..,g_m, h_{k+1},..,h_l .$$

Διαφορετικά η πιθανότητα να πειστεί ο Verifier είναι εξαιρετικά μικρή. Αυτό σημαίνει πως η απόδειξη γνώσης τέτοιων λογαρίθμων από τον Prover αποτελεί σχεδόν κατά 100% και απόδειξη ότι υπάρχουν κοινοί λογάριθμοι των a και b ως προς τις βάσεις $g_1,..,g_k$ και $h_1,..,h_k$ με αναπαραστάσεις στις βάσεις $g_1,..,g_m$ και $h_1,..,h_l$ αντίστοιχα.

4. <u>Εμπιστευτικότητα πληροφορίας</u>

Στην περίπτωση 1 οι κοινοί λογάριθμοι όπως και εκείνοι ως προς τις υπόλοιπες βάσεις που γνωρίζει ο Prover, αποτελούν πληροφορία που δεν μπορεί να γίνει γνωστή στον Verifier. Από την μία δεν την μαθαίνει άμεσα από τον Prover. Από την άλλη, στα πλαίσια της εκτέλεσης του πρωτοκόλλου γνώσης διακριτών λογαρίθμων του a ως προς τις βάσεις $g_1,..,g_m$, δεν είναι δυνατό να αποκαλυφθούν άμεσα ή έμμεσα σε αυτόν οι κοινοί λογάριθμοι, που είναι λογάριθμοι ως προς τα $g_1,..,g_k$, καθώς και αυτοί ως προς τα $g_{k+1},..,g_m$. Επίσης στα πλαίσια της εκτέλεσης του πρωτοκόλλου

γνώσης διακριτών λογαρίθμων του b ως προς τις βάσεις $h_1,..,h_l$, δεν είναι δυνατό να αποκαλυφθούν άμεσα ή έμμεσα στον Verifier οι κοινοί λογάριθμοι, που είναι λογάριθμοι ως προς τα $h_1,..,h_k$, καθώς και αυτοί ως προς τα $h_{k+1},..,h_l$. Τέλος στα πλαίσια της εκτέλεσης του πρωτοκόλλου γνώσης διακριτών λογαρίθμων του $a \cdot b$ ως προς τις βάσεις

$$g_1 \cdot h_1,..,g_k \cdot h_k, g_{k+1},..,g_m, h_{k+1},..,h_l,$$

δεν είναι δυνατό να αποκαλυφθούν άμεσα ή έμμεσα σε αυτόν όλοι οι προηγούμενοι λογάριθμοι.

Όπως αναφέρθηκε στην αρχή αυτής της υποενότητας, το παρών πρωτόκολλο είναι κατάλληλο να χρησιμοποιηθεί στην περίπτωση που τα $p, p', q, q', p' \cdot q'$ είναι άγνωστα στους Prover και Verifier, γιατί σε κανένα βήμα του δεν απαιτείται η χρήση και άρα η γνώση τους από αυτούς τους δύο. Πράγματι, όπως φαίνεται και από την παραπάνω παρουσίαση των βημάτων του πρωτοκόλλου δεν χρησιμοποιούνται πουθενά οι πέντε αυτές παράμετροι, κάτι που συμβαίνει και με καθένα από τα τρία πρωτόκολλα γνώσης διακριτών λογαρίθμων που λαμβάνουν μέρος στο παρών πρωτόκολλο, όπως αναφέρθηκε στην υποενότητα 5.1.

5.4. Zkp Πρωτόκολλο Εγκυρότητας Πιστοποιητικού

[6] Στην υποενότητα αυτή παρουσιάζεται και αναλύεται ένα zkp πρωτόκολλο το οποίο χρησιμοποιεί ο Prover για να πείσει τον Verifier ότι κατέχει ένα έγκυρο πιστοποιητικό, το οποίο εκδόθηκε και υπογράφτηκε από την εκδότρια Αρχή σύμφωνα με το σχήμα των CL ψηφιακών υπογραφών. Στην περίπτωση που ο ισχυρισμός του Prover είναι αληθής, τότε όπως αναφέρθηκε στην υποενότητα 4.4 ο ίδιος μπορεί να επιβεβαιώσει την ισχύ της εξίσωσης

$$Z = \left(A^e \cdot R_1^{m_1} \cdot R_2^{m_2} \cdot S^v\right) \bmod n \quad (71),$$

όπου $m_1, (A, e, v), m_2$ είναι αντίστοιχα ο κώδικας του πιστοποιητικού που υπολόγισε ο ίδιος ο Prover κατά τη φάση της επιβεβαίωσης, η υπογραφή της Αρχής στο πιστοποιητικό και το γινόμενο των πρώτων αριθμών στους οποίους είναι κωδικοποιημένες οι τιμές των πεδίων του πιστοποιητικού. Οι τρεις αυτές παράμετροι είναι η πληροφορία που έχει σταλθεί από την Αρχή στον Prover και πρέπει κατά τη διάρκεια και μετά το τέλος της εκτέλεσης του συγκεκριμένου πρωτοκόλλου να μην αποκαλυφθεί άμεσα ή έμμεσα στον Verifier. Το πρωτόκολλο και η απόδειξη ότι πετυχαίνει τον σκοπό του έχουν ως εξής:

- <u>Prover</u>
  - Επιλέγει τυχαία $r \in \mathbb{Z}^*$.
  - Υπολογίζει $\begin{cases} S^{-1} \\ A' = \left(A \cdot \left(S^{-1}\right)^r\right) \bmod n \quad (100), \text{ έτσι ώστε } A' \neq 1. \\ v' = v + e \cdot r \end{cases}$
  - Εκτελεί με τον Verifier το πρωτόκολλο γνώσης διακριτών λογαρίθμων του Z ως προς τις βάσεις A', R_1, R_2, S.
- <u>Verifier</u>
  - Αν αποδειχτεί ότι ο Prover γνωρίζει διακριτούς λογαρίθμους του Z ως προς τις βάσεις A', R_1, R_2, S, τότε αυτός κατέχει ένα έγκυρο

πιστοποιητικό που εκδόθηκε και υπογράφτηκε από την εκδότρια Αρχή σύμφωνα με το σχήμα των CL ψηφιακών υπογραφών.

Απόδειξη

1. Ο Prover κατέχει ένα έγκυρο πιστοποιητικό και το πρωτόκολλο τηρείται

Σε αυτήν την περίπτωση από την πρώτη εξίσωση του συστήματος της (100) συνεπάγεται ότι

$$A'^e \equiv \left(A \cdot S^{-r}\right)^e \bmod n \Rightarrow A'^e \equiv \left(A^e \cdot \left(S^{-r}\right)^e\right) \bmod n \Rightarrow$$

$$\left(A'^e \cdot R_1^{m_1} \cdot R_2^{m_2}\right) \equiv \left(A^e \cdot R_1^{m_1} \cdot R_2^{m_2} \cdot S^{-r \cdot e}\right) \bmod n .$$

Επίσης λόγω της δεύτερης εξίσωσης του ίδιου συστήματος, θα ισχύει ότι

$$-e \cdot r = v - v'$$

και άρα η τελευταία ισοδυναμία συνεπάγεται ότι

$$\left(A'^e \cdot R_1^{m_1} \cdot R_2^{m_2}\right) \equiv \left(A^e \cdot R_1^{m_1} \cdot R_2^{m_2} \cdot S^{v-v'}\right) \bmod n \Rightarrow$$

$$\left(A'^e \cdot R_1^{m_1} \cdot R_2^{m_2}\right) \equiv \left(A^e \cdot R_1^{m_1} \cdot R_2^{m_2} \cdot S^{v} \cdot S^{-v'}\right) \bmod n \Rightarrow$$

$$\left(A'^e \cdot R_1^{m_1} \cdot R_2^{m_2} \cdot S^{v'}\right) \equiv \left(A^e \cdot R_1^{m_1} \cdot R_2^{m_2} \cdot S^{v}\right) \bmod n \xrightarrow{(71)}$$

$$Z = \left(A'^e \cdot R_1^{m_1} \cdot R_2^{m_2} \cdot S^{v'}\right) \bmod n \quad (101).$$

Από την (101) προκύπτει πως η τριάδα $\left(A', e, v'\right)$ ικανοποιεί την (71) όπως ακριβώς και η υπογραφή $\left(A, e, v\right)$. Εφόσον $A, S^{-1} \in QR_n^*$, σύμφωνα με την (100) και την Πρόταση 20.3 θα ισχύει $A' \in QR_n^*$ και επειδή $A' \neq 1$, τότε $A' \in QR_n^* - \{1\}$. Ο Prover ως κάτοχος ενός έγκυρου πιστοποιητικού ξέρει τα e, m_1, m_2, v' τα οποία αποτελούν στην (101) διακριτούς λογαρίθμους του Z ως προς τις βάσεις $A', R_1, R_2, S \in QR_n^* - \{1\}$ αντίστοιχα. Έτσι από τη στιγμή που γνωρίζει διακριτούς λογαρίθμους του Z ως προς αυτές τις βάσεις, θα αποδείξει τη γνώση του αυτή στον Verifier όταν και οι δύο χρησιμοποιήσουν το zkp πρωτόκολλο γνώσης διακριτών λογαρίθμων. Η απόδειξη αυτή θα γίνει χωρίς να αποκαλυφθούν άμεσα ή έμμεσα οι συγκεκριμένοι διακριτοί λογάριθμοι.

2. Ο Prover δεν κατέχει κάποιο έγκυρο πιστοποιητικό και το πρωτόκολλο τηρείται

Σε αυτήν την περίπτωση εφόσον το πρωτόκολλο τηρείται, ο Prover θα επιχειρήσει να εκτελέσει κανονικά το πρωτόκολλο γνώσης διακριτών λογαρίθμων. Όμως από τη στιγμή που δεν κατέχει κάποιο έγκυρο πιστοποιητικό, δεν μπορεί να υπολογίσει τα A', v' σύμφωνα με την (100), αφού δεν ξέρει τα A, e, v. Προκειμένου να ισχύσει η (101), με δεδομένες τις παραμέτρους n, S, R_1, R_2, Z του δημοσίου κλειδιού της Αρχής, ο Prover θα πρέπει να βρει μια κατάλληλη πεντάδα $\left(m_1, m_2, A', e, v'\right)$. Όμως όπως αναφέρθηκε και αποδείχτηκε στην υποενότητα 4.4, καμιά άλλη οντότητα εκτός της Αρχής δε θα μπορούσε **από μόνη της** να δημιουργήσει μια τέτοια πεντάδα. Έτσι προκειμένου ο Prover να εκτελέσει το πρωτόκολλο γνώσης διακριτών λογαρίθμων, θα επιλέξει τυχαία μία βάση $A' \in QR_n^* - \{1\}$ και από τη στιγμή που δε θα μπορεί να μάθει διακριτούς λογαρίθμους του Z ως προς τις βάσεις A', R_1, R_2, S, δε θα μπορέσει να εκτελέσει το πρωτόκολλο επιτυχώς.

Να σημειωθεί πως η παραπάνω τονισμένη έκφραση ‘από μόνη της’ σημαίνει χωρίς κάποια επιπρόσθετη πληροφορία. Στην προηγούμενη περίπτωση που ο Prover κατείχε

ένα έγκυρο πιστοποιητικό, μπόρεσε να βρει μια πεντάδα (m_1, m_2, A', e, v') που να ικανοποιεί την (101), αλλά όχι από μόνος του καθώς το m_1 το υπολόγισε από το πιστοποιητικό που παρέλαβε από την Αρχή, τα m_2, e του τα έστειλε έτοιμα η ίδια και για τον υπολογισμό των A', v' στηρίχτηκε εκτός από το e και στα A, v που και αυτά τα παρέλαβε από την Αρχή.

3. <u>Ο Prover δεν κατέχει κάποιο έγκυρο πιστοποιητικό και επιλέγει να μην τηρήσει το πρωτόκολλο</u>

Σε αυτήν την περίπτωση ο Prover ενεργεί έτσι προκειμένου να ξεγελάσει τον Verifier ώστε να τον πείσει για τον ψευδή ισχυρισμό του. Η μόνη δυνατότητα που έχει για να λειτουργήσει αντικανονικά είναι να μην εκτελέσει όπως προβλέπεται το πρωτόκολλο γνώσης διακριτών λογαρίθμων του Z ως προς τις βάσεις A', R_1, R_2, S. Αν το εκτελούσε κανονικά, τότε όπως αναφέρθηκε προηγούμενα το αποτέλεσμα θα ήταν για τον ίδιο ανεπιτυχές αφού δεν είναι κάτοχος έγκυρου πιστοποιητικού. Θα μπορούσε επομένως να αλλοιώσει κάποια από τα Z, R_1, R_2, S ώστε με την προσθήκη ενός κατάλληλου A' να εκτελέσει αυτό το πρωτόκολλο με διαφορετικές παραμέτρους που θα του εξασφάλιζαν το επιτυχές για αυτόν αποτέλεσμα. Όμως και οι τέσσερις προηγούμενες παράμετροι είναι γνωστές στον Verifier ως μέρος του δημοσίου κλειδιού της εκδότριας Αρχής. Έτσι όταν του κοινοποιηθούν οι αλλοιωμένες παράμετροι από τον Prover στην αρχή της εκτέλεσης του πρωτοκόλλου γνώσης διακριτών λογαρίθμων, αυτός θα τις εντοπίσει, θα καταλάβει ότι αυτό δεν τηρείται από τον Prover και θα διακόψει τη συμμετοχή του σε αυτό μην μπορώντας στο τέλος να διαπιστώσει εάν ο ισχυρισμός του Prover είναι αληθής.

Έτσι στην περίπτωση που ο Prover δεν κατέχει κάποιο έγκυρο πιστοποιητικό και επιλέξει να μην τηρήσει το πρωτόκολλο που εξετάζεται στην παρούσα υποενότητα, δε θα καταφέρει να εκτελέσει επιτυχώς το πρωτόκολλο γνώσης διακριτών λογαρίθμων του Z ως προς τις βάσεις A', R_1, R_2, S.

Συνεπώς από την παρούσα απόδειξη προκύπτει πως μόνο όταν ο Prover κατέχει ένα έγκυρο πιστοποιητικό και το πρωτόκολλο τηρηθεί μπορεί να πείσει τον Verifier ότι γνωρίζει διακριτούς λογαρίθμους του Z ως προς τις βάσεις A', R_1, R_2, S για κάποιο $A' \in QR_n^* - \{1\}$. Αυτό σημαίνει πως η απόδειξη γνώσης τέτοιων λογαρίθμων από τον Prover αποτελεί και απόδειξη κατοχής έγκυρου πιστοποιητικού εκ μέρους του. Στην περίπτωση που γνωρίζει τέτοιους λογαρίθμους, ο λογάριθμος του Z ως προς τη βάση R_1 είναι ο κώδικας του πιστοποιητικού που υπολόγισε ο ίδιος κατά τη φάση της επιβεβαίωσης και αυτός ως προς τη βάση R_2 είναι το γινόμενο των πρώτων αριθμών στους οποίους είναι κωδικοποιημένες οι τιμές των πεδίων του πιστοποιητικού.

4. <u>Εμπιστευτικότητα πληροφορίας</u>

Η πληροφορία που αποτελείται από αυτούς τους δύο λογαρίθμους m_1, m_2 και την υπογραφή (A, e, v) δεν είναι δυνατό να γίνει γνωστή στον Verifier. Όσο εκτελείται το πρωτόκολλο που εξετάζεται σε αυτήν την υποενότητα δεν την μαθαίνει άμεσα από τον Prover. Από την άλλη, κατά τη διάρκεια και μετά το τέλος της εκτέλεσης του πρωτοκόλλου γνώσης διακριτών λογαρίθμων του Z ως προς τις βάσεις A', R_1, R_2, S, οι τέσσερις λογάριθμοι e, m_1, m_2, v' δεν αποκαλύπτονται άμεσα ή έμμεσα σε αυτόν. Από τη στιγμή που δεν ξέρει τα e, v', r, μια και το τελευταίο δεν του κοινοποιείται από τον Prover, αδυνατεί να υπολογίσει από την εξίσωση

$$v' = v + e \cdot r$$

το v. Επίσης από την πρώτη εξίσωση της (100) συνεπάγεται ότι

$$A' = \left(A \cdot S^{-r}\right) \bmod n \Rightarrow \left(A' \cdot S^{r}\right) \equiv A \bmod n \Rightarrow A = \left(A' \cdot S^{r}\right) \bmod n \quad (102),$$

αφού $A \in QR_n^*$ και άρα $A \in \mathbb{Z}_n^*$, οπότε $A < n$ και συνεπώς

$$A = A \bmod n.$$

Επειδή $r \in \mathbb{Z}^*$, ο Prover επιλέγει ένα r διαφορετικό από το 0. Αν επέλεγε το 0 για την τιμή του r, τότε η πρώτη εξίσωση της (100) θα συνεπαγόταν

$$A' = \left(A \cdot \left(S^{-1}\right)^0\right) \bmod n = \left(A \cdot 1\right) \bmod n \Rightarrow A' = A.$$

Έτσι ο Verifier θα μάθαινε το A αφού στην αρχή της εκτέλεσης του παραπάνω πρωτοκόλλου γνώσης διακριτών λογαρίθμων θα κοινοποιούνταν από τον Prover σε αυτόν ως μία από τις τέσσερις βάσεις, συγκεκριμένα η πρώτη στη θέση του A'. Από τη στιγμή που $r \neq 0$, τυχαίνει να είναι $A' \neq A$ και έτσι όταν στην αρχή της εκτέλεσης αυτού του πρωτοκόλλου γνώσης διακριτών λογαρίθμων λαμβάνει την πρώτη βάση A', λαμβάνει έναν αριθμό διαφορετικό του A. Από την άλλη δε θα μπορούσε να χρησιμοποιήσει την (102) προκειμένου να μάθει το A αφού δε γνωρίζει το r. Έτσι εκτός από τα e, m_1, m_2, v, ο Verifier αδυνατεί να πληροφορηθεί και το A.

Αν ο Prover είναι κάτοχος έγκυρου πιστοποιητικού και προκειμένου να υπολογίσει το A' προτιμήσει να επιλέξει για την τιμή του r το 0 με αποτέλεσμα να ισχύει $A' = A$, τότε σε αυτήν την περίπτωση ο Verifier θα μάθει την πρώτη παράμετρο της υπογραφής (A, e, v) του πιστοποιητικού. Κάτι τέτοιο όμως δεν είναι επιθυμητό για τον Prover, διότι ξέροντας ο Verifier το A μπορεί να το ταυτοποιήσει με την πρώτη παράμετρο κάποιας CL ψηφιακής υπογραφής που μπορεί να πληροφορηθεί και η οποία να έχει καταγραφεί στα αρχεία ενός ιδιωτικού ή δημόσιου φορέα ως το αποτέλεσμα κάποιας ηλεκτρονικής συναλλαγής. Σε μια τέτοια περίπτωση ο Verifier είναι δυνατό να υποθέσει πως πιθανόν αυτή η υπογραφή είναι ίδια με την (A, e, v), παρόλο που δε γνωρίζει τα e, v για να τα συγκρίνει με τις άλλες δύο παραμέτρους της υπογραφής που πληροφορήθηκε. Υποθέτοντας πως οι δύο υπογραφές είναι ίδιες, ο Verifier υποθέτει πως ο Prover ήταν αυτός που διενήργησε την παραπάνω ηλεκτρονική συναλλαγή με τον φορέα, ο οποίος θέλοντας να ελέγξει την εγκυρότητα του πιστοποιητικού του, ζήτησε και έλαβε από αυτόν την υπογραφή (A, e, v) την οποία και μετά καταχώρισε. Αν όντως ο Prover διενήργησε την παραπάνω συναλλαγή, τότε ο Verifier υποθέτει κάτι που είναι αλήθεια εγείροντας έτσι θέμα παραβίασης της ιδιωτικότητάς του Prover. Για τον λόγο αυτό όποτε ο τελευταίος θελήσει να αποδείξει ότι είναι κάτοχος έγκυρου πιστοποιητικού, προκειμένου να χρησιμοποιήσει το πρωτόκολλο γνώσης διακριτών λογαρίθμων, επιλέγει για τον υπολογισμό του A' μια τιμή του r διαφορετική από το 0.

5.5. Zkp Πρωτόκολλο Πεδίου με Τιμή Ίση με μια Δεδομένη Τιμή

[6] Στην υποενότητα αυτή παρουσιάζεται και αναλύεται ένα zkp πρωτόκολλο το οποίο χρησιμοποιεί ο Prover για να πείσει τον Verifier ότι η τιμή ενός πεδίου του έγκυρου πιστοποιητικού που κατέχει είναι ίση με μια δεδομένη τιμή. Η τιμή αυτού του πεδίου είναι η πληροφορία που σχετίζεται με τον προηγούμενο ισχυρισμό και στην περίπτωση που αυτός είναι αληθής δε θα παραμείνει μυστική στον Verifier, καθώς μετά την εκτέλεση του συγκεκεκριμένου πρωτοκόλλου θα αποδειχτεί σε αυτόν ότι είναι ίση με τη δεδομένη τιμή. Στην περίπτωση που ο Prover δεν καταφέρει να

αποδείξει το αληθές του ισχυρισμού του, τότε η τιμή του συγκεκριμένου πεδίου πρέπει να συνεχίσει να παραμένει μυστική στον Verifier κατά τη διάρκεια και μετά το τέλος της εκτέλεσης του πρωτοκόλλου. Όπως αναφέρθηκε στο τέλος της ενότητας 5, θεωρείται πως πριν την εκτέλεση του παρόντος πρωτοκόλλου έχει ήδη αποδειχτεί η εγκυρότητα του πιστοποιητικού του Prover μέσω του πρωτοκόλλου εγκυρότητας πιστοποιητικού, το οποίο παρουσιάστηκε και αναλύθηκε στην προηγούμενη υποενότητα. Το παρών πρωτόκολλο είναι κατάλληλο να εφαρμοστεί στην περίπτωση του τελευταίου παραδείγματος της ενότητας 2, όπου ο ισχυρισμός είναι ο εξής: '*το πεδίο του επιπέδου μόρφωσης έχει την τιμή 'Πανεπιστήμιο''*. Η δεδομένη τιμή σε αυτήν την περίπτωση είναι η τιμή '*Πανεπιστήμιο*'. Το πρωτόκολλο και η απόδειξη ότι πετυχαίνει τον σκοπό του παρουσιάζονται παρακάτω.

- Verifier
  - Επιλέγει από τη δημοσιοποιημένη λίστα των κωδικών των τιμών των πεδίων της Αρχής τον πρώτο αριθμό v που αντιστοιχεί στη δεδομένη τιμή την οποία ο Prover θέλει να αποδείξει ότι είναι η τιμή ενός συγκεκριμένου πεδίου του πιστοποιητικού του.
  - Υπολογίζει $R = R_2^{\,v} \bmod n$ (103), όπου θεωρείται πως $R \neq 1$.
  - Στέλνει στον Prover το R.
- Prover
  - Επιλέγει από τη δημοσιοποιημένη λίστα των κωδικών των τιμών των πεδίων της Αρχής τον πρώτο αριθμό v.
  - Υπολογίζει $d = \frac{m_2}{v}$ (104), όπου m_2 είναι το γινόμενο των πρώτων αριθμών στους οποίους είναι κωδικοποιημένες οι τιμές των πεδίων του πιστοποιητικού του.
  - Εκτελεί με τον Verifier το πρωτόκολλο γνώσης διακριτών λογαρίθμων του Z ως προς τις βάσεις A', R_1, R, S, όπου A' είναι υπολογισμένο από το πρωτόκολλο εγκυρότητας πιστοποιητικού που εκτέλεσε προηγούμενα με τον Verifier για να αποδείξει ότι κατέχει ένα έγκυρο πιστοποιητικό.
- Verifier
  - Αν αποδειχτεί ότι ο Prover γνωρίζει διακριτούς λογαρίθμους του Z ως προς τις βάσεις A', R_1, R, S, τότε αυτός κατέχει ένα έγκυρο πιστοποιητικό όπου η τιμή του συγκεκριμένου πεδίου του είναι ίση με τη δεδομένη τιμή.

Απόδειξη

Εφόσον ο Prover προηγουμένως εκτέλεσε με επιτυχία το πρωτόκολλο εγκυρότητας πιστοποιητικού, τότε θα ισχύει

$$Z = \left(A'^{e} \cdot R_1^{m_1} \cdot R_2^{m_2} \cdot S^{v'} \right) \bmod n \quad (101).$$

1. Η τιμή του συγκεκριμένου πεδίου του έγκυρου πιστοποιητικού του Prover είναι ίση με τη δεδομένη τιμή και το πρωτόκολλο τηρείται

Σε αυτήν την περίπτωση στο γινόμενο m_2 των πρώτων αριθμών στους οποίους είναι κωδικοποιημένες οι τιμές των πεδίων του πιστοποιητικού, θα περιέχεται ως

παράγοντάς του ο πρώτος αριθμός v που αντιστοιχεί στη δεδομένη τιμή, δηλαδή θα $\exists d \in \mathbb{Z}^*$ ώστε να είναι

$$m_2 = v \cdot d \ .$$

Έτσι η (101) γίνεται

$$Z = \left(A'^e \cdot R_1^{m_1} \cdot R_2^{v \cdot d} \cdot S^{v'} \right) \bmod n \ \ (105).$$

Από την (103) συνεπάγεται ότι

$$R^d \equiv \left(R_2^{\ v} \right)^d \bmod n \Rightarrow R^d \equiv R_2^{\ v \cdot d} \bmod n \Rightarrow$$

$$\left(A'^e \cdot R_1^{m_1} \cdot R^d \cdot S^{v'} \right) \equiv \left(A'^e \cdot R_1^{m_1} \cdot R_2^{v \cdot d} \cdot S^{v'} \right) \bmod n \xrightarrow{(105)}$$

$$Z = \left(A'^e \cdot R_1^{m_1} \cdot R^d \cdot S^{v'} \right) \bmod n \ \ (106).$$

Ο Prover μπορεί να υπολογίσει το

$$d = \frac{m_2}{v}$$

εφόσον γνωρίζει τα m_2, v και έτσι να μάθει στην (106) έναν διακριτό λογάριθμο του Z ως προς το R, το οποίο ήδη το πληροφορήθηκε από τον Verifier. Εφόσον $R_2 \in QR_n^*$, σύμφωνα με την (103) και την Πρόταση 20.2 θα ισχύει $R \in QR_n^*$ και επειδή $R \neq 1$, τότε $R \in QR_n^* - \{1\}$. Επίσης γνωρίζει τα e, m_1, v' και έτσι ξέρει στην (106) διακριτούς λογαρίθμους του Z ως προς τα A', R_1, S αντίστοιχα. Από τη στιγμή που γνωρίζει διακριτούς λογαρίθμους του Z ως προς τις βάσεις $A', R_1, R, S \in QR_n^* - \{1\}$, θα αποδείξει τη γνώση του αυτή στον Verifier όταν και οι δύο χρησιμοποιήσουν το zkp πρωτόκολλο γνώσης διακριτών λογαρίθμων. Η απόδειξη αυτή θα γίνει χωρίς να αποκαλυφθούν άμεσα ή έμμεσα στον Verifier οι συγκεκριμένοι διακριτοί λογάριθμοι.

2. <u>Η δεδομένη τιμή δεν είναι ίδια με αυτήν που έχει το συγκεκριμένο πεδίο του έγκυρου πιστοποιητικού του Prover και το πρωτόκολλο τηρείται</u>

Σε αυτήν την περίπτωση στο γινόμενο m_2 των πρώτων αριθμών στους οποίους είναι κωδικοποιημένες οι τιμές των πεδίων του πιστοποιητικού, δε θα περιέχεται ως παράγοντάς του ο πρώτος αριθμός v που αντιστοιχεί στη δεδομένη τιμή, δηλαδή δε θα $\exists d \in \mathbb{Z}^*$ ώστε να είναι

$$m_2 = v \cdot d \ .$$

Από τη στιγμή που ο Prover αδυνατεί να βρει κάποιο $d \in \mathbb{Z}^*$ ώστε να ισχύει

$$d = \frac{m_2}{v}$$

όπως έκανε πριν, δε θα μπορέσει να ακολουθήσει την προηγούμενη διαδικασία προκειμένου να πληροφορηθεί διακριτούς λογαρίθμους του Z ως προς τις βάσεις A', R_1, R, S. Θα δειχτεί ότι σχεδόν κατά 100% αυτός δε γνωρίζει τέτοιους λογαρίθμους. Τίθεται ο ισχυρισμός πως γνωρίζει κάποιους.

Σχεδόν σίγουρα η γνώση αυτών δε θα προήλθε προσπαθώντας ο ίδιος να λύσει την εξίσωση

$$Z = \left(A'^{x_1} \cdot R_1^{x_2} \cdot R^{x_3} \cdot S^{x_4} \right) \bmod n \ \ (107)$$

ως προς $x_1, x_2, x_3, x_4 \in \mathbb{Z}^*$, καθώς κάτι τέτοιο θα ήταν πάρα πολύ δύσκολο σύμφωνα με το Δεύτερο Ισχυρισμό Διακριτού Λογαρίθμου.

Λαμβάνοντας υπόψη του ότι ισχύει η (103), αφού σύμφωνα με την υπόθεση το πρωτόκολλο τηρείται και άρα ο Verifier θα υπολόγισε σωστά το R από αυτήν τη σχέση, αλλά και ότι είναι κάτοχος έγκυρου πιστοποιητικού και ισχύει επίσης η (101), μια δεύτερη εναλλακτική οδός που πιθανόν θα τον οδηγούσε στη γνώση αυτών των λογαρίθμων θα ήταν να ακολουθούσε τις παρακάτω συνεπαγωγές προκειμένου να συμπεράνει τη συνθήκη που θα έπρεπε να τηρούν τα x_1, x_2, x_3, x_4. Από την (103) συνεπάγεται πως

$$R^{x_3} \equiv \left(R_2{}^{v}\right)^{x_3} \bmod n \Rightarrow R^{x_3} \equiv R_2{}^{v \cdot x_3} \bmod n \Rightarrow$$

$$\left(A'^{x_1} \cdot R_1^{x_2} \cdot R^{x_3} \cdot S^{x_4}\right) \equiv \left(A'^{x_1} \cdot R_1^{x_2} \cdot R_2{}^{v \cdot x_3} \cdot S^{x_4}\right) \bmod n \xrightarrow{(107)}$$

$$Z = \left(A'^{x_1} \cdot R_1^{x_2} \cdot R_2{}^{v \cdot x_3} \cdot S^{x_4}\right) \bmod n \xrightarrow{(101)}$$

$$\left(A'^{e} \cdot R_1^{m_1} \cdot R_2{}^{m_2} \cdot S^{v'}\right) \equiv \left(A'^{x_1} \cdot R_1^{x_2} \cdot R_2{}^{v \cdot x_3} \cdot S^{x_4}\right) \bmod n \Rightarrow$$

$$\left(A'^{e} \cdot R_1^{m_1} \cdot R_2{}^{m_2} \cdot S^{v'} \cdot A'^{-x_1} \cdot R_1^{-x_2} \cdot R_2{}^{-v \cdot x_3} \cdot S^{-x_4}\right) \equiv 1 \bmod n \Rightarrow$$

$$\left(A'^{e-x_1} \cdot R_1^{m_1-x_2} \cdot R_2{}^{m_2-v \cdot x_3} \cdot S^{v'-x_4}\right) \equiv 1 \bmod n .$$

Από την τελευταία ισοδυναμία προκύπτει πως η συνθήκη που πρέπει να ικανοποιούν τα x_1, x_2, x_3, x_4 είναι ότι τα

$$e - x_1, m_1 - x_2, m_2 - v \cdot x_3, v' - x_4$$

θα πρέπει να αποτελούν διακριτούς λογαρίθμους του 1 ως προς τις βάσεις $A', R_1, R_2, S \in QR_n^* - \{1\}$ αντίστοιχα. Επειδή ο Prover δε γνωρίζει τα p', q', αφού αυτά κρατούνται μυστικά από την εκδότρια Αρχή, τότε σύμφωνα με την Πρόταση 21 θα ήταν πάρα πολύ δύσκολο να βρει μία μη μηδενική τετράδα διακριτών λογαρίθμων του 1 ως προς τις βάσεις A', R_1, R_2, S, ώστε αρχικά να τη δοκιμάσει εάν θα μπορούσε να αποτελέσει τιμή της τετράδας

$$\left(e - x_1, m_1 - x_2, m_2 - v \cdot x_3, v' - x_4\right)$$

και αν ναι μετά να δοκιμάσει αν τα x_1, x_2, x_3, x_4 που θα είχε υπολογίσει ικανοποιούσαν την (107). Από την άλλη αν επέλεγε να δοκιμάσει την ίδια την μηδενική τετράδα $(0,0,0,0)$, θα διαπίστωνε πως δε θα μπορούσε να αποτελέσει τιμή της

$$\left(e - x_1, m_1 - x_2, m_2 - v \cdot x_3, v' - x_4\right),$$

καθώς θα ήταν αδύνατο να ισχύσει

$$\begin{cases} e - x_1 = 0 \\ m_1 - x_2 = 0 \\ m_2 - v \cdot x_3 = 0 \\ v' - x_4 = 0 \end{cases}$$

και άρα

$$m_2 = v \cdot x_3,$$

αφού δεν υπάρχει $x_3 \in \mathbb{Z}^*$ που να ικανοποιεί την τελευταία εξίσωση όπως αναφέρθηκε προηγούμενα. Επομένως ο Prover δε θα μπορούσε να υπολογίσει κάποια $x_1, x_2, x_3, x_4 \in \mathbb{Z}^*$ που να τηρούσαν την παραπάνω συνθήκη ώστε μετά να δοκιμάσει αν αυτά ικανοποιούσαν την (107). Έτσι αν ακολουθούσε τη δεύτερη εναλλακτική

οδό, σχεδόν κατά 100% δε θα μπορούσε να λάβει γνώση κάποιων διακριτών λογαρίθμων του Z ως προς τις βάσεις A', R_1, R, S.

Ένας τρίτος τρόπος θα ήταν να βρει ένα τέτοιο $r \in \mathbb{Z}^*$ ώστε να ισχύει η σχέση

$$R = \left(R_2 \cdot \left(S^{-1} \right)^r \right) \bmod n \ (108).$$

Μετά θα υπολόγιζε το v'' από την εξίσωση

$$v'' = v' + m_2 \cdot r \ (109).$$

Τότε από την (108) συνεπάγεται ότι

$$R^{m_2} \equiv \left(R_2 \cdot S^{-r} \right)^{m_2} \bmod n \Rightarrow R^{m_2} \equiv \left({R_2}^{m_2} \cdot \left(S^{-r} \right)^{m_2} \right) \bmod n \Rightarrow$$

$$\left(A'^e \cdot {R_1}^{m_1} \cdot R^{m_2} \right) \equiv \left(A'^e \cdot {R_1}^{m_1} \cdot {R_2}^{m_2} \cdot S^{-r \cdot m_2} \right) \bmod n.$$

Από την (109) προκύπτει ότι

$$-m_2 \cdot r = v' - v''$$

και άρα η τελευταία ισοδυναμία συνεπάγεται πως

$$\left(A'^e \cdot {R_1}^{m_1} \cdot R^{m_2} \right) \equiv \left(A'^e \cdot {R_1}^{m_1} \cdot {R_2}^{m_2} \cdot S^{v'-v''} \right) \bmod n \Rightarrow$$

$$\left(A'^e \cdot {R_1}^{m_1} \cdot R^{m_2} \right) \equiv \left(A'^e \cdot {R_1}^{m_1} \cdot {R_2}^{m_2} \cdot S^{v'} \cdot S^{-v''} \right) \bmod n \Rightarrow$$

$$\left(A'^e \cdot {R_1}^{m_1} \cdot R^{m_2} \cdot S^{v''} \right) \equiv \left(A'^e \cdot {R_1}^{m_1} \cdot {R_2}^{m_2} \cdot S^{v'} \right) \bmod n \xrightarrow{(101)}$$

$$Z = \left(A'^e \cdot {R_1}^{m_1} \cdot R^{m_2} \cdot S^{v''} \right) \bmod n.$$

Από την τελευταία εξίσωση προκύπτει πως τα e, m_1, m_2, v'' είναι διακριτοί λογάριθμοι του Z ως προς τις βάσεις A', R_1, R, S αντίστοιχα και ταυτόχρονα αυτοί που θα μάθαινε ο Prover αν ακολουθούσε τον τρίτο τρόπο. Επειδή όμως από την (108) συνεπάγεται ότι

$$\left(R \cdot {R_2}^{-1} \right) \equiv \left(S^{-1} \right)^r \bmod n,$$

τότε ο Prover προκειμένου να βρει το r θα έπρεπε να υπολογίσει έναν διακριτό λογάριθμο του $R \cdot {R_2}^{-1}$ ως προς τη βάση S^{-1}, κάτι που σύμφωνα με τον Πρώτο Ισχυρισμό Διακριτού Λογαρίθμου θα ήταν πάρα πολύ δύσκολο. Έτσι ενώ θα ήξερε τους τρεις πρώτους λογαρίθμους e, m_1, m_2, δε θα μπορούσε σχεδόν σίγουρα να γνωρίζει το v'' αφού θα αδυνατούσε να το υπολογίσει από την (109) στην οποία θα του ήταν σχεδόν κατά 100% άγνωστο το r, σε αντίθεση με τα γνωστά v', m_2.

Συνεπώς σχεδόν σίγουρα με κανέναν τρόπο δε θα μπορούσε ο Prover να λάβει γνώση κάποιων διακριτών λογαρίθμων του Z ως προς τις βάσεις A', R_1, R, S και έτσι ο παραπάνω ισχυρισμός που τέθηκε δεν αληθεύει σχεδόν κατά 100%. Επομένως όταν η δεδομένη τιμή δεν είναι ίδια με αυτήν που έχει το συγκεκριμένο πεδίο του πιστοποιητικού, ο Prover σχεδόν σίγουρα δε γνωρίζει διακριτούς λογαρίθμους του Z ως προς τις βάσεις A', R_1, R, S. Εφόσον σύμφωνα με την υπόθεση τηρείται το παρών πρωτόκολλο, ο Prover θα εκτελέσει κανονικά όπως προβλέπεται με τον Verifier το πρωτόκολλο γνώσης διακριτών λογαρίθμων του Z ως προς τις παραπάνω βάσεις και το αποτέλεσμα θα είναι σχεδόν 100% ανεπιτυχές για τον ίδιο.

3. <u>Η δεδομένη τιμή δεν περιέχεται στο συγκεκριμένο πεδίο του πιστοποιητικού και ο Prover επιλέγει να μην τηρήσει το πρωτόκολλο</u>

Σε αυτήν την περίπτωση ο Prover ενεργεί έτσι προκειμένου να ξεγελάσει τον Verifier ώστε να τον πείσει για τον ψευδή ισχυρισμό του. Η μόνη δυνατότητα που έχει για να λειτουργήσει αντικανονικά είναι να μην εκτελέσει όπως προβλέπεται το πρωτόκολλο

γνώσης διακριτών λογαρίθμων του Z ως προς τις βάσεις A', R_1, R, S. Αν το εκτελούσε κανονικά, τότε όπως αναφέρθηκε προηγούμενα το αποτέλεσμα θα ήταν για τον ίδιο ανεπιτυχές αφού η δεδομένη τιμή δεν περιέχεται στο συγκεκριμένο πεδίο του πιστοποιητικού. Θα μπορούσε επομένως να αλλοιώσει κάποια από τα Z, A', R_1, R, S ώστε να εκτελέσει αυτό το πρωτόκολλο με διαφορετικές παραμέτρους που θα του εξασφάλιζαν το επιτυχές για αυτόν αποτέλεσμα. Όμως και οι πέντε προηγούμενες παράμετροι είναι γνωστές στον Verifier, τα Z, R_1, S ως μέρος του δημοσίου κλειδιού της εκδότριας Αρχής, το A' από το πρωτόκολλο εγκυρότητας πιστοποιητικού που εκτέλεσε προηγούμενα με τον Prover και το R επειδή το υπολόγισε ο ίδιος από τη σχέση (103). Έτσι όταν του κοινοποιηθούν οι αλλοιωμένες παράμετροι από τον Prover στην αρχή της εκτέλεσης του πρωτοκόλλου γνώσης διακριτών λογαρίθμων, αυτός θα τις εντοπίσει, θα καταλάβει ότι αυτό δεν τηρείται από τον Prover και θα διακόψει τη συμμετοχή του σε αυτό μην μπορώντας στο τέλος να διαπιστώσει εάν ο ισχυρισμός του Prover είναι αληθής.
Έτσι στην περίπτωση που η δεδομένη τιμή δεν περιέχεται στο συγκεκριμένο πεδίο του πιστοποιητικού και ο Prover επιλέξει να μην τηρήσει το πρωτόκολλο που εξετάζεται στην παρούσα υποενότητα, δε θα καταφέρει να εκτελέσει επιτυχώς το πρωτόκολλο γνώσης διακριτών λογαρίθμων του Z ως προς τις βάσεις A', R_1, R, S.

Συνεπώς από την παρούσα απόδειξη προκύπτει πως μόνο όταν η δεδομένη τιμή περιέχεται στο συγκεκριμένο πεδίο του έγκυρου πιστοποιητικού του Prover και το πρωτόκολλο τηρηθεί, ο ίδιος μπορεί να πείσει σίγουρα τον Verifier ότι γνωρίζει διακριτούς λογαρίθμους του Z ως προς τις βάσεις A', R_1, R, S. Διαφορετικά η πιθανότητα να πειστεί ο Verifier είναι εξαιρετικά μικρή. Αυτό σημαίνει πως η απόδειξη γνώσης τέτοιων λογαρίθμων από τον Prover αποτελεί σχεδόν κατά 100% και απόδειξη ότι η δεδομένη τιμή είναι αυτή που έχει το συγκεκριμένο πεδίο του έγκυρου πιστοποιητικού του.

4. <u>Εμπιστευτικότητα πληροφορίας</u>

Όπως αναφέρθηκε στην εισαγωγή αυτής της υποενότητας, η τιμή αυτού του πεδίου είναι η πληροφορία που αποκαλύπτεται στον Verifier όταν είναι ίση με τη δεδομένη τιμή, καθώς η συγκεκριμένη ισότητα αποδεικνύεται σε αυτόν με την εκτέλεση του παρόντος πρωτοκόλλου. Στην περίπτωση που δεν αποδεικνύεται, τότε αυτή η πληροφορία δεν μπορεί να γίνει γνωστή στον Verifier. Από την μία δεν μαθαίνει άμεσα από τον Prover την τιμή του συγκεκριμένου πεδίου και από την άλλη δεν μπορεί να λάβει γνώση αυτής της τιμής έμμεσα από τον πρώτο αριθμό στον οποίο αντιστοιχίζεται. Αν ήξερε αυτόν τον αριθμό θα μπορούσε να χρησιμοποιήσει τη δημοσιοποιημένη λίστα των κωδικών των τιμών των πεδίων της Αρχής προκειμένου μέσω αυτού να βρει την τιμή του συγκεκριμένου πεδίου. Όμως αφενός δεν τον μαθαίνει άμεσα από τον Prover και αφετέρου δεν μπορεί να τον πληροφορηθεί έμμεσα υπολογίζοντάς τον. Πράγματι, ξέροντας όλες τις δυνατές τιμές που μπορεί να λάβει το συγκεκριμένο πεδίο, θα μπορούσε αρχικά να επιλέξει από την προηγούμενη λίστα τους πρώτους αριθμούς που αντιστοιχούν σε αυτές. Ύστερα θα επιχειρούσε να διαιρέσει το m_2 με τον καθέναν από αυτούς και για εκείνον τον πρώτο αριθμό που θα το διαιρούσε ακριβώς θα συμπέραινε ότι αποτελεί πρώτο παράγοντά του και άρα η τιμή η οποία θα αντιστοιχιζόταν σε αυτόν θα ήταν αυτή που θα είχε το συγκεκριμένο πεδίο του πιστοποιητικού. Όμως απαραίτητη προϋπόθεση θα ήταν η γνώση του m_2 την οποία δε θα μπορούσε να έχει, καθώς όταν προηγουμένως στα πλαίσια της εκτέλεσης του πρωτοκόλλου εγκυρότητας πιστοποιητικού εκτέλεσε με τον Prover το

πρωτόκολλο γνώσης διακριτών λογαρίθμων του Z ως προς τα A', R_1, R_2, S, δεν ήταν δυνατό να πληροφορηθεί τους διακριτούς λογαρίθμους που ξέρει ο Prover ως προς τις τέσσερις αυτές βάσεις, άρα και τον m_2 ως προς το R_2.

5.5.1. Zkp Πρωτόκολλο Πεδίων με Τιμές Ίσες με κάποιες Δεδομένες Τιμές

[6] Στην υποενότητα αυτή παρουσιάζεται ένα zkp πρωτόκολλο που αποτελεί επέκταση αυτού της προηγούμενης υποενότητας. Ο Prover το χρησιμοποιεί για να πείσει τον Verifier ότι οι τιμές περισσότερων του ενός πεδίων του έγκυρου πιστοποιητικού που κατέχει είναι ίσες με κάποιες δεδομένες τιμές. Οι τιμές αυτών των πεδίων είναι η πληροφορία που σχετίζεται με τον προηγούμενο ισχυρισμό και στην περίπτωση που αυτός είναι αληθής δε θα παραμείνουν μυστικές στον Verifier, καθώς μετά την εκτέλεση του συγκεκριμένου πρωτοκόλλου θα αποδειχτεί σε αυτόν ότι είναι ίσες με τις δεδομένες τιμές. Στην περίπτωση που ο Prover δεν καταφέρει να αποδείξει το αληθές του ισχυρισμού του, τότε οι τιμές των συγκεκριμένων πεδίων πρέπει να συνεχίσουν να παραμένουν μυστικές στον Verifier κατά τη διάρκεια και μετά το τέλος της εκτέλεσης του πρωτοκόλλου. Όπως αναφέρθηκε στο τέλος της ενότητας 5, θεωρείται πως πριν την εκτέλεση του παρόντος πρωτοκόλλου έχει ήδη αποδειχτεί η εγκυρότητα του πιστοποιητικού του Prover μέσω του πρωτοκόλλου εγκυρότητας πιστοποιητικού, το οποίο παρουσιάστηκε και αναλύθηκε στην υποενότητα 5.4. Ένα παράδειγμα χρήσης του παρόντος πρωτοκόλλου θα ήταν η περίπτωση στην οποία ο ισχυρισμός θα είχε ως εξής: '*τα πεδία του επιπέδου μόρφωσης και οικογενειακής κατάστασης έχουν τιμές 'Πανεπιστήμιο' και 'Άγαμος' αντίστοιχα*'. Οι δεδομένες τιμές σε αυτήν την περίπτωση είναι οι '*Πανεπιστήμιο*' και '*Άγαμος*'. Το πρωτόκολλο και η απόδειξη ότι πετυχαίνει τον σκοπό του παρουσιάζονται παρακάτω.

- Verifier
  - $\forall i \in \{1,..,k\}$, όπου $k \in \mathbb{N}^* - \{1\}$ είναι ο αριθμός των δεδομένων τιμών, επιλέγει από τη δημοσιοποιημένη λίστα των κωδικών των τιμών των πεδίων της Αρχής τον πρώτο αριθμό v_i που αντιστοιχεί στην iοστή δεδομένη τιμή την οποία ο Prover θέλει να αποδείξει ότι είναι η τιμή ενός συγκεκριμένου πεδίου του πιστοποιητικού του.
  - Υπολογίζει $R = R_2^{\prod_{i=1}^{k} v_i} \bmod n$, όπου θεωρείται πως $R \neq 1$.
  - Στέλνει στον Prover το R.
- Prover
  - $\forall i \in \{1,..,k\}$ επιλέγει από τη δημοσιοποιημένη λίστα των κωδικών των τιμών των πεδίων της Αρχής τον πρώτο αριθμό v_i.
  - Υπολογίζει $d = \frac{m_2}{\prod_{i=1}^{k} v_i}$, όπου m_2 είναι το γινόμενο των πρώτων αριθμών στους οποίους είναι κωδικοποιημένες οι τιμές των πεδίων του πιστοποιητικού του.

- Εκτελεί με τον Verifier το πρωτόκολλο γνώσης διακριτών λογαρίθμων του Z ως προς τις βάσεις A', R_1, R, S, όπου A' είναι υπολογισμένο από το πρωτόκολλο εγκυρότητας πιστοποιητικού που εκτέλεσε προηγούμενα με τον Verifier για να αποδείξει ότι κατέχει ένα έγκυρο πιστοποιητικό.

- Verifier
  - Αν αποδειχτεί ότι ο Prover γνωρίζει διακριτούς λογαρίθμους του Z ως προς τις βάσεις A', R_1, R, S, τότε αυτός κατέχει ένα έγκυρο πιστοποιητικό όπου οι τιμές των k συγκεκριμένων πεδίων του είναι ίσες με τις k δεδομένες τιμές.

Απόδειξη

Αν οι k τιμές των συγκεκριμένων πεδίων του έγκυρου πιστοποιητικού του Prover είναι οι ίδιες με τις k δεδομένες τιμές, τότε $\forall i \in \{1,..,k\}$ στο γινόμενο m_2 των πρώτων αριθμών στους οποίους είναι κωδικοποιημένες οι τιμές των πεδίων του πιστοποιητικού, θα περιέχεται ως παράγοντάς του ο πρώτος αριθμός v_i που αντιστοιχεί στην i οστή δεδομένη τιμή, δηλαδή θα $\exists d_i \in \mathbb{Z}^*$ ώστε να είναι

$$m_2 = v_i \cdot d_i .$$

Επειδή τα v_i είναι πρώτοι αριθμοί διαφορετικοί μεταξύ τους, τότε λόγω των τελευταίων εξισώσεων και της Πρότασης 6 θα $\exists d \in \mathbb{Z}^*$ ώστε να ισχύει

$$m_2 = \left(\prod_{i=1}^{k} v_i \right) \cdot d .$$

Η απόδειξη του παρόντος πρωτοκόλλου είναι παρόμοια με αυτήν που δόθηκε στην προηγούμενη υποενότητα.

5.6. Πρώτο Zkp Πρωτόκολλο Πεδίου με Τιμή Διαφορετική από μια Δεδομένη Τιμή

Στην υποενότητα αυτή παρουσιάζεται και αναλύεται η πρώτη έκδοση ενός zkp πρωτοκόλλου το οποίο χρησιμοποιεί ο Prover για να πείσει τον Verifier ότι η τιμή ενός πεδίου του έγκυρου πιστοποιητικού που κατέχει είναι διαφορετική από μια δεδομένη τιμή. Η τιμή αυτού του πεδίου είναι η πληροφορία που σχετίζεται με τον προηγούμενο ισχυρισμό και θα πρέπει να συνεχίσει να παραμένει μυστική στον Verifier κατά τη διάρκεια και μετά το τέλος της εκτέλεσης του συγκεκριμένου πρωτοκόλλου. Όπως αναφέρθηκε στο τέλος της ενότητας 5, θεωρείται πως πριν την εκτέλεση του παρόντος πρωτοκόλλου έχει ήδη αποδειχτεί η εγκυρότητα του πιστοποιητικού του Prover μέσω του πρωτοκόλλου εγκυρότητας πιστοποιητικού. Ένα παράδειγμα χρήσης του παρόντος πρωτοκόλλου θα ήταν η περίπτωση στην οποία ο ισχυρισμός θα είχε ως εξής: '*το πεδίο του επιπέδου μόρφωσης δεν έχει την τιμή 'Πανεπιστήμιο''*. Η δεδομένη τιμή σε αυτήν την περίπτωση είναι η τιμή '*Πανεπιστήμιο*'. Το πρωτόκολλο και η απόδειξη ότι πετυχαίνει τον σκοπό του παρουσιάζονται παρακάτω.

- Verifier
  - Επιλέγει από τη δημοσιοποιημένη λίστα των κωδικών των τιμών των πεδίων της Αρχής τον πρώτο αριθμό v που αντιστοιχεί στη δεδομένη

τιμή την οποία ο Prover θέλει να αποδείξει ότι δεν είναι η τιμή ενός συγκεκριμένου πεδίου του πιστοποιητικού του.

- Υπολογίζει $\begin{cases} R_2^{-1} \\ R = \left(R_2^{-1}\right)^{v} \bmod n \end{cases}$ (110), όπου θεωρείται πως $R \neq 1$.
- Στέλνει στον Prover το R.

- Prover
  - Επιλέγει από τη δημοσιοποιημένη λίστα των κωδικών των τιμών των πεδίων της Αρχής τον πρώτο αριθμό v.
  - [6] Υπολογίζει R_2^{-1} και $x, y \in \mathbb{Z}^*$ τέτοια ώστε $v \cdot x + m_2 \cdot y = 1$ (111), όπου m_2 είναι το γινόμενο των πρώτων αριθμών στους οποίους είναι κωδικοποιημένες οι τιμές των πεδίων του πιστοποιητικού του. Ο υπολογισμός των x, y γίνεται εκτελώντας τον επεκτεινόμενο Ευκλείδειο αλγόριθμο με εισόδους τα v, m_2.
  - Υπολογίζει $\begin{cases} -y \\ e \cdot y \\ m_1 \cdot y \\ v' \cdot y \end{cases}$, όπου e είναι η μία από τις τρεις παραμέτρους της υπογραφής του πιστοποιητικού, m_1 είναι ο κώδικάς του που υπολόγισε ο ίδιος κατά τη φάση της επιβεβαίωσης και v' είναι υπολογισμένο από το πρωτόκολλο εγκυρότητας πιστοποιητικού που εκτέλεσε προηγούμενα με τον Verifier για να αποδείξει ότι κατέχει ένα έγκυρο πιστοποιητικό.
  - Εκτελεί με τον Verifier το πρωτόκολλο γνώσης διακριτών λογαρίθμων του R_2^{-1} ως προς τις βάσεις Z, A', R_1, R, S, όπου A' είναι υπολογισμένο από το πρωτόκολλο εγκυρότητας πιστοποιητικού.

- Verifier
  - Αν αποδειχτεί ότι ο Prover γνωρίζει διακριτούς λογαρίθμους του R_2^{-1} ως προς τις βάσεις Z, A', R_1, R, S, τότε αυτός κατέχει ένα έγκυρο πιστοποιητικό όπου η τιμή του συγκεκριμένου πεδίου του δεν είναι ίση με τη δεδομένη τιμή.

Απόδειξη

Εφόσον ο Prover προηγουμένως εκτέλεσε με επιτυχία το πρωτόκολλο εγκυρότητας πιστοποιητικού, τότε θα ισχύει

$$Z = \left(A'^{e} \cdot R_1^{m_1} \cdot R_2^{m_2} \cdot S^{v'}\right) \bmod n \ (101).$$

1. Η τιμή του συγκεκριμένου πεδίου του έγκυρου πιστοποιητικού του Prover δεν είναι ίση με τη δεδομένη τιμή και το πρωτόκολλο τηρείται

Σε αυτήν την περίπτωση στο γινόμενο m_2 των πρώτων αριθμών στους οποίους είναι κωδικοποιημένες οι τιμές των πεδίων του πιστοποιητικού, δε θα περιέχεται ως πρώτος παράγοντάς του ο πρώτος αριθμός v που αντιστοιχεί στη δεδομένη τιμή και επομένως δε θα το διαιρεί. Εφόσον ο πρώτος v δεν είναι διαιρέτης του m_2, τότε

σύμφωνα με την Πρόταση 1 οι δύο αυτοί αριθμοί είναι πρώτοι μεταξύ τους και άρα λόγω της Πρότασης 3 θα $\exists x, y \in \mathbb{Z}^*$ ώστε να ισχύει

$$v \cdot x + m_2 \cdot y = 1 \text{ (111)}.$$

Ο Prover μπορεί να υπολογίσει τα x, y εφόσον γνωρίζει τα v, m_2. Τα x, y είναι διαφορετικά του 0 γιατί αλλιώς από την (111) θα πρόεκυπτε ότι το v ή το m_2 θα ήταν ίσο με 1 ή -1, κάτι που δεν ισχύει αφού αυτά είναι μεγαλύτερα του 1. Αφού $y \neq 0$, τότε από την (111) συνεπάγεται ότι

$$m_2 \cdot y = 1 - v \cdot x \Rightarrow m_2 = \frac{1 - v \cdot x}{y}$$

και συνεπώς η (101) συνεπάγεται

$$Z = \left(A'^e \cdot R_1^{m_1} \cdot R_2^{\frac{1-v\cdot x}{y}} \cdot S^{v'} \right) \bmod n \Rightarrow Z^y \equiv \left(A'^e \cdot R_1^{m_1} \cdot R_2^{\frac{1-v\cdot x}{y}} \cdot S^{v'} \right)^y \bmod n =$$

$$\left(\left(A'^e\right)^y \cdot \left(R_1^{m_1}\right)^y \cdot \left(R_2^{\frac{1-v\cdot x}{y}} \right)^y \cdot \left(S^{v'}\right)^y \right) \bmod n = \left(A'^{e\cdot y} \cdot R_1^{m_1 \cdot y} \cdot R_2^{\frac{(1-v\cdot x)}{y}\cdot y} \cdot S^{v'\cdot y} \right) \bmod n =$$

$$\left(A'^{e\cdot y} \cdot R_1^{m_1 \cdot y} \cdot R_2^{1-v\cdot x} \cdot S^{v'\cdot y} \right) \bmod n \Rightarrow Z^y \equiv \left(A'^{e\cdot y} \cdot R_1^{m_1 \cdot y} \cdot R_2 \cdot R_2^{-v\cdot x} \cdot S^{v'\cdot y} \right) \bmod n \Rightarrow$$

$$\left(R_2^{-1} \cdot Z^y \right) \equiv \left(A'^{e\cdot y} \cdot R_1^{m_1 \cdot y} \cdot R_2^{-v\cdot x} \cdot S^{v'\cdot y} \right) \bmod n \Rightarrow$$

$$R_2^{-1} = \left(Z^{-y} \cdot A'^{e\cdot y} \cdot R_1^{m_1 \cdot y} \cdot R_2^{-v\cdot x} \cdot S^{v'\cdot y} \right) \bmod n \text{ (112)},$$

αφού $R_2^{-1} \in QR_n^*$ και άρα $R_2^{-1} \in \mathbb{Z}_n^*$, οπότε $R_2^{-1} < n$. Από την (110) συνεπάγεται ότι

$$R \equiv R_2^{-v} \bmod n \Rightarrow R^x \equiv \left(R_2^{-v} \right)^x \bmod n \Rightarrow R^x \equiv R_2^{-v\cdot x} \bmod n \Rightarrow$$

$$\left(Z^{-y} \cdot A'^{e\cdot y} \cdot R_1^{m_1 \cdot y} \cdot R^x \cdot S^{v'\cdot y} \right) \equiv \left(Z^{-y} \cdot A'^{e\cdot y} \cdot R_1^{m_1 \cdot y} \cdot R_2^{-v\cdot x} \cdot S^{v'\cdot y} \right) \bmod n \xrightarrow{(112)}$$

$$R_2^{-1} = \left(Z^{-y} \cdot A'^{e\cdot y} \cdot R_1^{m_1 \cdot y} \cdot R^x \cdot S^{v'\cdot y} \right) \bmod n \text{ (113)}.$$

Ο Prover μπορεί να υπολογίσει τα

$$-y, e \cdot y, m_1 \cdot y, v' \cdot y,$$

εφόσον γνωρίζει τα e, m_1, v' και έχει υπολογίσει από πριν το y και έτσι να μάθει στην (113) διακριτούς λογαρίθμους του R_2^{-1} ως προς τα Z, A', R_1, S αντίστοιχα. Επίσης έχει υπολογίσει από πριν το x, οπότε στην ίδια εξίσωση γνωρίζει και έναν διακριτό λογάριθμο του R_2^{-1} ως προς το R, το οποίο ήδη το πληροφορήθηκε από τον Verifier. Εφόσον $R_2^{-1} \in QR_n^*$, σύμφωνα με την (110) και την Πρόταση 20.2 θα ισχύει $R \in QR_n^*$ και επειδή $R \neq 1$, τότε $R \in QR_n^* - \{1\}$. Από τη στιγμή που ξέρει διακριτούς λογαρίθμους του R_2^{-1} ως προς τις βάσεις $Z, A', R_1, R, S \in QR_n^* - \{1\}$, θα αποδείξει τη γνώση του αυτή στον Verifier όταν και οι δύο χρησιμοποιήσουν το zkp πρωτόκολλο γνώσης διακριτών λογαρίθμων. Η απόδειξη αυτή θα γίνει χωρίς να αποκαλυφθούν άμεσα ή έμμεσα στον Verifier οι συγκεκριμένοι διακριτοί λογάριθμοι.

2. <u>Η δεδομένη τιμή είναι ίδια με αυτήν που έχει το συγκεκριμένο πεδίο του έγκυρου πιστοποιητικού του Prover και το πρωτόκολλο τηρείται</u>

Σε αυτήν την περίπτωση ο πρώτος αριθμός v στον οποίο αντιστοιχίζεται η δεδομένη τιμή είναι πρώτος παράγοντας του γινομένου m_2 και άρα διαιρέτης του. Η αντιθετοαντίστροφη πρόταση του ευθύ της Πρότασης 1 διατυπώνεται ως εξής: αν ο

πρώτος αριθμός p είναι διαιρέτης του $n \in \mathbb{N}$, τότε οι p, n δεν είναι πρώτοι μεταξύ τους. Άρα τα v, m_2 δεν είναι πρώτοι μεταξύ τους. Επίσης η αντιθετοαντίστροφη πρόταση του αντιστρόφου της Πρότασης 3 διατυπώνεται ως εξής: αν οι $a, b \in \mathbb{N}$ δεν είναι πρώτοι μεταξύ τους, τότε δεν $\exists x, y \in \mathbb{Z}$ ώστε

$$a \cdot x + b \cdot y = 1.$$

Άρα για τα v, m_2 που δεν είναι πρώτοι μεταξύ τους θα ισχύει το ίδιο. Από τη στιγμή που ο Prover αδυνατεί να βρει κάποια $x, y \in \mathbb{Z}^*$ ώστε να ισχύει

$$v \cdot x + m_2 \cdot y = 1 \quad (111)$$

όπως έκανε πριν, δε θα μπορέσει να ακολουθήσει την προηγούμενη διαδικασία προκειμένου να πληροφορηθεί διακριτούς λογαρίθμους του R_2^{-1} ως προς τις βάσεις Z, A', R_1, R, S. Θα δειχτεί ότι σχεδόν κατά 100% αυτός δε γνωρίζει τέτοιους λογαρίθμους. Τίθεται ο ισχυρισμός πως γνωρίζει κάποιους.
Σχεδόν σίγουρα η γνώση αυτών δε θα προήλθε προσπαθώντας ο ίδιος να λύσει την εξίσωση

$$R_2^{-1} = \left(Z^{x_1} \cdot A'^{x_2} \cdot R_1^{x_3} \cdot R^{x_4} \cdot S^{x_5}\right) \bmod n \quad (114)$$

ως προς $x_1, x_2, x_3, x_4, x_5 \in \mathbb{Z}^*$, καθώς κάτι τέτοιο θα ήταν πάρα πολύ δύσκολο σύμφωνα με το Δεύτερο Ισχυρισμό Διακριτού Λογαρίθμου.
Λαμβάνοντας υπόψη του ότι ισχύει η (110), αφού σύμφωνα με την υπόθεση το πρωτόκολλο τηρείται και άρα ο Verifier θα υπολόγισε σωστά το R από αυτήν τη σχέση, αλλά και ότι είναι κάτοχος έγκυρου πιστοποιητικού και ισχύει επίσης η (101), μια δεύτερη εναλλακτική οδός που πιθανόν θα τον οδηγούσε στη γνώση αυτών των λογαρίθμων θα ήταν να ακολουθούσε τις παρακάτω συνεπαγωγές προκειμένου να συμπεράνει τη συνθήκη που θα έπρεπε να τηρούν τα x_1, x_2, x_3, x_4, x_5. Από την (110) συνεπάγεται πως

$$R^{x_4} \equiv \left(R_2^{-v}\right)^{x_4} \bmod n \Rightarrow R^{x_4} \equiv R_2^{-v \cdot x_4} \bmod n \Rightarrow$$
$$\left(Z^{x_1} \cdot A'^{x_2} \cdot R_1^{x_3} \cdot R^{x_4} \cdot S^{x_5}\right) \equiv \left(Z^{x_1} \cdot A'^{x_2} \cdot R_1^{x_3} \cdot R_2^{-v \cdot x_4} \cdot S^{x_5}\right) \bmod n \xrightarrow{(114)}$$
$$R_2^{-1} = \left(Z^{x_1} \cdot A'^{x_2} \cdot R_1^{x_3} \cdot R_2^{-v \cdot x_4} \cdot S^{x_5}\right) \bmod n \Rightarrow$$
$$\left(R_2^{-1} \cdot Z^{-x_1}\right) \equiv \left(A'^{x_2} \cdot R_1^{x_3} \cdot R_2^{-v \cdot x_4} \cdot S^{x_5}\right) \bmod n \Rightarrow$$
$$Z^{-x_1} \equiv \left(A'^{x_2} \cdot R_1^{x_3} \cdot R_2 \cdot R_2^{-v \cdot x_4} \cdot S^{x_5}\right) \bmod n \Rightarrow$$
$$Z^{-x_1} \equiv \left(A'^{x_2} \cdot R_1^{x_3} \cdot R_2^{1-v \cdot x_4} \cdot S^{x_5}\right) \bmod n \quad (115).$$

Η (101) συνεπάγεται ότι

$$Z^{-x_1} \equiv \left(A'^{e} \cdot R_1^{m_1} \cdot R_2^{m_2} \cdot S^{v'}\right)^{-x_1} \bmod n = \left(\left(A'^{e}\right)^{-x_1} \cdot \left(R_1^{m_1}\right)^{-x_1} \cdot \left(R_2^{m_2}\right)^{-x_1} \cdot \left(S^{v'}\right)^{-x_1}\right) \bmod n \Rightarrow$$
$$Z^{-x_1} \equiv \left(A'^{-e \cdot x_1} \cdot R_1^{-m_1 \cdot x_1} \cdot R_2^{-m_2 \cdot x_1} \cdot S^{-v' \cdot x_1}\right) \bmod n \xrightarrow{(115)}$$
$$\left(A'^{x_2} \cdot R_1^{x_3} \cdot R_2^{1-v \cdot x_4} \cdot S^{x_5}\right) \equiv \left(A'^{-e \cdot x_1} \cdot R_1^{-m_1 \cdot x_1} \cdot R_2^{-m_2 \cdot x_1} \cdot S^{-v' \cdot x_1}\right) \bmod n \Rightarrow$$
$$\left(A'^{x_2} \cdot R_1^{x_3} \cdot R_2^{1-v \cdot x_4} \cdot S^{x_5} \cdot A'^{e \cdot x_1} \cdot R_1^{m_1 \cdot x_1} \cdot R_2^{m_2 \cdot x_1} \cdot S^{v' \cdot x_1}\right) \equiv 1 \bmod n \Rightarrow$$
$$\left(A'^{x_2 + e \cdot x_1} \cdot R_1^{x_3 + m_1 \cdot x_1} \cdot R_2^{1-v \cdot x_4 + m_2 \cdot x_1} \cdot S^{x_5 + v' \cdot x_1}\right) \equiv 1 \bmod n.$$

Από την τελευταία ισοδυναμία προκύπτει πως η συνθήκη που πρέπει να ικανοποιούν τα x_1, x_2, x_3, x_4, x_5 είναι ότι τα

$$x_2 + e \cdot x_1, x_3 + m_1 \cdot x_1, 1 - v \cdot x_4 + m_2 \cdot x_1, x_5 + v' \cdot x_1$$

θα πρέπει να αποτελούν διακριτούς λογαρίθμους του 1 ως προς τις βάσεις $A', R_1, R_2, S \in QR_n^* - \{1\}$ αντίστοιχα. Επειδή ο Prover δε γνωρίζει τα p', q', αφού αυτά κρατούνται μυστικά από την εκδότρια Αρχή, τότε σύμφωνα με την Πρόταση 21 θα ήταν πάρα πολύ δύσκολο να βρει μία μη μηδενική τετράδα διακριτών λογαρίθμων του 1 ως προς τις βάσεις A', R_1, R_2, S, ώστε αρχικά να τη δοκιμάσει εάν θα μπορούσε να αποτελέσει τιμή της τετράδας

$$\left(x_2 + e \cdot x_1, x_3 + m_1 \cdot x_1, 1 - v \cdot x_4 + m_2 \cdot x_1, x_5 + v' \cdot x_1\right)$$

και αν ναι μετά να δοκιμάσει αν τα x_1, x_2, x_3, x_4, x_5 που θα είχε υπολογίσει ικανοποιούσαν την (114). Από την άλλη αν επέλεγε να δοκιμάσει την ίδια την μηδενική τετράδα $(0,0,0,0)$, θα διαπίστωνε πως δε θα μπορούσε να αποτελέσει τιμή της

$$\left(x_2 + e \cdot x_1, x_3 + m_1 \cdot x_1, 1 - v \cdot x_4 + m_2 \cdot x_1, x_5 + v' \cdot x_1\right),$$

καθώς θα ήταν αδύνατο να ισχύσει

$$\begin{cases} x_2 + e \cdot x_1 = 0 \\ x_3 + m_1 \cdot x_1 = 0 \\ 1 - v \cdot x_4 + m_2 \cdot x_1 = 0 \\ x_5 + v' \cdot x_1 = 0 \end{cases}$$

και άρα

$$v \cdot x_4 - m_2 \cdot x_1 = 1 \Rightarrow v \cdot x_4 + m_2 \cdot (-x_1) = 1 \Rightarrow v \cdot x_4 + m_2 \cdot z = 1,$$

όπου $z = -x_1$, $z \in \mathbb{Z}^*$, αφού δεν υπάρχουν $x_4, z \in \mathbb{Z}^*$ που να ικανοποιούν την τελευταία εξίσωση όπως αναφέρθηκε προηγούμενα. Επομένως ο Prover θα δε θα μπορούσε να υπολογίσει κάποια $x_1, x_2, x_3, x_4, x_5 \in \mathbb{Z}^*$ που να τηρούσαν την παραπάνω συνθήκη ώστε μετά να δοκιμάσει αν αυτά ικανοποιούσαν την (114). Έτσι αν ακολουθούσε τη δεύτερη εναλλακτική οδό, σχεδόν κατά 100% δε θα μπορούσε να λάβει γνώση κάποιων διακριτών λογαρίθμων του R_2^{-1} ως προς τις βάσεις Z, A', R_1, R, S.

Ένας τρίτος τρόπος θα ήταν να βρει ένα τέτοιο $r \in \mathbb{Z}^*$ ώστε να ισχύει η σχέση

$$R = \left(R_2 \cdot \left(S^{-1}\right)^r\right) \bmod n \quad (116).$$

Μετά θα υπολόγιζε το v'' από την εξίσωση

$$v'' = v' + m_2 \cdot r \quad (117).$$

Τότε όπως αποδείχτηκε στην απόδειξη της υποενότητας 5.5, θα είναι

$$Z = \left(A'^e \cdot R_1^{m_1} \cdot R^{m_2} \cdot S^{v''}\right) \bmod n.$$

Έστω τυχαίο $x \in \mathbb{Z}^*$, τότε η τελευταία εξίσωση συνεπάγεται ότι

$$Z^x \equiv \left(A'^e \cdot R_1^{m_1} \cdot R^{m_2} \cdot S^{v''}\right)^x \bmod n = \left(\left(A'^e\right)^x \cdot \left(R_1^{m_1}\right)^x \cdot \left(R^{m_2}\right)^x \cdot \left(S^{v''}\right)^x\right) \bmod n \Rightarrow$$

$$Z^x \equiv \left(A'^{e \cdot x} \cdot R_1^{m_1 \cdot x} \cdot R^{m_2 \cdot x} \cdot S^{v'' \cdot x}\right) \bmod n \Rightarrow$$

$$\left(R_2^{-1} \cdot Z^x\right) \equiv \left(A'^{e \cdot x} \cdot R_1^{m_1 \cdot x} \cdot R^{m_2 \cdot x} \cdot R_2^{-1} \cdot S^{v'' \cdot x}\right) \bmod n \quad (118).$$

Από την (116) συνεπάγεται ότι

$$R = \left(R_2 \cdot \left(S^{-1}\right)^r\right) \bmod n \Rightarrow \left(R \cdot R_2^{-1}\right) \equiv S^{-r} \bmod n \Rightarrow R_2^{-1} \equiv \left(R^{-1} \cdot S^{-r}\right) \bmod n \Rightarrow$$

$$\left(A'^{e\cdot x}\cdot R_1^{\,m_1\cdot x}\cdot R^{m_2\cdot x}\cdot R_2^{\,-1}\cdot S^{v''\cdot x}\right)\equiv\left(A'^{e\cdot x}\cdot R_1^{\,m_1\cdot x}\cdot R^{m_2\cdot x}\cdot R^{-1}\cdot S^{-r}\cdot S^{v''\cdot x}\right)\bmod n\xrightarrow{(118)}$$

$$\left(R_2^{\,-1}\cdot Z^{x}\right)\equiv\left(A'^{e\cdot x}\cdot R_1^{\,m_1\cdot x}\cdot R^{m_2\cdot x-1}\cdot S^{v''\cdot x-r}\right)\bmod n\Rightarrow$$

$$R_2^{\,-1}=\left(Z^{-x}\cdot A'^{e\cdot x}\cdot R_1^{\,m_1\cdot x}\cdot R^{m_2\cdot x-1}\cdot S^{v''\cdot x-r}\right)\bmod n\ (119).$$

Η (117) συνεπάγεται ότι

$$v''=v'+m_2\cdot r\Rightarrow v''\cdot x=\left(v'+m_2\cdot r\right)\cdot x\Rightarrow v''\cdot x=v'\cdot x+m_2\cdot r\cdot x\Rightarrow$$

$$v''\cdot x-r=v'\cdot x+m_2\cdot r\cdot x-r\Rightarrow v''\cdot x-r=v'\cdot x+\left(m_2\cdot x-1\right)\cdot r.$$

Λόγω της τελευταίας εξίσωσης η (119) γίνεται

$$R_2^{\,-1}=\left(Z^{-x}\cdot A'^{e\cdot x}\cdot R_1^{\,m_1\cdot x}\cdot R^{m_2\cdot x-1}\cdot S^{v'\cdot x+\left(m_2\cdot x-1\right)\cdot r}\right)\bmod n.$$

Από την τελευταία σχέση προκύπτει πως τα

$$-x,e\cdot x,m_1\cdot x,m_2\cdot x-1,v'\cdot x+\left(m_2\cdot x-1\right)\cdot r$$

αποτελούν διακριτούς λογαρίθμους του $R_2^{\,-1}$ ως προς τις βάσεις Z,A',R_1,R,S αντίστοιχα και ταυτόχρονα αυτούς που θα μάθαινε ο Prover αν ακολουθούσε τον τρίτο τρόπο. Να επισημανθεί πως από τη στιγμή που η τιμή του x μπορεί να είναι οποιαδήποτε στο $\mathbb{Z}^*$, ο Prover θα μάθαινε άπειρες τέτοιες πεντάδες διακριτών λογαρίθμων. Επειδή όμως από την (116) συνεπάγεται ότι

$$R\cdot R_2^{\,-1}\equiv\left(S^{-1}\right)^{r}\bmod n,$$

τότε ο Prover προκειμένου να βρει το r θα έπρεπε να υπολογίσει έναν διακριτό λογάριθμο του $R\cdot R_2^{\,-1}$ ως προς τη βάση S^{-1}, κάτι που σύμφωνα με τον Πρώτο Ισχυρισμό Διακριτού Λογαρίθμου θα ήταν πάρα πολύ δύσκολο. Έτσι ενώ θα ήξερε τους τέσσερις πρώτους λογαρίθμους

$$-x,e\cdot x,m_1\cdot x,m_2\cdot x-1$$

επιλέγοντας ένα οποιοδήποτε $x\in\mathbb{Z}^*$, δε θα μπορούσε σχεδόν σίγουρα να γνωρίζει το

$$v'\cdot x+\left(m_2\cdot x-1\right)\cdot r$$

αφού θα αδυνατούσε να το υπολογίσει καθώς θα του ήταν σχεδόν κατά 100% άγνωστο το r, σε αντίθεση με τα γνωστά v',m_2,x.

Συνεπώς σχεδόν σίγουρα με κανέναν τρόπο δε θα μπορούσε ο Prover να λάβει γνώση κάποιων διακριτών λογαρίθμων του $R_2^{\,-1}$ ως προς τις βάσεις Z,A',R_1,R,S και έτσι ο παραπάνω ισχυρισμός που τέθηκε δεν αληθεύει σχεδόν κατά 100%. Επομένως όταν η δεδομένη τιμή είναι ίδια με αυτήν που έχει το συγκεκριμένο πεδίο του πιστοποιητικού, ο Prover σχεδόν σίγουρα δε γνωρίζει διακριτούς λογαρίθμους του $R_2^{\,-1}$ ως προς τις βάσεις Z,A',R_1,R,S. Εφόσον σύμφωνα με την υπόθεση τηρείται το παρών πρωτόκολλο, ο Prover θα εκτελέσει κανονικά όπως προβλέπεται με τον Verifier το πρωτόκολλο γνώσης διακριτών λογαρίθμων του $R_2^{\,-1}$ ως προς τις παραπάνω βάσεις και το αποτέλεσμα θα είναι σχεδόν 100% ανεπιτυχές για τον ίδιο.

3. <u>Η δεδομένη τιμή περιέχεται στο συγκεκριμένο πεδίο του πιστοποιητικού και ο Prover επιλέγει να μην τηρήσει το πρωτόκολλο</u>

Σε αυτήν την περίπτωση ο Prover ενεργεί έτσι προκειμένου να ξεγελάσει τον Verifier ώστε να τον πείσει για τον ψευδή ισχυρισμό του. Η μόνη δυνατότητα που έχει για να λειτουργήσει αντικανονικά είναι να μην εκτελέσει όπως προβλέπεται το πρωτόκολλο γνώσης διακριτών λογαρίθμων του $R_2^{\,-1}$ ως προς τις βάσεις Z,A',R_1,R,S. Αν το εκτελούσε κανονικά, τότε όπως αναφέρθηκε προηγούμενα το αποτέλεσμα θα ήταν

για τον ίδιο ανεπιτυχές αφού η δεδομένη τιμή περιέχεται στο συγκεκριμένο πεδίο του πιστοποιητικού. Θα μπορούσε επομένως να αλλοιώσει κάποια από τα $R_2^{-1}, Z, A', R_1, R, S$ ώστε να εκτελέσει αυτό το πρωτόκολλο με διαφορετικές παραμέτρους που θα του εξασφάλιζαν το επιτυχές για αυτόν αποτέλεσμα. Όμως και οι έξι προηγούμενες παράμετροι είναι γνωστές στον Verifier, τα Z, R_1, S ως μέρος του δημοσίου κλειδιού της εκδότριας Αρχής, το A' από το πρωτόκολλο εγκυρότητας πιστοποιητικού που εκτέλεσε προηγούμενα με τον Prover και τα R_2^{-1}, R επειδή τα υπολόγισε ο ίδιος, το δεύτερο από τη σχέση (110). Έτσι όταν του κοινοποιηθούν οι αλλοιωμένες παράμετροι από τον Prover στην αρχή της εκτέλεσης του πρωτοκόλλου γνώσης διακριτών λογαρίθμων, αυτός θα τις εντοπίσει, θα καταλάβει ότι αυτό δεν τηρείται από τον Prover και θα διακόψει τη συμμετοχή του σε αυτό μην μπορώντας στο τέλος να διαπιστώσει εάν ο ισχυρισμός του Prover είναι αληθής.

Έτσι στην περίπτωση που η δεδομένη τιμή περιέχεται στο συγκεκριμένο πεδίο του πιστοποιητικού και ο Prover επιλέξει να μην τηρήσει το πρωτόκολλο που εξετάζεται στην παρούσα υποενότητα, δε θα καταφέρει να εκτελέσει επιτυχώς το πρωτόκολλο γνώσης διακριτών λογαρίθμων του R_2^{-1} ως προς τις βάσεις Z, A', R_1, R, S.

Συνεπώς από την παρούσα απόδειξη προκύπτει πως μόνο όταν η δεδομένη τιμή δεν περιέχεται στο συγκεκριμένο πεδίο του έγκυρου πιστοποιητικού του Prover και το πρωτόκολλο τηρηθεί, ο ίδιος μπορεί να πείσει σίγουρα τον Verifier ότι γνωρίζει διακριτούς λογαρίθμους του R_2^{-1} ως προς τις βάσεις Z, A', R_1, R, S. Διαφορετικά η πιθανότητα να πειστεί ο Verifier είναι εξαιρετικά μικρή. Αυτό σημαίνει πως η απόδειξη γνώσης τέτοιων λογαρίθμων από τον Prover αποτελεί σχεδόν κατά 100% και απόδειξη ότι η δεδομένη τιμή δεν είναι η τιμή του συγκεκριμένου πεδίου του έγκυρου πιστοποιητικού του.

4. <u>Εμπιστευτικότητα πληροφορίας</u>

Η τιμή αυτού του πεδίου αποτελεί πληροφορία που δεν μπορεί να γίνει γνωστή στον Verifier. Από την μία δεν μαθαίνει άμεσα από τον Prover αυτήν την τιμή και από την άλλη δεν μπορεί να λάβει γνώση της έμμεσα από τον πρώτο αριθμό στον οποίο αντιστοιχίζεται. Αν ήξερε αυτόν τον αριθμό θα μπορούσε να χρησιμοποιήσει τη δημοσιοποιημένη λίστα των κωδικών των τιμών των πεδίων της Αρχής προκειμένου μέσω αυτού να βρει την τιμή του συγκεκριμένου πεδίου. Όμως αφενός δεν τον μαθαίνει άμεσα από τον Prover και αφετέρου δεν μπορεί να τον πληροφορηθεί έμμεσα υπολογίζοντάς τον. Για το δεύτερο θα ακολουθούσε τη διαδικασία που αναφέρθηκε στην παράγραφο 4 της απόδειξης της υποενότητας 5.5. και η οποία βασίζεται στη γνώση του m_2 που όμως δε θα μπορούσε να έχει.

Από την μία, όταν προηγουμένως στα πλαίσια της εκτέλεσης του πρωτοκόλλου εγκυρότητας πιστοποιητικού εκτέλεσε με τον Prover το πρωτόκολλο γνώσης διακριτών λογαρίθμων του Z ως προς τα A', R_1, R_2, S, δεν ήταν δυνατό να πληροφορηθεί τους διακριτούς λογαρίθμους που ξέρει ο Prover ως προς τις τέσσερις αυτές βάσεις, άρα και τον m_2 ως προς το R_2.

Από την άλλη, στην περίπτωση που ο ισχυρισμός του Prover είναι αληθής και το παρών πρωτόκολλο τηρηθεί, τότε όπως αναφέρθηκε στην παρούσα απόδειξη θα $\exists x, y \in \mathbb{Z}^*$ ώστε να ισχύει

$$v \cdot x + m_2 \cdot y = 1$$

και το πρωτόκολλο γνώσης διακριτών λογαρίθμων του R_2^{-1} ως προς τις βάσεις Z, A', R_1, R, S θα εκτελεστεί επιτυχώς. Αν ο Verifier επιχειρούσε να λύσει την προηγούμενη εξίσωση ως προς m_2, θα ήταν απαραίτητη η γνώση των x, y την οποία δε θα είχε. Ο λόγος θα ήταν ότι κατά την επιτυχή εκτέλεση του προηγούμενου πρωτοκόλλου γνώσης διακριτών λογαρίθμων δεν είναι δυνατό να πληροφορηθεί τους λογαρίθμους που ξέρει ο Prover και οι οποίοι είναι οι

$$-y, e \cdot y, m_1 \cdot y, x, v' \cdot y \, .$$

Έτσι δεν μπορεί να λάβει γνώση του πρώτου και του τέταρτου λογαρίθμου που είναι ο $-y$ και x αντίστοιχα.

5.6.1. Πρώτο Zkp Πρωτόκολλο Πεδίων με Τιμές Διαφορετικές από κάποιες Δεδομένες Τιμές

Στην υποενότητα αυτή παρουσιάζεται ένα zkp πρωτόκολλο που είναι επέκταση αυτού της προηγούμενης υποενότητας. Αποτελεί την πρώτη έκδοση ενός zkp πρωτοκόλλου το οποίο χρησιμοποιεί ο Prover για να πείσει τον Verifier ότι οι τιμές περισσότερων του ενός πεδίων του έγκυρου πιστοποιητικού που κατέχει είναι διαφορετικές από κάποιες δεδομένες τιμές. Οι τιμές αυτών των πεδίων είναι η πληροφορία που σχετίζεται με τον προηγούμενο ισχυρισμό και θα πρέπει να συνεχίσουν να παραμένουν μυστικές στον Verifier κατά τη διάρκεια και μετά το τέλος της εκτέλεσης του συγκεκριμένου πρωτοκόλλου. Όπως αναφέρθηκε στο τέλος της ενότητας 5, θεωρείται πως πριν την εκτέλεση του παρόντος πρωτοκόλλου έχει ήδη αποδειχτεί η εγκυρότητα του πιστοποιητικού του Prover μέσω του πρωτοκόλλου εγκυρότητας πιστοποιητικού. Ένα παράδειγμα χρήσης του παρόντος πρωτοκόλλου θα ήταν η περίπτωση στην οποία ο ισχυρισμός θα είχε ως εξής: '*τα πεδία του επιπέδου μόρφωσης και οικογενειακής κατάστασης δεν έχουν τις τιμές 'Πανεπιστήμιο' και 'Άγαμος' αντίστοιχα*'. Οι δεδομένες τιμές σε αυτήν την περίπτωση είναι οι '*Πανεπιστήμιο*' και '*Άγαμος*'. Το πρωτόκολλο και η απόδειξη ότι πετυχαίνει τον σκοπό του παρουσιάζονται παρακάτω.

- Verifier
  - $\forall i \in \{1,..,k\}$, όπου $k \in \mathbb{N}^* - \{1\}$ είναι ο αριθμός των δεδομένων τιμών, επιλέγει από τη δημοσιοποιημένη λίστα των κωδικών των τιμών των πεδίων της Αρχής τον πρώτο αριθμό v_i που αντιστοιχεί στην i οστή δεδομένη τιμή την οποία ο Prover θέλει να αποδείξει ότι δεν αποτελεί την τιμή ενός συγκεκριμένου πεδίου του πιστοποιητικού του.
  - Υπολογίζει $\begin{cases} R_2^{-1} \\ R = \left(R_2^{-1}\right)^{\prod_{i=1}^{k} v_i} \bmod n \end{cases}$, όπου θεωρείται πως $R \neq 1$.
  - Στέλνει στον Prover το R.
- Prover
  - $\forall i \in \{1,..,k\}$ επιλέγει από τη δημοσιοποιημένη λίστα των κωδικών των τιμών των πεδίων της Αρχής τον πρώτο αριθμό v_i.

- Υπολογίζει R_2^{-1} και $x, y \in \mathbb{Z}^*$ τέτοια ώστε $\left(\prod_{i=1}^{k} v_i\right) \cdot x + m_2 \cdot y = 1$, όπου m_2 το γινόμενο των πρώτων αριθμών στους οποίους είναι κωδικοποιημένες οι τιμές των πεδίων του πιστοποιητικού του. Ο υπολογισμός των x, y γίνεται εκτελώντας τον επεκτεινόμενο Ευκλείδειο αλγόριθμο με εισόδους τα $\prod_{i=1}^{k} v_i, m_2$.
- Υπολογίζει $\begin{cases} -y \\ e \cdot y \\ m_1 \cdot y \\ v' \cdot y \end{cases}$, όπου e είναι η μία από τις τρεις παραμέτρους της υπογραφής του πιστοποιητικού, m_1 είναι ο κώδικάς του που υπολόγισε ο ίδιος κατά τη φάση της επιβεβαίωσης και v' είναι υπολογισμένο από το πρωτόκολλο εγκυρότητας πιστοποιητικού που εκτέλεσε προηγούμενα με τον Verifier για να αποδείξει ότι κατέχει ένα έγκυρο πιστοποιητικό.
- Εκτελεί με τον Verifier το πρωτόκολλο γνώσης διακριτών λογαρίθμων του R_2^{-1} ως προς τις βάσεις Z, A', R_1, R, S, όπου A' είναι υπολογισμένο από το πρωτόκολλο εγκυρότητας πιστοποιητικού.

- Verifier
  - Αν αποδειχτεί ότι ο Prover γνωρίζει διακριτούς λογαρίθμους του R_2^{-1} ως προς τις βάσεις Z, A', R_1, R, S, τότε αυτός κατέχει ένα έγκυρο πιστοποιητικό όπου οι τιμές των k συγκεκριμένων πεδίων του δεν είναι ίσες με τις k δεδομένες τιμές.

Απόδειξη

Αν οι k τιμές των συγκεκριμένων πεδίων του έγκυρου πιστοποιητικού του Prover διαφέρουν από τις k δεδομένες τιμές, τότε $\forall i \in \{1,..,k\}$ στο γινόμενο m_2 των πρώτων αριθμών στους οποίους είναι κωδικοποιημένες οι τιμές των πεδίων του πιστοποιητικού, δε θα περιέχεται ως παράγοντάς του ο πρώτος αριθμός v_i που αντιστοιχεί στην iοστή δεδομένη τιμή και επομένως δε θα το διαιρεί. Εφόσον $\forall i \in \{1,..,k\}$ ο πρώτος v_i δεν είναι διαιρέτης του m_2, τότε σύμφωνα με την Πρόταση 1 οι δύο αυτοί αριθμοί είναι πρώτοι μεταξύ τους και άρα λόγω της Πρότασης 5.1 το m_2 θα είναι πρώτο με το γινόμενο $\prod_{i=1}^{k} v_i$. Τότε λόγω της Πρότασης 3 θα $\exists x, y \in \mathbb{Z}^*$ ώστε να ισχύει

$$\left(\prod_{i=1}^{k} v_i\right) \cdot x + m_2 \cdot y = 1.$$

Τα x, y είναι διαφορετικά του 0 γιατί αλλιώς από την τελευταία εξίσωση θα προέκυπτε ότι το $\prod_{i=1}^{k} v_i$ ή το m_2 θα ήταν ίσο με 1 ή -1, κάτι που δεν ισχύει αφού

αυτά είναι μεγαλύτερα του 1. Η απόδειξη του παρόντος πρωτοκόλλου είναι παρόμοια με αυτήν που δόθηκε στην προηγούμενη υποενότητα.

5.7. Δεύτερο Zkp Πρωτόκολλο Πεδίου με Τιμή Διαφορετική από μια Δεδομένη Τιμή

[6] Στην υποενότητα αυτή παρουσιάζεται και αναλύεται η δεύτερη έκδοση ενός zkp πρωτοκόλλου το οποίο χρησιμοποιεί ο Prover για να πείσει τον Verifier ότι η τιμή ενός πεδίου του έγκυρου πιστοποιητικού που κατέχει είναι διαφορετική από μια δεδομένη τιμή. Όπως αναφέρθηκε στο τέλος της ενότητας 5, θεωρείται πως πριν την εκτέλεση του παρόντος πρωτοκόλλου έχει ήδη αποδειχτεί η εγκυρότητα του πιστοποιητικού του Prover μέσω του πρωτοκόλλου εγκυρότητας πιστοποιητικού. Το πρωτόκολλο και η απόδειξη ότι πετυχαίνει τον σκοπό του παρουσιάζονται παρακάτω.

- Prover
  - Επιλέγει τυχαία $r \in \mathbb{Z}^*$.
  - Υπολογίζει $D = \left(g^{m_2} \cdot g'^{r}\right) \bmod n$ (120), έτσι ώστε $D \neq 1$, όπου g, g' είναι δημόσια γνωστά στοιχεία του $QR_n^* - \{1\}$ που δημιούργησε η Αρχή κατά τη φάση δημιουργίας παραμέτρων και m_2 είναι το γινόμενο των πρώτων αριθμών στους οποίους είναι κωδικοποιημένες οι τιμές των πεδίων του πιστοποιητικού του.
  - Εκτελεί με τον Verifier το πρωτόκολλο ισότητας διακριτών λογαρίθμων των Z, D ως προς τις βάσεις R_2, g με αναπαραστάσεις στις βάσεις A', R_1, R_2, S και g, g' αντίστοιχα. Το A' είναι υπολογισμένο από το πρωτόκολλο εγκυρότητας πιστοποιητικού που εκτέλεσε προηγούμενα με τον Verifier για να αποδείξει ότι κατέχει ένα έγκυρο πιστοποιητικό.
- Verifier
  - Αν δεν αποδειχτεί ότι υπάρχει κοινός διακριτός λογάριθμος των Z, D ως προς τις βάσεις R_2, g με αναπαραστάσεις στις βάσεις A', R_1, R_2, S και g, g' αντίστοιχα, τότε διακόπτει το παρών πρωτόκολλο.
  - Επιλέγει από τη δημοσιοποιημένη λίστα των κωδικών των τιμών των πεδίων της Αρχής τον πρώτο αριθμό v που αντιστοιχεί στη δεδομένη τιμή την οποία ο Prover θέλει να αποδείξει ότι δεν είναι η τιμή ενός συγκεκριμένου πεδίου του πιστοποιητικού του.
  - Υπολογίζει $G = g^v \bmod n$ (121), όπου θεωρείται πως $G \neq 1$.
  - Στέλνει στον Prover το G.
- Prover
  - Επιλέγει από τη δημοσιοποιημένη λίστα των κωδικών των τιμών των πεδίων της Αρχής τον πρώτο αριθμό v.
  - Υπολογίζει $x, y \in \mathbb{Z}^*$ τέτοια ώστε $v \cdot x + m_2 \cdot y = 1$ (111). Ο υπολογισμός γίνεται εκτελώντας τον επεκτεινόμενο Ευκλείδειο αλγόριθμο με εισόδους τα v, m_2.
  - Υπολογίζει $-r \cdot y$.

- Εκτελεί με τον Verifier το πρωτόκολλο γνώσης διακριτών λογαρίθμων του g ως προς τις βάσεις D, G, g'.

- Verifier
  - Αν αποδειχτεί ότι ο Prover γνωρίζει διακριτούς λογαρίθμους του g ως προς τις βάσεις D, G, g', τότε αυτός κατέχει ένα έγκυρο πιστοποιητικό όπου η τιμή του συγκεκριμένου πεδίου του δεν είναι ίση με τη δεδομένη τιμή.

Απόδειξη

Εφόσον ο Prover προηγουμένως εκτέλεσε με επιτυχία το πρωτόκολλο εγκυρότητας πιστοποιητικού, τότε θα ισχύει

$$Z = \left(A'^{e} \cdot R_1^{m_1} \cdot R_2^{m_2} \cdot S^{v'}\right) \bmod n \quad (101).$$

1. Το πρωτόκολλο τηρείται ανεξάρτητα εάν η τιμή του συγκεκριμένου πεδίου του έγκυρου πιστοποιητικού του Prover δεν είναι ίση ή είναι με τη δεδομένη τιμή

Σε αυτήν την περίπτωση ο Prover θα υπολογίσει κανονικά σύμφωνα με το πρωτόκολλο το D από τη σχέση

$$D = \left(g^{m_2} \cdot g'^{r}\right) \bmod n \quad (120).$$

Επειδή $g, g' \in QR_n^*$, σύμφωνα με την (120) και την Πρόταση 20.3 θα ισχύει $D \in QR_n^*$ και επειδή $D \neq 1$, τότε $D \in QR_n^* - \{1\}$. Ο Prover ξέρει ότι τα γνωστά σε αυτόν e, m_1, m_2, v' αποτελούν διακριτούς λογαρίθμους του Z ως προς τις βάσεις A', R_1, R_2, S αντίστοιχα, όπως φαίνεται από την (101). Επίσης ξέρει ότι τα γνωστά σε αυτόν m_2, r αποτελούν διακριτούς λογαρίθμους του D ως προς τις βάσεις g, g' αντίστοιχα, όπως φαίνεται από την (120). Έτσι γνωρίζει πως όταν τα Z, D αναπαρίστανται στις βάσεις $A', R_1, R_2, S \in QR_n^* - \{1\}$ και $g, g' \in QR_n^* - \{1\}$ αντίστοιχα, τότε ένας κοινός τους λογάριθμος ως προς τις βάσεις R_2, g αντιστοίχως είναι το m_2. Αυτό σημαίνει πως θα εκτελέσει με επιτυχία το πρωτόκολλο ισότητας λογαρίθμων, αποδεικνύοντας στον Verifier την ύπαρξη κοινού λογαρίθμου όπως ο m_2 χωρίς όμως ο συγκεκριμένος να γίνει γνωστός σε αυτόν. Εφόσον το πρωτόκολλο τηρείται ο Verifier θα υπολογίσει κανονικά σύμφωνα με αυτό το G από τη σχέση

$$G = g^{v} \bmod n \quad (121).$$

Επειδή $g \in QR_n^*$, σύμφωνα με την (121) και την Πρόταση 20.2 θα ισχύει $G \in QR_n^*$ και επειδή $G \neq 1$, τότε $G \in QR_n^* - \{1\}$.

1.1. Η τιμή του συγκεκριμένου πεδίου του έγκυρου πιστοποιητικού του Prover δεν είναι ίση με τη δεδομένη τιμή

Σε αυτήν την υποπερίπτωση, όπως αναφέρθηκε και στην απόδειξη της πρώτης έκδοσης του πρωτοκόλλου στην υποενότητα 5.6, στο γινόμενο m_2 δε θα περιέχεται ως παράγοντάς του ο πρώτος αριθμός v και θα $\exists x, y \in \mathbb{Z}^*$ ώστε να ισχύει

$$v \cdot x + m_2 \cdot y = 1 \quad (111).$$

Ο Prover μπορεί να υπολογίσει τα x, y εφόσον γνωρίζει τα v, m_2. Από την (120) συνεπάγεται ότι

$$D^y \equiv \left(g^{m_2}\cdot g'^{r}\right)^y \bmod n = \left(\left(g^{m_2}\right)^y \cdot \left(g'^{r}\right)^y\right) \bmod n \Rightarrow D^y \equiv \left(g^{m_2\cdot y}\cdot g'^{r\cdot y}\right) \bmod n \ (122).$$

Επίσης από την (121) συνεπάγεται ότι

$$G^x \equiv \left(g^v\right)^x \bmod n \Rightarrow G^x \equiv g^{v\cdot x} \bmod n \xrightarrow{(122)} \left(D^y \cdot G^x\right) \equiv \left(g^{m_2\cdot y}\cdot g'^{r\cdot y}\cdot g^{v\cdot x}\right) \bmod n =$$
$$\left(g^{m_2\cdot y+v\cdot x}\cdot g'^{r\cdot y}\right) \bmod n \xrightarrow{(111)} \left(D^y \cdot G^x\right) \equiv \left(g^1\cdot g'^{r\cdot y}\right) \bmod n \Rightarrow$$
$$\left(D^y \cdot G^x \cdot g'^{-r\cdot y}\right) \equiv g \bmod n \Rightarrow g = \left(D^y \cdot G^x \cdot g'^{-r\cdot y}\right) \bmod n \ (123),$$

αφού $g \in QR_n^*$ και άρα $g \in \mathbb{Z}_n^*$ που σημαίνει πως $g < n$. Ο Prover μαθαίνει το G όταν το λαμβάνει από τον Verifier. Εφόσον υπολογίζει τα y, x, τότε γνωρίζει στην (123) διακριτούς λογαρίθμους του g ως προς τα D, G αντίστοιχα. Επίσης όπως προαναφέρθηκε ξέρει το r και συνεπώς μπορεί να υπολογίσει το $-r\cdot y$ μαθαίνοντας στην ίδια σχέση έναν λογάριθμο του g ως προς το g'. Από τη στιγμή που ο Prover ξέρει διακριτούς λογαρίθμους του g ως προς τις βάσεις $D, G, g' \in QR_n^* - \{1\}$, θα αποδείξει τη γνώση του αυτή στον Verifier όταν και οι δύο χρησιμοποιήσουν το zkp πρωτόκολλο γνώσης διακριτών λογαρίθμων. Η απόδειξη αυτή θα γίνει χωρίς να αποκαλυφθούν άμεσα ή έμμεσα στον Verifier οι συγκεκριμένοι διακριτοί λογάριθμοι.

1.2. <u>Η τιμή του συγκεκριμένου πεδίου του έγκυρου πιστοποιητικού του Prover είναι ίση με τη δεδομένη τιμή</u>

Σε αυτήν την υποπερίπτωση, όπως αναφέρθηκε και στην απόδειξη της πρώτης έκδοσης του πρωτοκόλλου στην υποενότητα 5.6, τα v, m_2 δεν είναι πρώτοι μεταξύ τους και συνεπώς δεν $\exists x, y \in \mathbb{Z}$ ώστε

$$v\cdot x + m_2 \cdot y = 1 \ (111).$$

Από τη στιγμή που ο Prover αδυνατεί να βρει κάποια $x, y \in \mathbb{Z}^*$ ώστε να ισχύει η (111) όπως έκανε πριν, δε θα μπορέσει να ακολουθήσει την προηγούμενη διαδικασία προκειμένου να πληροφορηθεί διακριτούς λογαρίθμους του g ως προς τις βάσεις D, G, g'. Θα δειχτεί ότι σχεδόν κατά 100% αυτός δε γνωρίζει τέτοιους λογαρίθμους. Τίθεται ο ισχυρισμός πως γνωρίζει κάποιους.

Σχεδόν σίγουρα η γνώση αυτών δε θα προήλθε προσπαθώντας ο ίδιος να λύσει την εξίσωση

$$g = \left(D^{x_1}\cdot G^{x_2}\cdot g'^{x_3}\right) \bmod n \ (124)$$

ως προς $x_1, x_2, x_3 \in \mathbb{Z}^*$, καθώς κάτι τέτοιο θα ήταν πάρα πολύ δύσκολο σύμφωνα με το Δεύτερο Ισχυρισμό Διακριτού Λογαρίθμου.

Λαμβάνοντας υπόψη του ότι ισχύουν οι (120), (121), αφού σύμφωνα με την υπόθεση το πρωτόκολλο τηρείται και άρα ο Verifier θα υπολόγισε σωστά το G από την (121), μια δεύτερη εναλλακτική οδός που πιθανόν θα τον οδηγούσε στη γνώση αυτών των λογαρίθμων θα ήταν να ακολουθούσε τις παρακάτω συνεπαγωγές προκειμένου να συμπεράνει τη συνθήκη που θα έπρεπε να τηρούν τα x_1, x_2, x_3. Από την (120) συνεπάγεται πως

$$D^{x_1} \equiv \left(g^{m_2}\cdot g'^{r}\right)^{x_1} \bmod n = \left(\left(g^{m_2}\right)^{x_1} \cdot \left(g'^{r}\right)^{x_1}\right) \bmod n \Rightarrow D^{x_1} \equiv \left(g^{m_2\cdot x_1}\cdot g'^{r\cdot x_1}\right) \bmod n \ (125).$$

Επίσης από την (121) συνεπάγεται ότι

$$G^{x_2} \equiv \left(g^v\right)^{x_2} \bmod n \Rightarrow G^{x_2} \equiv g^{v\cdot x_2} \bmod n \xrightarrow{(125)}$$
$$\left(D^{x_1} \cdot G^{x_2}\right) \equiv \left(g^{m_2\cdot x_1}\cdot g'^{r\cdot x_1}\cdot g^{v\cdot x_2}\right) \bmod n \Rightarrow \left(D^{x_1} \cdot G^{x_2}\right) \equiv \left(g^{m_2\cdot x_1+v\cdot x_2}\cdot g'^{r\cdot x_1}\right) \bmod n \Rightarrow$$

$$\left(D^{x_1}\cdot G^{x_2}\cdot g'^{x_3}\right)\equiv\left(g^{m_2\cdot x_1+v\cdot x_2}\cdot g'^{r\cdot x_1}\cdot g'^{x_3}\right)\bmod n\xrightarrow{(124)}$$

$$g=\left(g^{m_2\cdot x_1+v\cdot x_2}\cdot g'^{r\cdot x_1+x_3}\right)\bmod n\Rightarrow\left(g\cdot g'^{-(r\cdot x_1+x_3)}\right)\equiv\left(g^{m_2\cdot x_1+v\cdot x_2}\right)\bmod n\Rightarrow$$

$$g'^{-(r\cdot x_1+x_3)}\equiv\left(g^{m_2\cdot x_1+v\cdot x_2}\cdot g^{-1}\right)\bmod n\Rightarrow g'^{-(r\cdot x_1+x_3)}\equiv g^{m_2\cdot x_1+v\cdot x_2-1}\bmod n\ (126).$$

Σύμφωνα με την (64) που αναφέρεται στην υποενότητα 4.1, ισχύει

$$g'=g^{l_{g'}}\bmod n,$$

όπου το $l_{g'}\in\{2,..,p'\cdot q'-1\}$ κρατείται μυστικό από την Αρχή. Έτσι ο Prover δεν το ξέρει και πάρα πολύ δύσκολα θα μπορούσε να το υπολογίσει από την τελευταία εξίσωση λόγω του Πρώτου Ισχυρισμού Διακριτού Λογαρίθμου. Επίσης όπως αναφέρεται στην ίδια υποενότητα, η τάξη του g ως προς n είναι ίση με $p'\cdot q'$. Λόγω της (64) συνεπάγεται πως

$$g'^{-(r\cdot x_1+x_3)}\equiv\left(g^{l_{g'}}\right)^{-(r\cdot x_1+x_3)}\bmod n\xrightarrow{(126)}g^{m_2\cdot x_1+v\cdot x_2-1}\equiv g^{-l_{g'}\cdot(r\cdot x_1+x_3)}\bmod n.$$

Σύμφωνα με την Πρόταση 15.2 και αφού η τάξη του g ως προς n ισούται με $p'\cdot q'$, προκύπτει από την τελευταία ισοδυναμία πως

$$\left(m_2\cdot x_1+v\cdot x_2-1+l_{g'}\cdot\left(r\cdot x_1+x_3\right)\right)\equiv 0\bmod\left(p'\cdot q'\right).$$

Δηλαδή $\exists d\in\mathbb{Z}$ ώστε

$$m_2\cdot x_1+v\cdot x_2-1+l_{g'}\cdot\left(r\cdot x_1+x_3\right)=p'\cdot q'\cdot d\ .$$

Από την τελευταία εξίσωση προκύπτει πως η συνθήκη που πρέπει να ικανοποιούν τα x_1,x_2,x_3 είναι ότι το

$$m_2\cdot x_1+v\cdot x_2-1+l_{g'}\cdot\left(r\cdot x_1+x_3\right)$$

θα πρέπει να είναι πολλαπλάσιο του $p'\cdot q'$, το οποίο με τη σειρά του να σημειωθεί ότι είναι διάφορο του 0 αφού τα p',q' είναι πρώτοι αριθμοί. Επειδή ο Prover δε τα γνωρίζει, αφού αυτά κρατούνται μυστικά από την εκδότρια Αρχή, τότε δε θα μπορούσε να υπολογίσει το γινόμενό τους $p'\cdot q'$ και να βρει ένα μη μηδενικό πολλαπλάσιό του, ώστε αρχικά να το δοκιμάσει εάν θα μπορούσε να αποτελέσει τιμή του

$$m_2\cdot x_1+v\cdot x_2-1+l_{g'}\cdot\left(r\cdot x_1+x_3\right)$$

και αν ναι μετά να δοκιμάσει αν τα x_1,x_2,x_3 που θα είχε υπολογίσει ικανοποιούσαν την (124). Έτσι η μόνη επιλογή του θα ήταν το μηδενικό πολλαπλάσιο, οπότε για $d=0$ θα μετασχημάτιζε την παραπάνω εξίσωση στη σχέση

$$m_2\cdot x_1+v\cdot x_2-1+l_{g'}\cdot\left(r\cdot x_1+x_3\right)=0$$

η οποία λόγω του ότι $l_{g'}\in\{2,..,p'\cdot q'-1\}$ και άρα $l_{g'}\neq 0$, θα ισοδυναμεί με

$$m_2\cdot x_1+v\cdot x_2-1=-l_{g'}\cdot\left(r\cdot x_1+x_3\right)\Leftrightarrow r\cdot x_1+x_3=\left(m_2\cdot x_1+v\cdot x_2-1\right)\cdot\frac{1}{-l_{g'}}\Leftrightarrow$$

$$x_3=-\left(m_2\cdot x_1+v\cdot x_2-1\right)\cdot\frac{1}{l_{g'}}-r\cdot x_1\Leftrightarrow x_3=\left(1-m_2\cdot x_1-v\cdot x_2\right)\cdot\frac{1}{l_{g'}}-r\cdot x_1\ (127).$$

Ο Prover θα επέλεγε τυχαία κάποια $x_1,x_2\in\mathbb{Z}^*$ και θα προσπαθούσε να επιλύσει ως προς x_3 την (127). Επειδή όπως αναφέρθηκε προηγούμενα δεν $\exists x,y\in\mathbb{Z}$ ώστε

$$m_2\cdot x+v\cdot y=1$$

και άρα ισοδύναμα

$$1-m_2\cdot x-v\cdot y=0,$$

τότε για οποιαδήποτε τυχαία επιλογή των $x_1, x_2 \in \mathbb{Z}^*$ εκ μέρους του Prover, θα ίσχυε ότι

$$1 - m_2 \cdot x_1 - v \cdot x_2 \neq 0 \quad (128).$$

Στην (127) η μόνη παράμετρος που θα του ήταν άγνωστη εκτός του x_3 θα ήταν το $l_{g'}$ που όπως προαναφέρθηκε πάρα πολύ δύσκολα θα μπορούσε να υπολογίσει. Από τη στιγμή που θα ίσχυε η (128), τότε το γινόμενο

$$\left(1 - m_2 \cdot x_1 - v \cdot x_2\right) \cdot \frac{1}{l_{g'}}$$

θα του ήταν επίσης άγνωστο με αποτέλεσμα να αδυνατούσε να επιλύσει την (127) ως προς x_3. Επομένως ο Prover δε θα μπορούσε να υπολογίσει κάποια $x_1, x_2, x_3 \in \mathbb{Z}^*$ που να τηρούσαν την παραπάνω συνθήκη ώστε μετά να δοκιμάσει αν αυτά ικανοποιούσαν την (124). Έτσι αν ακολουθούσε τη δεύτερη εναλλακτική οδό, σχεδόν κατά 100% δε θα μπορούσε να λάβει γνώση κάποιων διακριτών λογαρίθμων του g ως προς τις βάσεις D, G, g'.

Συνεπώς σχεδόν σίγουρα με κανέναν τρόπο δε θα μπορούσε ο Prover να πληροφορηθεί διακριτούς λογαρίθμους του g ως προς αυτές τις βάσεις και έτσι ο παραπάνω ισχυρισμός που τέθηκε δεν αληθεύει σχεδόν κατά 100%. Επομένως όταν η δεδομένη τιμή είναι ίδια με αυτήν που έχει το συγκεκριμένο πεδίο του πιστοποιητικού, ο Prover σχεδόν σίγουρα δε γνωρίζει διακριτούς λογαρίθμους του g ως προς τις βάσεις D, G, g'. Εφόσον σύμφωνα με την υπόθεση τηρείται το παρών πρωτόκολλο, ο Prover θα εκτελέσει κανονικά όπως προβλέπεται με τον Verifier το πρωτόκολλο γνώσης διακριτών λογαρίθμων του g ως προς τις παραπάνω βάσεις και το αποτέλεσμα θα είναι σχεδόν 100% ανεπιτυχές για τον ίδιο.

2. <u>Η δεδομένη τιμή περιέχεται στο συγκεκριμένο πεδίο του πιστοποιητικού και ο Prover επιλέγει να μην τηρήσει το πρωτόκολλο</u>

Σε αυτήν την περίπτωση ο Prover ενεργεί έτσι προκειμένου να ξεγελάσει τον Verifier ώστε να τον πείσει για τον ψευδή ισχυρισμό του. Μια δυνατότητα που έχει για να λειτουργήσει αντικανονικά είναι να μην εκτελέσει όπως προβλέπεται το πρωτόκολλο γνώσης διακριτών λογαρίθμων του g ως προς τις βάσεις D, G, g', αφού προηγουμένως έχει τηρήσει όλα τα βήματα. Αν το εκτελούσε κανονικά, τότε όπως αναφέρθηκε προηγούμενα το αποτέλεσμα θα ήταν για τον ίδιο ανεπιτυχές αφού η δεδομένη τιμή περιέχεται στο συγκεκριμένο πεδίο του πιστοποιητικού. Θα μπορούσε επομένως να αλλοιώσει κάποια από τα g, D, G, g' ώστε να εκτελέσει αυτό το πρωτόκολλο με διαφορετικές παραμέτρους που θα του εξασφάλιζαν το επιτυχές για αυτόν αποτέλεσμα. Όμως και οι τέσσερις προηγούμενες παράμετροι είναι γνωστές στον Verifier, τα g, g' ως δημοσιοποιημένα από την Αρχή, το D από το πρωτόκολλο ισότητας διακριτών λογαρίθμων που εκτέλεσε προηγούμενα με τον Prover και το G επειδή το υπολόγισε ο ίδιος από τη σχέση (121). Έτσι όταν του κοινοποιηθούν οι αλλοιωμένες παράμετροι από τον Prover στην αρχή της εκτέλεσης του πρωτοκόλλου γνώσης διακριτών λογαρίθμων, αυτός θα τις εντοπίσει, θα καταλάβει ότι αυτό δεν τηρείται από τον Prover και θα διακόψει τη συμμετοχή του σε αυτό μην μπορώντας στο τέλος να διαπιστώσει εάν ο ισχυρισμός του Prover είναι αληθής.

Από την άλλη, λαμβάνοντας υπόψη ο Prover πως το G που θα του στείλει ο Verifier δίνεται από τη σχέση

$$G = g^v \bmod n \quad (121),$$

θα μπορούσε να προσπαθήσει να υπολογίσει ένα τέτοιο D ώστε για κάποια $x_1, x_2, x_3 \in \mathbb{Z}^*$ που θα επέλεγε να ίσχυε η σχέση

$$g = \left(D^{x_1} \cdot G^{x_2} \cdot g'^{x_3}\right) \bmod n \quad (124),$$

ώστε να μπορούσε μετά να εκτελέσει επιτυχώς το πρωτόκολλο γνώσης διακριτών λογαρίθμων αφού τα x_1, x_2, x_3 που θα ήξερε θα αποτελούσαν διακριτούς λογαρίθμους του g ως προς τις βάσεις D, G, g'. Συγκεκριμένα το D που θα υπολόγιζε θα έπρεπε να ήταν της μορφής

$$D = \left(g^{m_2} \cdot g''^{r}\right) \bmod n \quad (120)$$

με $r \in \mathbb{Z}^*$, προκειμένου να εκτελούσε με επιτυχία το πρωτόκολλο ισότητας διακριτών λογαρίθμων και έτσι το πρωτόκολλο που εξετάζεται σε αυτήν την υποενότητα να μη διακοπτόταν από τον Verifier. Από όλες τις παραμέτρους η μόνη που δε θα ήξερε εκτός του D θα ήταν το r, καθώς τις υπόλοιπες

$$g, g', G, x_1, x_2, x_3, v, m_2$$

θα τις γνώριζε. Άρα θα προσπαθούσε να υπολογίσει ένα κατάλληλο $r \in \mathbb{Z}^*$ και όχι να το επέλεγε οπωσδήποτε τυχαία σύμφωνα με το παρών πρωτόκολλο. Για αυτόν τον υπολογισμό θα ακολουθούσε τις προηγούμενες συνεπαγωγές που θα τον οδηγούσαν στην (126) και από εκεί στη συνθήκη που θα έπρεπε να τηρεί το r: το

$$m_2 \cdot x_1 + v \cdot x_2 - 1 + l_{g'} \cdot \left(r \cdot x_1 + x_3\right)$$

θα πρέπει να είναι πολλαπλάσιο του $p' \cdot q'$. Προχωρώντας θα έφτανε στη σχέση

$$m_2 \cdot x_1 + v \cdot x_2 - 1 + l_{g'} \cdot \left(r \cdot x_1 + x_3\right) = 0$$

που επειδή $l_{g'} \neq 0$ και $x_1 \neq 0$, αφού $x_1 \in \mathbb{Z}^*$, θα ισοδυναμεί με

$$m_2 \cdot x_1 + v \cdot x_2 - 1 = -l_{g'} \cdot \left(r \cdot x_1 + x_3\right) \Leftrightarrow r \cdot x_1 + x_3 = \left(m_2 \cdot x_1 + v \cdot x_2 - 1\right) \cdot \frac{1}{-l_{g'}} \Leftrightarrow$$

$$r \cdot x_1 = -\left(m_2 \cdot x_1 + v \cdot x_2 - 1\right) \cdot \frac{1}{l_{g'}} - x_3 \Leftrightarrow r = \frac{\left(1 - m_2 \cdot x_1 - v \cdot x_2\right)}{x_1} \cdot \frac{1}{l_{g'}} - \frac{x_3}{x_1} \quad (129).$$

Εφόσον σύμφωνα με την υπόθεση η δεδομένη τιμή περιέχεται στο συγκεκριμένο πεδίο του πιστοποιητικού, τότε όπως προαναφέρθηκε δεν $\exists x, y \in \mathbb{Z}$ ώστε

$$v \cdot x + m_2 \cdot y = 1$$

και έτσι για οποιαδήποτε επιλογή των $x_1, x_2 \in \mathbb{Z}^*$ εκ μέρους του Prover, θα ίσχυε ότι

$$m_2 \cdot x_1 + v \cdot x_2 \neq 1 \Rightarrow 1 - m_2 \cdot x_1 - v \cdot x_2 \neq 0 \Rightarrow \frac{1 - m_2 \cdot x_1 - v \cdot x_2}{x_1} \neq 0 \quad (130).$$

Στην (129) η μόνη παράμετρος που θα του ήταν άγνωστη εκτός του r θα ήταν το $l_{g'}$ που όπως προαναφέρθηκε πάρα πολύ δύσκολα θα μπορούσε να υπολογίσει. Από τη στιγμή που θα ίσχυε η (130), τότε το γινόμενο

$$\frac{\left(1 - m_2 \cdot x_1 - v \cdot x_2\right)}{x_1} \cdot \frac{1}{l_{g'}}$$

θα του ήταν επίσης άγνωστο με αποτέλεσμα να αδυνατούσε να επιλύσει την (129) ως προς r. Επομένως ο Prover για οποιαδήποτε $x_1, x_2, x_3 \in \mathbb{Z}^*$ που θα επέλεγε, δε θα μπορούσε να υπολογίσει κάποιο $r \in \mathbb{Z}^*$ που να τηρούσε την παραπάνω συνθήκη προκειμένου μετά να το χρησιμοποιούσε για να υπολόγιζε από την (120) το D και ύστερα να δοκίμαζε αν αυτό το D ικανοποιούσε την (124). Έτσι δε θα ήταν εφικτός ο υπολογισμός ενός κατάλληλου D ώστε για κάποια x_1, x_2, x_3 να ίσχυε η (124) και να

μπορούσε μετά να εκτελέσει επιτυχώς το πρωτόκολλο γνώσης διακριτών λογαρίθμων.

Έτσι στην περίπτωση που η δεδομένη τιμή περιέχεται στο συγκεκριμένο πεδίο του πιστοποιητικού και ο Prover επιλέξει να μην τηρήσει το πρωτόκολλο που εξετάζεται στην παρούσα υποενότητα, δε θα καταφέρει να εκτελέσει επιτυχώς το πρωτόκολλο γνώσης διακριτών λογαρίθμων του g ως προς τις βάσεις D, G, g'.

Συνεπώς από την παρούσα απόδειξη προκύπτει πως μόνο όταν η δεδομένη τιμή δεν περιέχεται στο συγκεκριμένο πεδίο του έγκυρου πιστοποιητικού του Prover και το πρωτόκολλο τηρηθεί, ο ίδιος μπορεί να πείσει σίγουρα τον Verifier ότι γνωρίζει διακριτούς λογαρίθμους του g ως προς τις βάσεις D, G, g'. Διαφορετικά η πιθανότητα να πειστεί ο Verifier είναι εξαιρετικά μικρή. Αυτό σημαίνει πως η απόδειξη γνώσης τέτοιων λογαρίθμων από τον Prover αποτελεί σχεδόν κατά 100% και απόδειξη ότι η δεδομένη τιμή δεν είναι η τιμή του συγκεκριμένου πεδίου του έγκυρου πιστοποιητικού του.

4. <u>Εμπιστευτικότητα πληροφορίας</u>

Η τιμή αυτού του πεδίου αποτελεί πληροφορία που δεν μπορεί να γίνει γνωστή στον Verifier. Από την μία δεν μαθαίνει άμεσα από τον Prover αυτήν την τιμή και από την άλλη δεν μπορεί να λάβει γνώση της έμμεσα από τον πρώτο αριθμό στον οποίο αντιστοιχίζεται. Αν ήξερε αυτόν τον αριθμό θα μπορούσε να χρησιμοποιήσει τη δημοσιοποιημένη λίστα των κωδικών των τιμών των πεδίων της Αρχής προκειμένου μέσω αυτού να βρει την τιμή του συγκεκριμένου πεδίου. Όμως αφενός δεν τον μαθαίνει άμεσα από τον Prover και αφετέρου δεν μπορεί να τον πληροφορηθεί έμμεσα υπολογίζοντάς τον. Για το δεύτερο θα ακολουθούσε τη διαδικασία που αναφέρθηκε στην παράγραφο 4 της απόδειξης της υποενότητας 5.5. και η οποία βασίζεται στη γνώση του m_2 που όμως δε θα μπορούσε να έχει.

Από την μία, όταν προηγουμένως στα πλαίσια της εκτέλεσης του πρωτοκόλλου εγκυρότητας πιστοποιητικού εκτέλεσε με τον Prover το πρωτόκολλο γνώσης διακριτών λογαρίθμων του Z ως προς τα A', R_1, R_2, S, δεν ήταν δυνατό να πληροφορηθεί τους διακριτούς λογαρίθμους που ξέρει ο Prover ως προς τις τέσσερις αυτές βάσεις, άρα και τον m_2 ως προς το R_2.

Από την άλλη, στην περίπτωση που εκτελέσει με τον Prover επιτυχώς το πρωτόκολλο ισότητας διακριτών λογαρίθμων των Z, D ως προς τις βάσεις R_2, g με αναπαραστάσεις στις βάσεις A', R_1, R_2, S και g, g' αντίστοιχα, δεν μπορεί να πληροφορηθεί τον κοινό λογάριθμο που ξέρει ο Prover και ο οποίος είναι ο m_2.

Τέλος, στην περίπτωση που ο ισχυρισμός του Prover είναι αληθής και το παρών πρωτόκολλο τηρηθεί, τότε όπως αναφέρθηκε στην παρούσα απόδειξη θα $\exists x, y \in \mathbb{Z}^*$ ώστε να ισχύει

$$v \cdot x + m_2 \cdot y = 1$$

και το πρωτόκολλο γνώσης διακριτών λογαρίθμων του g ως προς τις βάσεις D, G, g' θα εκτελεστεί επιτυχώς. Αν ο Verifier επιχειρούσε να λύσει την προηγούμενη εξίσωση ως προς m_2, θα ήταν απαραίτητη η γνώση των x, y την οποία δε θα είχε. Ο λόγος θα ήταν ότι κατά την επιτυχή εκτέλεση του προηγούμενου πρωτοκόλλου γνώσης διακριτών λογαρίθμων δεν είναι δυνατό να πληροφορηθεί τους λογαρίθμους που ξέρει ο Prover και οι οποίοι είναι οι

$$y, x, -r \cdot y .$$

Έτσι δεν μπορεί να λάβει γνώση του πρώτου και του δεύτερου λογαρίθμου που είναι ο y και x αντίστοιχα.

5.7.1. Δεύτερο Zkp Πρωτόκολλο Πεδίων με Τιμές Διαφορετικές από κάποιες Δεδομένες Τιμές

[6] Στην υποενότητα αυτή παρουσιάζεται ένα zkp πρωτόκολλο που είναι επέκταση αυτού της προηγούμενης υποενότητας. Αποτελεί τη δεύτερη έκδοση ενός zkp πρωτοκόλλου το οποίο χρησιμοποιεί ο Prover για να πείσει τον Verifier ότι οι τιμές περισσότερων του ενός πεδίων του έγκυρου πιστοποιητικού που κατέχει είναι διαφορετικές από κάποιες δεδομένες τιμές. Όπως αναφέρθηκε στο τέλος της ενότητας 5, θεωρείται πως πριν την εκτέλεση του παρόντος πρωτοκόλλου έχει ήδη αποδειχτεί η εγκυρότητα του πιστοποιητικού του Prover μέσω του πρωτοκόλλου εγκυρότητας πιστοποιητικού. Το πρωτόκολλο και η απόδειξη ότι πετυχαίνει τον σκοπό του παρουσιάζονται παρακάτω.

- Prover
  - Επιλέγει τυχαία $r \in \mathbb{Z}^*$.
  - Υπολογίζει $D = \left(g^{m_2} \cdot g'^{r}\right) \bmod n$, έτσι ώστε $D \neq 1$, όπου g, g' είναι δημόσια γνωστά στοιχεία του $QR_n^* - \{1\}$ που δημιούργησε η Αρχή κατά τη φάση δημιουργίας παραμέτρων και m_2 είναι το γινόμενο των πρώτων αριθμών στους οποίους είναι κωδικοποιημένες οι τιμές των πεδίων του πιστοποιητικού του.
  - Εκτελεί με τον Verifier το πρωτόκολλο ισότητας διακριτών λογαρίθμων των Z, D ως προς τις βάσεις R_2, g με αναπαραστάσεις στις βάσεις A', R_1, R_2, S και g, g' αντίστοιχα. Το A' είναι υπολογισμένο από το πρωτόκολλο εγκυρότητας πιστοποιητικού που εκτέλεσε προηγούμενα με τον Verifier για να αποδείξει ότι κατέχει ένα έγκυρο πιστοποιητικό.
- Verifier
  - Αν δεν αποδειχτεί ότι υπάρχει κοινός διακριτός λογάριθμος των Z, D ως προς τις βάσεις R_2, g με αναπαραστάσεις στις βάσεις A', R_1, R_2, S και g, g' αντίστοιχα, τότε διακόπτει το παρών πρωτόκολλο.
  - $\forall i \in \{1,..,k\}$, όπου $k \in \mathbb{N}^* - \{1\}$ είναι ο αριθμός των δεδομένων τιμών, επιλέγει από τη δημοσιοποιημένη λίστα των κωδικών των τιμών των πεδίων της Αρχής τον πρώτο αριθμό v_i που αντιστοιχεί στην iοστή δεδομένη τιμή την οποία ο Prover θέλει να αποδείξει ότι δεν αποτελεί την τιμή ενός συγκεκριμένου πεδίου του πιστοποιητικού του.
  - Υπολογίζει $G = g^{\prod_{i=1}^{k} v_i} \bmod n$, όπου θεωρείται πως $G \neq 1$.
  - Στέλνει στον Prover το G.
- Prover
  - $\forall i \in \{1,..,k\}$ επιλέγει από τη δημοσιοποιημένη λίστα των κωδικών των τιμών των πεδίων της Αρχής τον πρώτο αριθμό v_i.

- Υπολογίζει $x, y \in \mathbb{Z}^*$ τέτοια ώστε $\left(\prod_{i=1}^{k} v_i\right) \cdot x + m_2 \cdot y = 1$. Ο υπολογισμός γίνεται εκτελώντας τον επεκτεινόμενο Ευκλείδειο αλγόριθμο με εισόδους τα $\prod_{i=1}^{k} v_i, m_2$.
- Υπολογίζει $-r \cdot y$.
- Εκτελεί με τον Verifier το πρωτόκολλο γνώσης διακριτών λογαρίθμων του g ως προς τις βάσεις D, G, g'.

- Verifier
  - Αν αποδειχτεί ότι ο Prover γνωρίζει διακριτούς λογαρίθμους του g ως προς τις βάσεις D, G, g', τότε αυτός κατέχει ένα έγκυρο πιστοποιητικό όπου οι τιμές των k συγκεκριμένων πεδίων του δεν είναι ίσες με τις k δεδομένες τιμές.

Απόδειξη

Αν οι k τιμές των συγκεκριμένων πεδίων του έγκυρου πιστοποιητικού του Prover διαφέρουν από τις k δεδομένες τιμές, τότε $\forall i \in \{1,..,k\}$ στο γινόμενο m_2 των πρώτων αριθμών στους οποίους είναι κωδικοποιημένες οι τιμές των πεδίων του πιστοποιητικού, δε θα περιέχεται ως παράγοντάς του ο πρώτος αριθμός v_i που αντιστοιχεί στην iοστή δεδομένη τιμή και επομένως δε θα το διαιρεί. Εφόσον $\forall i \in \{1,..,k\}$ ο πρώτος v_i δεν είναι διαιρέτης του m_2, τότε σύμφωνα με την Πρόταση 1 οι δύο αυτοί αριθμοί είναι πρώτοι μεταξύ τους και άρα λόγω της Πρότασης 5.1 το m_2 θα είναι πρώτο με το γινόμενο $\prod_{i=1}^{k} v_i$. Τότε λόγω της Πρότασης 3 θα $\exists x, y \in \mathbb{Z}^*$ ώστε να ισχύει

$$\left(\prod_{i=1}^{k} v_i\right) \cdot x + m_2 \cdot y = 1.$$

Τα x, y είναι διαφορετικά του 0 γιατί αλλιώς από την τελευταία εξίσωση θα προέκυπτε ότι το $\prod_{i=1}^{k} v_i$ ή το m_2 θα ήταν ίσο με 1 ή -1, κάτι που δεν ισχύει αφού αυτά είναι μεγαλύτερα του 1. Η απόδειξη του παρόντος πρωτοκόλλου είναι παρόμοια με αυτήν που δόθηκε στην προηγούμενη υποενότητα.

5.8. Zkp Πρωτόκολλο Πεδίου με Τιμή από ένα Δεδομένο Σύνολο Τιμών

[6] Στην υποενότητα αυτή παρουσιάζεται και αναλύεται ένα zkp πρωτόκολλο το οποίο χρησιμοποιεί ο Prover για να πείσει τον Verifier ότι η τιμή ενός πεδίου του έγκυρου πιστοποιητικού που κατέχει ανήκει σε ένα δεδομένο σύνολο τιμών. Η τιμή αυτού του πεδίου είναι η πληροφορία που σχετίζεται με τον προηγούμενο ισχυρισμό και θα πρέπει να συνεχίσει να παραμένει μυστική στον Verifier κατά τη διάρκεια και μετά το τέλος της εκτέλεσης του συγκεκριμένου πρωτοκόλλου. Όπως αναφέρθηκε στο τέλος της ενότητας 5, θεωρείται πως πριν την εκτέλεση του παρόντος πρωτοκόλλου έχει ήδη αποδειχτεί η εγκυρότητα του πιστοποιητικού του Prover μέσω του πρωτοκόλλου εγκυρότητας πιστοποιητικού. Ένα παράδειγμα χρήσης του

παρόντος πρωτοκόλλου θα ήταν η *περίπτωση* στην οποία ο ισχυρισμός θα είχε ως εξής: '*η τιμή του πεδίου της οικογενειακής κατάστασης είναι μία από τις 'Άγαμος', 'Έγγαμος χωρίς παιδιά', 'Έγγαμος με ένα παιδί'*'. Το δεδομένο σύνολο τιμών σε αυτήν την περίπτωση είναι το

{'*Άγαμος*','*Έγγαμος χωρίς παιδιά*','*Έγγαμος με ένα παιδί*'}.

Το πρωτόκολλο και η απόδειξη ότι πετυχαίνει τον σκοπό του παρουσιάζονται παρακάτω.

- Prover
  - Επιλέγει τυχαία $r \in \mathbb{Z}^*$ και από τη δημοσιοποιημένη λίστα των κωδικών των τιμών των πεδίων της Αρχής τον πρώτο αριθμό v που αντιστοιχεί στην τιμή ενός συγκεκριμένου πεδίου του πιστοποιητικού του, την οποία ο ίδιος θέλει να αποδείξει ότι ανήκει σε ένα δεδομένο σύνολο τιμών χωρίς να μπορεί αυτή να γίνει γνωστή στον Verifier.
  - Υπολογίζει $D = \left(g^v \cdot g'^r\right) \bmod n$ (131), έτσι ώστε $D \neq 1$, όπου g, g' είναι δημόσια γνωστά στοιχεία του $QR_n^* - \{1\}$ που υπολόγισε η Αρχή κατά τη φάση δημιουργίας παραμέτρων.
  - Επιλέγει τυχαία $s \in \mathbb{Z}^*$.
  - Υπολογίζει $D' = \left(f^v \cdot f'^s\right) \bmod P$ (132), έτσι ώστε $D' \neq 1$, όπου P είναι δημόσια γνωστός περιττός πρώτος αριθμός που υπολόγισε η Αρχή κατά τη φάση δημιουργίας παραμέτρων και f, f' είναι δημόσια γνωστά στοιχεία του $QR_P^* - \{1\}$ που δημιούργησε η Αρχή κατά την ίδια φάση.
  - Εκτελεί με τον Verifier το πρωτόκολλο ισότητας διακριτών λογαρίθμων διαφορετικών modulo των D, D' ως προς τις βάσεις g, f με αναπαραστάσεις στις βάσεις g, g' σε $\bmod n$ και f, f' σε $\bmod P$ αντίστοιχα.
- Verifier
  - Αν δεν αποδειχτεί ότι υπάρχει κοινός διακριτός λογάριθμος των D, D' ως προς τις βάσεις g, f με αναπαραστάσεις στις βάσεις g, g' σε $\bmod n$ και f, f' σε $\bmod P$ αντίστοιχα, τότε διακόπτει το παρών πρωτόκολλο.
- Prover
  - Υπολογίζει $x_1, x_2, y_1, y_2 \in \mathbb{Z}^*$ τέτοια ώστε

    $\begin{cases} P' \cdot x_1 + (v-1) \cdot y_1 = 1 \\ P' \cdot x_2 + (v+1) \cdot y_2 = 1 \end{cases}$ (133), όπου P' είναι δημόσια γνωστός περιττός πρώτος αριθμός που επέλεξε η Αρχή κατά τη φάση δημιουργίας παραμέτρων. Ο υπολογισμός των x_1, y_1 και x_2, y_2 γίνεται εκτελώντας δύο φορές τον επεκτεινόμενο Ευκλείδειο αλγόριθμο, την μία φορά με εισόδους τα $P', v-1$ και την άλλη τα $P', v+1$ αντίστοιχα.

- Υπολογίζει $\begin{cases} f^{-1} \\ G_1 = \left(D' \cdot f^{-1}\right) \bmod P \\ G_2 = \left(D' \cdot f\right) \bmod P \end{cases}$ (134), έτσι ώστε $G_1 \neq 1$ και $G_2 \neq 1$.
- Εκτελεί με τον Verifier το πρωτόκολλο γνώσης διακριτών λογαρίθμων modulo πρώτο αριθμό του f ως προς τις βάσεις G_1, f'.

- Verifier
  - Αν δεν αποδειχτεί ότι ο Prover γνωρίζει διακριτούς λογαρίθμους του f ως προς τις βάσεις G_1, f', τότε διακόπτει το παρών πρωτόκολλο.

- Prover
  - Εκτελεί με τον Verifier το πρωτόκολλο γνώσης διακριτών λογαρίθμων modulo πρώτο αριθμό του f ως προς τις βάσεις G_2, f'.

- Verifier
  - Αν δεν αποδειχτεί ότι ο Prover γνωρίζει διακριτούς λογαρίθμους του f ως προς τις βάσεις G_2, f', τότε διακόπτει το παρών πρωτόκολλο.

- Prover
  - Υπολογίζει $\begin{cases} d = \dfrac{m_2}{v} \\ -d \\ r \cdot d \end{cases}$, όπου m_2 είναι το γινόμενο των πρώτων αριθμών στους οποίους είναι κωδικοποιημένες οι τιμές των πεδίων του πιστοποιητικού του.
  - Εκτελεί με τον Verifier το πρωτόκολλο ισότητας διακριτών λογαρίθμων των $Z,1$ ως προς τις βάσεις R_2, g με αναπαραστάσεις στις βάσεις A', R_1, R_2, S και D, g, g' αντίστοιχα. Το A' είναι υπολογισμένο από το πρωτόκολλο εγκυρότητας πιστοποιητικού που εκτέλεσε προηγούμενα με τον Verifier για να αποδείξει ότι κατέχει ένα έγκυρο πιστοποιητικό.

- Verifier
  - Αν δεν αποδειχτεί ότι υπάρχει κοινός διακριτός λογάριθμος των $Z,1$ ως προς τις βάσεις R_2, g με αναπαραστάσεις στις βάσεις A', R_1, R_2, S και D, g, g' αντίστοιχα, τότε διακόπτει το παρών πρωτόκολλο.
  - $\forall i \in \{1,..,l\}$, όπου $l \in \mathbb{N}^* - \{1\}$ είναι ο αριθμός των τιμών του δεδομένου συνόλου, επιλέγει από τη δημοσιοποιημένη λίστα των κωδικών των τιμών των πεδίων της Αρχής τον πρώτο αριθμό e_i που αντιστοιχεί στην i οστή τιμή του συνόλου.
  - Υπολογίζει $G = g^{\prod_{i=1}^{l} e_i} \bmod n$ (135), όπου θεωρείται πως $G \neq 1$.
  - Στέλνει στον Prover το G.

- Prover
  - $\forall i \in \{1,..,l\}$ επιλέγει από τη δημοσιοποιημένη λίστα των κωδικών των τιμών των πεδίων της Αρχής τον πρώτο αριθμό e_i.
  - Υπολογίζει $\begin{cases} d' = \dfrac{\prod_{i=1}^{l} e_i}{v} \\ -r \cdot d' \end{cases}$.
  - Εκτελεί με τον Verifier το πρωτόκολλο γνώσης διακριτών λογαρίθμων του G ως προς τις βάσεις D, g'.
- Verifier
  - Αν αποδειχτεί ότι ο Prover γνωρίζει διακριτούς λογαρίθμους του G ως προς τις βάσεις D, g', τότε αυτός κατέχει ένα έγκυρο πιστοποιητικό όπου η τιμή του συγκεκριμένου πεδίου του ανήκει στο δεδομένο σύνολο τιμών.

Απόδειξη

Εφόσον ο Prover προηγουμένως εκτέλεσε με επιτυχία το πρωτόκολλο εγκυρότητας πιστοποιητικού, τότε θα ισχύει

$$Z = \left(A'^{e} \cdot R_1^{m_1} \cdot R_2^{m_2} \cdot S^{v'}\right) \bmod n \quad (101).$$

Στο γινόμενο m_2 των πρώτων αριθμών στους οποίους είναι κωδικοποιημένες οι τιμές των πεδίων του πιστοποιητικού, θα περιέχεται ως παράγοντάς του ο πρώτος αριθμός v που αντιστοιχεί στην τιμή του συγκεκριμένου πεδίου, δηλαδή θα $\exists d \in \mathbb{N}^*$ ώστε να είναι

$$m_2 = v \cdot d \quad (136).$$

1. Το πρωτόκολλο τηρείται ανεξάρτητα εάν η τιμή του συγκεκριμένου πεδίου του έγκυρου πιστοποιητικού του Prover ανήκει ή δεν ανήκει στο δεδομένο σύνολο τιμών

Σε αυτήν την περίπτωση ο Prover θα υπολογίσει κανονικά σύμφωνα με το πρωτόκολλο τα D, D' από τις σχέσεις

$$D = \left(g^{v} \cdot g''^{r}\right) \bmod n \quad (131),\ D' = \left(f^{v} \cdot f'^{s}\right) \bmod P \quad (132).$$

Εφόσον $g, g' \in QR_n^*$ και $f, f' \in QR_P^*$, σύμφωνα με τις (131), (132) και την Πρόταση 20.3 θα ισχύει αντίστοιχα $D \in QR_n^*$ και $D' \in QR_P^*$. Επίσης, επειδή $D \neq 1$ και $D' \neq 1$, τότε $D \in QR_n^* - \{1\}$ και $D' \in QR_P^* - \{1\}$. Ο Prover γνωρίζει ότι τα γνωστά σε αυτόν v, r αποτελούν διακριτούς λογαρίθμους $\bmod n$ του D ως προς τις βάσεις g, g' αντίστοιχα, όπως φαίνεται από την (131). Επίσης γνωρίζει ότι τα γνωστά σε αυτόν v, s αποτελούν διακριτούς λογαρίθμους $\bmod P$ του D' ως προς τις βάσεις f, f' αντίστοιχα, όπως φαίνεται από την (132). Έτσι ξέρει πως όταν τα D, D' αναπαρίστανται στις βάσεις $g, g' \in QR_n^* - \{1\}$ σε $\bmod n$ και $f, f' \in QR_P^* - \{1\}$ σε $\bmod P$ αντίστοιχα, τότε ένας κοινός τους λογάριθμος ως προς τις βάσεις g, f αντιστοίχως είναι το v. Αυτό σημαίνει πως θα εκτελέσει με επιτυχία το πρωτόκολλο ισότητας λογαρίθμων διαφορετικών modulo, αποδεικνύοντας στον Verifier την ύπαρξη κοινού λογαρίθμου όπως ο v χωρίς όμως ο συγκεκριμένος να γίνει γνωστός

σε αυτόν. Από τη στιγμή που οι αναπαραστάσεις των D, D' στις βάσεις g, g' και f, f' αντίστοιχα είναι σε διαφορετικά modulo, χρησιμοποιείται το πρωτόκολλο ισότητας λογαρίθμων διαφορετικών modulo και όχι εκείνο που περιγράφεται στην υποενότητα 5.3 στο οποίο οι δύο αναπαραστάσεις πρέπει να είναι σε ένα κοινό modulo. Το πρωτόκολλο ισότητας λογαρίθμων διαφορετικών modulo, που αναπτύσσεται στο paper της αναφοράς [9], δεν παρουσιάζεται και αναλύεται στην παρούσα εργασία.

Όπως αναφέρθηκε στην υποενότητα 4.1, ισχύει

$$P' > v_{\max} + 1,$$

όπου σύμφωνα με την υποενότητα 4.2 $v_{\max}$ είναι ο μέγιστος από όλους τους πρώτους αριθμούς στους οποίους είναι κωδικοποιημένες όλες οι τιμές που μπορούν να λάβουν όλα τα πεδία ενός πιστοποιητικού. Τότε για κάθε τέτοιον πρώτο αριθμό u θα ισχύει λόγω της τελευταίας ανισότητας ότι

$$u \le v_{\max} \Rightarrow u+1 \le v_{\max}+1 < P' \Rightarrow u-1 < u+1 < P' \Rightarrow \begin{cases} u+1 < P' \\ u-1 < P' \end{cases}.$$

Για $u = v$ θα ισχύει

$$\begin{cases} v+1 < P' \\ v-1 < P' \end{cases}$$

και συνεπώς εφόσον το P' είναι πρώτος αριθμός, τα $P', v+1$ θα είναι πρώτοι μεταξύ τους όπως επίσης και τα $P', v-1$. Τότε λόγω της Πρότασης 3 $\exists x_1, y_1, x_2, y_2 \in \mathbb{Z}$ ώστε να ισχύει

$$\begin{cases} P' \cdot x_1 + (v-1) \cdot y_1 = 1 \\ P' \cdot x_2 + (v+1) \cdot y_2 = 1 \end{cases} \quad (133).$$

Ο Prover μπορεί να υπολογίσει τα x_1, y_1, x_2, y_2 εφόσον γνωρίζει το v και το δημόσια γνωστό P'. Εφόσον το πρωτόκολλο τηρείται θα υπολογίσει κανονικά σύμφωνα με αυτό τα G_1, G_2 από τις σχέσεις

$$\begin{cases} G_1 = \left(D' \cdot f^{-1}\right) \bmod P \\ G_2 = \left(D' \cdot f\right) \bmod P \end{cases} \quad (134).$$

Όπως αναφέρθηκε στην υποενότητα 4.1, η τάξη του f ως προς P είναι ίση με P'. Επομένως θα ισχύει

$$f^{P'} \equiv 1 \bmod P \quad (137).$$

Από την (133) συνεπάγεται ότι

$$\begin{cases} P' \cdot x_1 = 1 - (v-1) \cdot y_1 \\ P' \cdot x_2 = 1 - (v+1) \cdot y_2 \end{cases} \quad (138).$$

Η (137) συνεπάγεται ότι

$$\begin{cases} \left(f^{P'}\right)^{x_1} \equiv 1 \bmod P \\ \left(f^{P'}\right)^{x_2} \equiv 1 \bmod P \end{cases} \Rightarrow \begin{cases} f^{P' \cdot x_1} \equiv 1 \bmod P \\ f^{P' \cdot x_2} \equiv 1 \bmod P \end{cases} \xrightarrow{(138)} \begin{cases} f^{1-(v-1) \cdot y_1} \equiv 1 \bmod P \\ f^{1-(v+1) \cdot y_2} \equiv 1 \bmod P \end{cases} \Rightarrow$$

$$\begin{cases} f \cdot f^{-(v-1) \cdot y_1} \equiv 1 \bmod P \\ f \cdot f^{-(v+1) \cdot y_2} \equiv 1 \bmod P \end{cases} \Rightarrow \begin{cases} f \equiv f^{(v-1) \cdot y_1} \bmod P \\ f \equiv f^{(v+1) \cdot y_2} \bmod P \end{cases} \quad (139).$$

Η (132) συνεπάγεται ότι

$$\begin{cases} D'^{y_1} \equiv \left(f^{v} \cdot f'^{s} \right)^{y_1} \bmod P = \left(\left(f^{v} \right)^{y_1} \cdot \left(f'^{s} \right)^{y_1} \right) \bmod P \Rightarrow D'^{y_1} \equiv \left(f^{v \cdot y_1} \cdot f'^{s \cdot y_1} \right) \bmod P \\ D'^{y_2} \equiv \left(f^{v} \cdot f'^{s} \right)^{y_2} \bmod P = \left(\left(f^{v} \right)^{y_2} \cdot \left(f'^{s} \right)^{y_2} \right) \bmod P \Rightarrow D'^{y_2} \equiv \left(f^{v \cdot y_2} \cdot f'^{s \cdot y_2} \right) \bmod P \end{cases} \Rightarrow$$

$$\begin{cases} \left(D'^{y_1} \cdot f'^{-s \cdot y_1} \right) \equiv f^{v \cdot y_1} \bmod P \\ \left(D'^{y_2} \cdot f'^{-s \cdot y_2} \right) \equiv f^{v \cdot y_2} \bmod P \end{cases} \Rightarrow$$

$$\begin{cases} \left(D'^{y_1} \cdot f'^{-s \cdot y_1} \cdot f^{-y_1} \right) \equiv \left(f^{v \cdot y_1} \cdot f^{-y_1} \right) \bmod P = f^{v \cdot y_1 - y_1} \bmod P = f^{(v-1) \cdot y_1} \bmod P \\ \left(D'^{y_2} \cdot f'^{-s \cdot y_2} \cdot f^{y_2} \right) \equiv \left(f^{v \cdot y_2} \cdot f^{y_2} \right) \bmod P = f^{v \cdot y_2 + y_2} \bmod P = f^{(v+1) \cdot y_2} \bmod P \end{cases} \xrightarrow{(139)}$$

$$\begin{cases} \left(D'^{y_1} \cdot f'^{-s \cdot y_1} \cdot f^{-y_1} \right) \equiv f \bmod P \\ \left(D'^{y_2} \cdot f'^{-s \cdot y_2} \cdot f^{y_2} \right) \equiv f \bmod P \end{cases} \Rightarrow \begin{cases} f \equiv \left(D'^{y_1} \cdot f^{-y_1} \cdot f'^{-s \cdot y_1} \right) \bmod P \\ f \equiv \left(D'^{y_2} \cdot f^{y_2} \cdot f'^{-s \cdot y_2} \right) \bmod P \end{cases} \Rightarrow$$

$$\begin{cases} f \equiv \left(\left(D' \cdot f^{-1} \right)^{y_1} \cdot f'^{-s \cdot y_1} \right) \bmod P \\ f \equiv \left(\left(D' \cdot f \right)^{y_2} \cdot f'^{-s \cdot y_2} \right) \bmod P \end{cases} \quad (140).$$

Η (134) συνεπάγεται ότι

$$\begin{cases} G_1^{\,y_1} \equiv \left(D' \cdot f^{-1} \right)^{y_1} \bmod P \\ G_2^{\,y_2} \equiv \left(D' \cdot f \right)^{y_2} \bmod P \end{cases} \Rightarrow \begin{cases} \left(G_1^{\,y_1} \cdot f'^{-s \cdot y_1} \right) \equiv \left(\left(D' \cdot f^{-1} \right)^{y_1} \cdot f'^{-s \cdot y_1} \right) \bmod P \\ \left(G_2^{\,y_2} \cdot f'^{-s \cdot y_2} \right) \equiv \left(\left(D' \cdot f \right)^{y_2} \cdot f'^{-s \cdot y_2} \right) \bmod P \end{cases} \xrightarrow{(140)}$$

$$\begin{cases} \left(G_1^{\,y_1} \cdot f'^{-s \cdot y_1} \right) \equiv f \bmod P \\ \left(G_2^{\,y_2} \cdot f'^{-s \cdot y_2} \right) \equiv f \bmod P \end{cases} \Rightarrow \begin{cases} f = \left(G_1^{\,y_1} \cdot f'^{-s \cdot y_1} \right) \bmod P \\ f = \left(G_2^{\,y_2} \cdot f'^{-s \cdot y_2} \right) \bmod P \end{cases} \quad (141),$$

αφού $f \in QR_P^*$ και άρα $f \in \mathbb{Z}_P^*$ που σημαίνει πως $f < P$. Εφόσον ο Prover έχει υπολογίσει το y_1 το ξέρει και άρα στην πρώτη εξίσωση της (141) γνωρίζει έναν διακριτό λογάριθμο του f ως προς το G_1. Επίσης ξέρει το s και άρα μπορεί να υπολογίσει το γινόμενο $-s \cdot y_1$ και να μάθει στην ίδια εξίσωση έναν διακριτό λογάριθμο του f ως προς το f'. Εφόσον το P είναι περιττός πρώτος αριθμός θα είναι $P \geq 3 > 2$ και επειδή $f \in QR_P^*$, τότε σύμφωνα με την Πρόταση 19 θα ισχύει $f^{-1} \in QR_P^*$. Επίσης όπως αποδείχτηκε προηγούμενα $D' \in QR_P^*$, οπότε σύμφωνα με την πρώτη εξίσωση της (134) και την Πρόταση 20.1 θα ισχύει $G_1 \in QR_P^*$. Επειδή $G_1 \neq 1$, τότε $G_1 \in QR_P^* - \{1\}$. Από τη στιγμή που ο Prover ξέρει διακριτούς λογαρίθμους του f ως προς τις βάσεις $G_1, f' \in QR_P^* - \{1\}$, θα αποδείξει τη γνώση του αυτή στον Verifier όταν και οι δύο χρησιμοποιήσουν το zkp πρωτόκολλο γνώσης διακριτών λογαρίθμων modulo πρώτο αριθμό του f ως προς αυτές τις βάσεις. Η απόδειξη θα γίνει χωρίς να αποκαλυφθούν άμεσα ή έμμεσα στον Verifier οι συγκεκριμένοι λογάριθμοι που γνωρίζει ο Prover.

Εφόσον ο τελευταίος έχει υπολογίσει το y_2 το ξέρει και άρα στη δεύτερη εξίσωση της (141) γνωρίζει έναν διακριτό λογάριθμο του f ως προς το G_2. Επίσης ξέρει το s και άρα μπορεί να υπολογίσει το γινόμενο $-s \cdot y_2$ και να μάθει στην ίδια εξίσωση έναν διακριτό λογάριθμο του f ως προς το f'. Επειδή $f, D' \in QR_P^*$, τότε σύμφωνα

με τη δεύτερη εξίσωση της (134) και την Πρόταση 20.1 θα ισχύει $G_2 \in QR_P^*$. Επίσης επειδή $G_2 \neq 1$, τότε $G_2 \in QR_P^* - \{1\}$. Από τη στιγμή που ο Prover ξέρει διακριτούς λογαρίθμους του f ως προς τις βάσεις G_2, $f' \in QR_P^* - \{1\}$, θα αποδείξει τη γνώση του αυτή στον Verifier όταν και οι δύο χρησιμοποιήσουν το zkp πρωτόκολλο γνώσης διακριτών λογαρίθμων modulo πρώτο αριθμό του f ως προς αυτές τις βάσεις. Η απόδειξη θα γίνει χωρίς να αποκαλυφθούν άμεσα ή έμμεσα στον Verifier οι συγκεκριμένοι λογάριθμοι που γνωρίζει ο Prover.
Η (131) συνεπάγεται ότι

$$D^d \equiv \left(g^v \cdot g'^r\right)^d \bmod n = \left(\left(g^v\right)^d \cdot \left(g'^r\right)^d\right) \bmod n = \left(g^{v \cdot d} \cdot g'^{r \cdot d}\right) \bmod n \xrightarrow{(136)}$$

$$D^d \equiv \left(g^{m_2} \cdot g'^{r \cdot d}\right) \bmod n \Rightarrow 1 = \left(D^{-d} \cdot g^{m_2} \cdot g'^{r \cdot d}\right) \bmod n \ (142).$$

Ο Prover μπορεί να υπολογίσει το

$$-d = -\frac{m_2}{v},$$

εφόσον γνωρίζει τα m_2, v και έτσι να μάθει στην (142) έναν διακριτό λογάριθμο του 1 ως προς το D. Επίσης από τη στιγμή που ξέρει το r μπορεί να υπολογίσει το $r \cdot d$ και να μάθει στην ίδια σχέση έναν διακριτό λογάριθμο του 1 ως προς το g'. Τέλος από τη στιγμή που ξέρει το m_2 γνωρίζει έναν λογάριθμο του 1 ως προς το g στην (142). Ο Prover ξέρει ότι τα γνωστά σε αυτόν e, m_1, m_2, v' αποτελούν διακριτούς λογαρίθμους του Z ως προς τις βάσεις A', R_1, R_2, S αντίστοιχα, όπως φαίνεται από την (101). Έτσι γνωρίζει πως όταν τα $Z, 1$ αναπαρίστανται στις βάσεις $A', R_1, R_2, S \in QR_n^* - \{1\}$ και $D, g, g' \in QR_n^* - \{1\}$ αντίστοιχα, τότε ένας κοινός τους λογάριθμος ως προς τις βάσεις R_2, g αντιστοίχως είναι το m_2. Αυτό σημαίνει πως θα εκτελέσει με επιτυχία το πρωτόκολλο ισότητας λογαρίθμων, αποδεικνύοντας στον Verifier την ύπαρξη κοινού λογαρίθμου όπως ο m_2 χωρίς όμως ο συγκεκριμένος να γίνει γνωστός σε αυτόν. Εφόσον το πρωτόκολλο τηρείται ο Verifier θα υπολογίσει κανονικά σύμφωνα με αυτό το G από τη σχέση

$$G = g^{\prod_{i=1}^{l} e_i} \bmod n \ (135).$$

Επειδή $g \in QR_n^*$, σύμφωνα με την (135) και την Πρόταση 20.2 θα ισχύει $G \in QR_n^*$ και επειδή $G \neq 1$, τότε $G \in QR_n^* - \{1\}$.

1.1. <u>Η τιμή του συγκεκριμένου πεδίου του έγκυρου πιστοποιητικού του Prover ανήκει στο δεδομένο σύνολο τιμών</u>

Σε αυτήν την υποπερίπτωση ο πρώτος αριθμός v που αντιστοιχεί στην τιμή του συγκεκριμένου πεδίου θα είναι ένας από τους πρώτους αριθμούς στους οποίους αντιστοιχίζονται οι τιμές αυτού του δεδομένου συνόλου, δηλαδή

$$v \in \{e_1, .., e_l\}.$$

Επομένως στο γινόμενο $\prod_{i=1}^{l} e_i$ το v θα περιέχεται ως παράγοντάς του και άρα θα $\exists d' \in \mathbb{N}^*$ ώστε να είναι

$$\prod_{i=1}^{l} e_i = v \cdot d'.$$

Λόγω της τελευταίας εξίσωσης η (135) γίνεται

$$G = g^{v \cdot d'} \bmod n \quad (143).$$

Η (131) συνεπάγεται ότι

$$D^{d'} \equiv \left(g^{v} \cdot g'^{r}\right)^{d'} \bmod n = \left(\left(g^{v}\right)^{d'} \cdot \left(g'^{r}\right)^{d'}\right) \bmod n \Rightarrow D^{d'} \equiv \left(g^{v \cdot d'} \cdot g'^{r \cdot d'}\right) \bmod n \Rightarrow$$

$$\left(D^{d'} \cdot g'^{-r \cdot d'}\right) \equiv g^{v \cdot d'} \bmod n \xrightarrow{(143)} \left(D^{d'} \cdot g'^{-r \cdot d'}\right) \equiv G \bmod n \Rightarrow$$

$$G = \left(D^{d'} \cdot g'^{-r \cdot d'}\right) \bmod n \quad (144),$$

αφού $G \in QR_n^*$ και άρα $G \in \mathbb{Z}_n^*$ που σημαίνει πως $G < n$. Ο Prover μαθαίνει το G όταν το λαμβάνει από τον Verifier. Εφόσον γνωρίζει ποιες είναι οι τιμές του δεδομένου συνόλου, μπορεί να βρει τα $e_1,..,e_l$ και επομένως να υπολογίσει το $\prod_{i=1}^{l} e_i$.

Επίσης ξέρει το v και άρα μπορεί να υπολογίσει το

$$d' = \frac{\prod_{i=1}^{l} e_i}{v}$$

και να μάθει στην (144) έναν διακριτό λογάριθμο του G ως προς το D. Εφόσον γνωρίζει το r, μπορεί να υπολογίσει το $-r \cdot d'$ μαθαίνοντας στην ίδια σχέση έναν λογάριθμο του G ως προς το g'. Από τη στιγμή που ο Prover ξέρει διακριτούς λογαρίθμους του G ως προς τις βάσεις $D, g' \in QR_n^* - \{1\}$, θα αποδείξει τη γνώση του αυτή στον Verifier όταν και οι δύο χρησιμοποιήσουν το zkp πρωτόκολλο γνώσης διακριτών λογαρίθμων του G ως αυτές τις βάσεις. Η απόδειξη θα γίνει χωρίς να αποκαλυφθούν άμεσα ή έμμεσα στον Verifier οι συγκεκριμένοι διακριτοί λογάριθμοι που ξέρει ο Prover.

1.2. <u>Η τιμή του συγκεκριμένου πεδίου του έγκυρου πιστοποιητικού του Prover δεν ανήκει στο δεδομένο σύνολο τιμών</u>

Σε αυτήν την υποπερίπτωση ο πρώτος αριθμός v που αντιστοιχεί στην τιμή του συγκεκριμένου πεδίου δε θα είναι ένας από τους πρώτους αριθμούς στους οποίους αντιστοιχίζονται οι τιμές αυτού του δεδομένου συνόλου, δηλαδή

$$v \notin \{e_1,..,e_l\}.$$

Επομένως στο γινόμενο $\prod_{i=1}^{l} e_i$ το v δε θα περιέχεται ως πρώτος παράγοντάς του και άρα δε θα το διαιρεί, δηλαδή δε θα $\exists d' \in \mathbb{N}^*$ ώστε να είναι

$$\prod_{i=1}^{l} e_i = v \cdot d'.$$

Από τη στιγμή που ο Prover αδυνατεί να βρει κάποιο $d' \in \mathbb{N}^*$ ώστε να ισχύει

$$d' = \frac{\prod_{i=1}^{l} e_i}{v}$$

όπως έκανε πριν, δε θα μπορέσει να ακολουθήσει την προηγούμενη διαδικασία προκειμένου να πληροφορηθεί διακριτούς λογαρίθμους του G ως προς τις βάσεις D, g'. Θα δειχτεί ότι σχεδόν κατά 100% αυτός δε γνωρίζει τέτοιους λογαρίθμους. Τίθεται ο ισχυρισμός πως γνωρίζει κάποιους.

Σχεδόν σίγουρα η γνώση αυτών δε θα προήλθε προσπαθώντας ο ίδιος να λύσει την εξίσωση

$$G = \left(D^{x_3} \cdot g'^{x_4} \right) \bmod n \quad (145)$$

ως προς $x_3, x_4 \in \mathbb{Z}^*$, καθώς κάτι τέτοιο θα ήταν πάρα πολύ δύσκολο σύμφωνα με το Δεύτερο Ισχυρισμό Διακριτού Λογαρίθμου.

Λαμβάνοντας υπόψη του ότι ισχύουν οι (131), (135), μια δεύτερη εναλλακτική οδός που πιθανόν θα τον οδηγούσε στη γνώση αυτών των λογαρίθμων θα ήταν να ακολουθούσε τις παρακάτω συνεπαγωγές προκειμένου να συμπεράνει τη συνθήκη που θα έπρεπε να τηρούν τα x_3, x_4. Από την (131) συνεπάγεται πως

$$D^{x_3} \equiv \left(g^{v} \cdot g'^{r} \right)^{x_3} \bmod n = \left(\left(g^{v} \right)^{x_3} \cdot \left(g'^{r} \right)^{x_3} \right) \bmod n \Rightarrow D^{x_3} \equiv \left(g^{v \cdot x_3} \cdot g'^{r \cdot x_3} \right) \bmod n \Rightarrow$$

$$\left(D^{x_3} \cdot g'^{x_4} \right) \equiv \left(g^{v \cdot x_3} \cdot g'^{r \cdot x_3} \cdot g'^{x_4} \right) \bmod n \xrightarrow{(145)}$$

$$G = \left(g^{v \cdot x_3} \cdot g'^{r \cdot x_3} \cdot g'^{x_4} \right) \bmod n \xrightarrow{(135)} g^{\prod_{i=1}^{l} e_i} \equiv \left(g^{v \cdot x_3} \cdot g'^{r \cdot x_3 + x_4} \right) \bmod n \Rightarrow$$

$$\left(g^{\prod_{i=1}^{l} e_i} \cdot g^{-v \cdot x_3} \right) \equiv g'^{r \cdot x_3 + x_4} \bmod n \Rightarrow g^{\prod_{i=1}^{l} e_i - v \cdot x_3} \equiv g'^{r \cdot x_3 + x_4} \bmod n \quad (146).$$

Σύμφωνα με την (64) που αναφέρεται στην υποενότητα 4.1, ισχύει

$$g' = g^{l_{g'}} \bmod n,$$

όπου το $l_{g'} \in \{2, .., p' \cdot q' - 1\}$ κρατείται μυστικό από την Αρχή. Έτσι ο Prover δεν το ξέρει και πάρα πολύ δύσκολα θα μπορούσε να το υπολογίσει από την τελευταία εξίσωση λόγω του Πρώτου Ισχυρισμού Διακριτού Λογαρίθμου. Επίσης όπως αναφέρεται στην ίδια υποενότητα, η τάξη του g ως προς n είναι ίση με $p' \cdot q'$. Λόγω της (64) συνεπάγεται πως

$$g'^{r \cdot x_3 + x_4} \equiv \left(g^{l_{g'}} \right)^{r \cdot x_3 + x_4} \bmod n \xrightarrow{(146)} g^{\prod_{i=1}^{l} e_i - v \cdot x_3} \equiv g^{l_{g'} \cdot (r \cdot x_3 + x_4)} \bmod n.$$

Σύμφωνα με την Πρόταση 15.2 και αφού η τάξη του g ως προς n ισούται με $p' \cdot q'$, προκύπτει από την τελευταία ισοδυναμία πως

$$\left(\prod_{i=1}^{l} e_i - v \cdot x_3 - l_{g'} \cdot \left(r \cdot x_3 + x_4 \right) \right) \equiv 0 \bmod \left(p' \cdot q' \right).$$

Δηλαδή $\exists d_1 \in \mathbb{Z}$ ώστε

$$\prod_{i=1}^{l} e_i - v \cdot x_3 - l_{g'} \cdot \left(r \cdot x_3 + x_4 \right) = p' \cdot q' \cdot d_1.$$

Από την τελευταία εξίσωση προκύπτει πως η συνθήκη που πρέπει να ικανοποιούν τα x_3, x_4 είναι ότι το

$$\prod_{i=1}^{l} e_i - v \cdot x_3 - l_{g'} \cdot \left(r \cdot x_3 + x_4 \right)$$

θα πρέπει να είναι πολλαπλάσιο του $p' \cdot q'$, το οποίο με τη σειρά του να σημειωθεί ότι είναι διάφορο του 0 αφού τα p', q' είναι πρώτοι αριθμοί. Επειδή ο Prover δε τα γνωρίζει, αφού αυτά κρατούνται μυστικά από την εκδότρια Αρχή, τότε δε θα μπορούσε να υπολογίσει το γινόμενό τους $p' \cdot q'$ και να βρει ένα μη μηδενικό πολλαπλάσιό του, ώστε αρχικά να το δοκιμάσει εάν θα μπορούσε να αποτελέσει τιμή του

$$\prod_{i=1}^{l} e_i - v \cdot x_3 - l_{g'} \cdot \left(r \cdot x_3 + x_4 \right)$$

και αν ναι μετά να δοκιμάσει αν τα x_3, x_4 που θα είχε υπολογίσει ικανοποιούσαν την (145). Έτσι η μόνη επιλογή του θα ήταν το μηδενικό πολλαπλάσιο, οπότε για $d_1 = 0$ θα μετασχημάτιζε την παραπάνω εξίσωση στη σχέση

$$\prod_{i=1}^{l} e_i - v \cdot x_3 - l_{g'} \cdot \left(r \cdot x_3 + x_4 \right) = 0$$

η οποία λόγω του ότι $l_{g'} \in \{2,.., p' \cdot q' - 1\}$ και άρα $l_{g'} \neq 0$, θα ισοδυναμεί με

$$\prod_{i=1}^{l} e_i - v \cdot x_3 = l_{g'} \cdot \left(r \cdot x_3 + x_4 \right) \Leftrightarrow r \cdot x_3 + x_4 = \left(\prod_{i=1}^{l} e_i - v \cdot x_3 \right) \cdot \frac{1}{l_{g'}} \Rightarrow$$

$$x_4 = \left(\prod_{i=1}^{l} e_i - v \cdot x_3 \right) \cdot \frac{1}{l_{g'}} - r \cdot x_3 \text{ (147).}$$

Ο Prover θα επέλεγε τυχαία κάποιο $x_3 \in \mathbb{Z}^*$ και θα προσπαθούσε να επιλύσει ως προς x_4 την (147). Επειδή όπως αναφέρθηκε προηγούμενα δεν $\exists d' \in \mathbb{N}^*$ ώστε

$$\prod_{i=1}^{l} e_i = v \cdot d'$$

και άρα ισοδύναμα

$$\prod_{i=1}^{l} e_i - v \cdot d' = 0,$$

τότε για οποιαδήποτε τυχαία επιλογή του $x_3 \in \mathbb{Z}^*$ εκ μέρους του Prover, θα ίσχυε ότι

$$\prod_{i=1}^{l} e_i - v \cdot x_3 \neq 0 \text{ (148).}$$

Στην (147) η μόνη παράμετρος που θα του ήταν άγνωστη εκτός του x_4 θα ήταν το $l_{g'}$ που όπως προαναφέρθηκε πάρα πολύ δύσκολα θα μπορούσε να υπολογίσει. Από τη στιγμή που θα ίσχυε η (148), τότε το γινόμενο

$$\left(\prod_{i=1}^{l} e_i - v \cdot x_3 \right) \cdot \frac{1}{l_{g'}}$$

θα του ήταν επίσης άγνωστο με αποτέλεσμα να αδυνατούσε να επιλύσει την (147) ως προς x_4. Επομένως ο Prover θα δε θα μπορούσε να υπολογίσει κάποια $x_3, x_4 \in \mathbb{Z}^*$ που να τηρούσαν την παραπάνω συνθήκη ώστε μετά να δοκιμάσει αν αυτά ικανοποιούσαν την (145). Έτσι αν ακολουθούσε τη δεύτερη εναλλακτική οδό σχεδόν κατά 100% δε θα μπορούσε να λάβει γνώση κάποιων διακριτών λογαρίθμων του G ως προς τις βάσεις D, g'.

Συνεπώς σχεδόν σίγουρα με κανέναν τρόπο δε θα μπορούσε ο Prover να πληροφορηθεί διακριτούς λογαρίθμους του G ως προς αυτές τις βάσεις και έτσι ο παραπάνω ισχυρισμός που τέθηκε δεν αληθεύει σχεδόν κατά 100%. Επομένως όταν η τιμή του συγκεκριμένου πεδίου του πιστοποιητικού δεν ανήκει στο δεδομένο σύνολο τιμών, ο Prover σχεδόν σίγουρα δε γνωρίζει διακριτούς λογαρίθμους του G ως προς τις βάσεις D, g'. Εφόσον σύμφωνα με την υπόθεση τηρείται το παρών πρωτόκολλο, ο Prover θα εκτελέσει κανονικά όπως προβλέπεται με τον Verifier το πρωτόκολλο γνώσης διακριτών λογαρίθμων του G ως προς τις παραπάνω βάσεις και το αποτέλεσμα θα είναι σχεδόν κατά 100% ανεπιτυχές για τον ίδιο.

2. <u>Η τιμή του συγκεκριμένου πεδίου του πιστοποιητικού δεν ανήκει στο δεδομένο σύνολο τιμών και ο Prover επιλέγει να μην τηρήσει το πρωτόκολλο</u>

Σε αυτήν την περίπτωση ο Prover ενεργεί έτσι προκειμένου να ξεγελάσει τον Verifier ώστε να τον πείσει για τον ψευδή ισχυρισμό του. Μια δυνατότητα που έχει για να λειτουργήσει αντικανονικά είναι να μην εκτελέσει όπως προβλέπεται το πρωτόκολλο γνώσης διακριτών λογαρίθμων του G ως προς τις βάσεις D, g', αφού προηγουμένως έχει τηρήσει όλα τα βήματα. Αν το εκτελούσε κανονικά, τότε όπως αναφέρθηκε προηγούμενα το αποτέλεσμα θα ήταν για τον ίδιο ανεπιτυχές αφού τιμή του συγκεκριμένου πεδίου του πιστοποιητικού δεν ανήκει στο δεδομένο σύνολο τιμών. Θα μπορούσε επομένως να αλλοιώσει κάποια από τα G, D, g' ώστε να εκτελέσει αυτό το πρωτόκολλο με διαφορετικές παραμέτρους που θα του εξασφάλιζαν το επιτυχές για αυτόν αποτέλεσμα. Όμως και οι τρεις προηγούμενες παράμετροι είναι γνωστές στον Verifier, το g' ως δημοσιοποιημένο από την Αρχή, το D από τα δύο πρωτόκολλα ισότητας διακριτών λογαρίθμων που εκτέλεσε προηγούμενα με τον Prover και το G επειδή το υπολόγισε ο ίδιος από τη σχέση (135). Έτσι όταν του κοινοποιηθούν οι αλλοιωμένες παράμετροι από τον Prover στην αρχή της εκτέλεσης του τελευταίου πρωτοκόλλου γνώσης διακριτών λογαρίθμων, αυτός θα τις εντοπίσει, θα καταλάβει ότι αυτό δεν τηρείται από τον Prover και θα διακόψει τη συμμετοχή του σε αυτό μην μπορώντας στο τέλος να διαπιστώσει εάν ο ισχυρισμός του Prover είναι αληθής.

Από την άλλη, λαμβάνοντας υπόψη ο Prover πως το G που θα του στείλει ο Verifier δίνεται από τη σχέση

$$G = g^{\prod_{i=1}^{l} e_i} \bmod n \quad (135),$$

θα μπορούσε να προσπαθήσει να υπολογίσει ένα τέτοιο D ώστε για κάποια $x_3, x_4 \in \mathbb{Z}^*$ που θα επέλεγε να ίσχυε η σχέση

$$G = \left(D^{x_3} \cdot g'^{x_4}\right) \bmod n \quad (145),$$

ώστε να μπορούσε μετά να εκτελέσει επιτυχώς το τελευταίο πρωτόκολλο γνώσης διακριτών λογαρίθμων αφού τα x_3, x_4 που θα ήξερε θα αποτελούσαν διακριτούς λογαρίθμους του G ως προς τις βάσεις D, g'. Συγκεκριμένα το D που θα υπολόγιζε θα έπρεπε να ήταν της μορφής

$$D = \left(g^{x_5} \cdot g''^{r}\right) \bmod n \quad (149)$$

για κάποια $x_5, r \in \mathbb{Z}^*$, γιατί διαφορετικά θα εκτελούσε ανεπιτυχώς το πρωτόκολλο ισότητας διακριτών λογαρίθμων διαφορετικών modulo και έτσι το πρωτόκολλο που εξετάζεται σε αυτήν την υποενότητα θα διακοπτόταν από τον Verifier. Όμως η επιλογή αυτής της μορφής για το D δε θα ήταν αρκετή προκειμένου να εκτελούσε με επιτυχία το πρωτόκολλο ισότητας διακριτών λογαρίθμων διαφορετικών modulo, καθώς παράλληλα θα έπρεπε να υπολογίσει και ένα D' της μορφής

$$D' = \left(f^{x_5} \cdot f''^{s}\right) \bmod P \quad (150)$$

για κάποιο $s \in \mathbb{Z}^*$. Επίσης θα έπρεπε να υπολογίσει κάποια $x_6, x_7 \in \mathbb{Z}^*$ τέτοια ώστε να ικανοποιούσαν μαζί με το D την εξίσωση

$$1 = \left(D^{x_6} \cdot g^{m_2} \cdot g'^{x_7}\right) \bmod n \quad (151),$$

προκειμένου να εκτελούσε με επιτυχία το πρωτόκολλο ισότητας διακριτών λογαρίθμων ώστε να μην υφίσταται το προηγούμενο ενδεχόμενο διακοπής. Τέλος, θα

έπρεπε να υπολογίσει και κάποια $y_3, y_4, y_5, y_6 \in \mathbb{Z}^*$ τέτοια ώστε να ικανοποιούσαν μαζί με το D' τις εξισώσεις

$$\begin{cases} f = \left(G_1^{y_3} \cdot f'^{y_4}\right) \bmod P \\ f = \left(G_2^{y_5} \cdot f'^{y_6}\right) \bmod P \end{cases} \quad (152),$$

όπου

$$\begin{cases} G_1 = \left(D' \cdot f^{-1}\right) \bmod P \\ G_2 = \left(D' \cdot f\right) \bmod P \end{cases} \quad (134),$$

προκειμένου να εκτελούσε με επιτυχία το δεύτερο και τρίτο από τα πέντε συνολικά πρωτόκολλα αντίστοιχα, ώστε να μην υφίσταται το προηγούμενο ενδεχόμενο διακοπής. Από όλες τις παραμέτρους αυτές που δε θα ήξερε εκτός των D, D' θα ήταν οι

$$x_5, x_6, x_7, y_3, y_4, y_5, y_6, r, s,$$

καθώς τις υπόλοιπες

$$g, g', G, x_3, x_4, m_2, f, f^{-1}, f', \prod_{i=1}^{l} e_i$$

θα τις γνώριζε. Άρα θα προσπαθούσε να υπολογίσει κατάλληλα

$$x_5, x_6, x_7, y_3, y_4, y_5, y_6, r, s \in \mathbb{Z}^*.$$

Για τον υπολογισμό των x_5, x_6, x_7, r θα ακολουθούσε τις παρακάτω συνεπαγωγές προκειμένου να συμπεράνει τις συνθήκες που θα έπρεπε να τηρούν, ξεκινώντας από την (149) και λαμβάνοντας υπόψη πως η τάξη του g ως προς n είναι ίση με $p' \cdot q'$.

$$D^{x_6} \equiv \left(g^{x_5} \cdot g'^{r}\right)^{x_6} \bmod n = \left(\left(g^{x_5}\right)^{x_6} \cdot \left(g'^{r}\right)^{x_6}\right) \bmod n \Rightarrow D^{x_6} \equiv \left(g^{x_5 \cdot x_6} \cdot g'^{r \cdot x_6}\right) \bmod n \Rightarrow$$

$$\left(D^{x_6} \cdot g^{m_2} \cdot g'^{x_7}\right) \equiv \left(g^{x_5 \cdot x_6} \cdot g'^{r \cdot x_6} \cdot g^{m_2} \cdot g'^{x_7}\right) \bmod n \xrightarrow{(151)}$$

$$1 = \left(g^{x_5 \cdot x_6 + m_2} \cdot g'^{r \cdot x_6 + x_7}\right) \bmod n \Rightarrow g'^{-(r \cdot x_6 + x_7)} \equiv g^{x_5 \cdot x_6 + m_2} \bmod n \xrightarrow{(64)}$$

$$\left(g^{l_{g'}}\right)^{-(r \cdot x_6 + x_7)} \equiv g^{x_5 \cdot x_6 + m_2} \bmod n \Rightarrow g^{-l_{g'} \cdot (r \cdot x_6 + x_7)} \equiv g^{x_5 \cdot x_6 + m_2} \bmod n \Rightarrow$$

$$\left(x_5 \cdot x_6 + m_2 + l_{g'} \cdot \left(r \cdot x_6 + x_7\right)\right) \equiv 0 \bmod \left(p' \cdot q'\right).$$

Η τελευταία ισοδυναμία αποτελεί μία συνθήκη που θα έπρεπε να τηρούν τα x_5, x_6, x_7, r: το

$$x_5 \cdot x_6 + m_2 + l_{g'} \cdot \left(r \cdot x_6 + x_7\right)$$

θα πρέπει να είναι πολλαπλάσιο του $p' \cdot q'$. Το τελευταίο με τη σειρά του είναι διάφορο του 0 αφού τα p', q' είναι πρώτοι αριθμοί. Επειδή ο Prover δε τα γνωρίζει, τότε δε θα μπορούσε να βρει ένα μη μηδενικό πολλαπλάσιο του $p' \cdot q'$ ώστε αρχικά να το δοκιμάσει εάν θα μπορούσε να αποτελέσει τιμή του

$$x_5 \cdot x_6 + m_2 + l_{g'} \cdot \left(r \cdot x_6 + x_7\right)$$

και αν ναι μετά να δημιουργήσει μια εξίσωση για τα x_5, x_6, x_7, r. Έτσι η μόνη επιλογή του θα ήταν το μηδενικό πολλαπλάσιο, οπότε θα μετασχημάτιζε την παραπάνω ισοδυναμία στην εξίσωση

$$x_5 \cdot x_6 + m_2 + l_{g'} \cdot \left(r \cdot x_6 + x_7\right) = 0 \quad (153).$$

Επίσης η (149) συνεπάγεται ότι

$$D^{x_3} \equiv \left(g^{x_5} \cdot g'^{r}\right)^{x_3} \bmod n = \left(\left(g^{x_5}\right)^{x_3} \cdot \left(g'^{r}\right)^{x_3}\right) \bmod n \Rightarrow D^{x_3} \equiv \left(g^{x_5 \cdot x_3} \cdot g'^{r \cdot x_3}\right) \bmod n \Rightarrow$$

$$\left(D^{x_3} \cdot g'^{x_4}\right) \equiv \left(g^{x_5 \cdot x_3} \cdot g'^{r \cdot x_3} \cdot g'^{x_4}\right) \bmod n \xrightarrow{(145)} G \equiv \left(g^{x_5 \cdot x_3} \cdot g'^{r \cdot x_3 + x_4}\right) \bmod n \xrightarrow{(135)}$$

$$g^{\prod_{i=1}^{l} e_i} \equiv \left(g^{x_5 \cdot x_3} \cdot g'^{r \cdot x_3 + x_4}\right) \bmod n \Rightarrow \left(g^{\prod_{i=1}^{l} e_i} \cdot g^{-x_5 \cdot x_3}\right) \equiv g'^{r \cdot x_3 + x_4} \bmod n \Rightarrow$$

$$g^{\prod_{i=1}^{l} e_i - x_5 \cdot x_3} \equiv g'^{r \cdot x_3 + x_4} \bmod n \xrightarrow{(64)} g^{\prod_{i=1}^{l} e_i - x_5 \cdot x_3} \equiv \left(g^{l_{g'}}\right)^{r \cdot x_3 + x_4} \bmod n \Rightarrow$$

$$g^{\prod_{i=1}^{l} e_i - x_5 \cdot x_3} \equiv g^{l_{g'} \cdot (r \cdot x_3 + x_4)} \bmod n \Rightarrow \left(\prod_{i=1}^{l} e_i - x_5 \cdot x_3 - l_{g'} \cdot \left(r \cdot x_3 + x_4\right)\right) \equiv 0 \bmod \left(p' \cdot q'\right).$$

Η τελευταία ισοδυναμία αποτελεί μία συνθήκη που θα έπρεπε να τηρούν όμως μόνο τα x_5, r σε αντίθεση με την προηγούμενη: το

$$\prod_{i=1}^{l} e_i - x_5 \cdot x_3 - l_{g'} \cdot \left(r \cdot x_3 + x_4\right)$$

θα πρέπει να είναι πολλαπλάσιο του $p' \cdot q'$. Επειδή ο Prover δε θα μπορούσε να βρει ένα μη μηδενικό πολλαπλάσιό του $p' \cdot q'$ ώστε αρχικά να το δοκιμάσει εάν θα μπορούσε να αποτελέσει τιμή του

$$\prod_{i=1}^{l} e_i - x_5 \cdot x_3 - l_{g'} \cdot \left(r \cdot x_3 + x_4\right)$$

και αν ναι μετά να δημιουργήσει μια εξίσωση για τα x_5, r, θα επέλεγε το μηδενικό πολλαπλάσιο, οπότε θα μετασχημάτιζε την παραπάνω ισοδυναμία στην εξίσωση

$$\prod_{i=1}^{l} e_i - x_5 \cdot x_3 - l_{g'} \cdot \left(r \cdot x_3 + x_4\right) = 0$$

η οποία λόγω του ότι $l_{g'} \neq 0$ και $x_3 \neq 0$, αφού $x_3 \in \mathbb{Z}^*$, θα ισοδυναμεί με

$$x_5 \cdot x_3 = \prod_{i=1}^{l} e_i - l_{g'} \cdot \left(r \cdot x_3 + x_4\right) \Leftrightarrow x_5 = \frac{1}{x_3} \cdot \left(\prod_{i=1}^{l} e_i - l_{g'} \cdot \left(r \cdot x_3 + x_4\right)\right) \Leftrightarrow$$

$$x_5 = \frac{\prod_{i=1}^{l} e_i}{x_3} - l_{g'} \cdot \frac{\left(r \cdot x_3 + x_4\right)}{x_3} \quad (154).$$

Ο Prover θα επέλεγε τυχαία κάποιο $r \in \mathbb{Z}^*$ και θα προσπαθούσε να επιλύσει ως προς x_5 την (154). Έστω ότι το r θα ήταν τέτοιο ώστε να ίσχυε

$$r \cdot x_3 + x_4 \neq 0,$$

τότε

$$\frac{r \cdot x_3 + x_4}{x_3} \neq 0 \quad (155).$$

Στην (154) η μόνη παράμετρος που θα του ήταν άγνωστη εκτός του x_5 θα ήταν το $l_{g'}$ το οποίο πάρα πολύ δύσκολα θα μπορούσε να υπολογίσει. Από τη στιγμή που θα ίσχυε η (155), τότε το γινόμενο

$$l_{g'} \cdot \frac{\left(r \cdot x_3 + x_4\right)}{x_3}$$

θα του ήταν επίσης άγνωστο με αποτέλεσμα να αδυνατούσε να επιλύσει την (154) ως προς x_5.

Από την άλλη, στην περίπτωση που είχε αρχικά επιλέξει τα x_3, x_4 με τέτοιο τρόπο ώστε το x_3 να διαιρούσε το x_4, τότε αν επέλεγε το r να ήταν ίσο με $-\frac{x_4}{x_3}$ θα ισχύει ισοδύναμα

$$r = -\frac{x_4}{x_3} \Leftrightarrow r \cdot x_3 = -x_4 \Leftrightarrow r \cdot x_3 + x_4 = 0 .$$

Σε αυτήν την περίπτωση η (154) γίνεται

$$x_5 = \frac{\prod_{i=1}^{l} e_i}{x_3} - l_{g'} \cdot \frac{0}{x_3} = \frac{\prod_{i=1}^{l} e_i}{x_3} - 0 \Leftrightarrow x_5 = \frac{\prod_{i=1}^{l} e_i}{x_3} \quad (156).$$

Αν το x_3 που είχε επιλέξει αρχικά δε διαιρούσε το $\prod_{i=1}^{l} e_i$, τότε θα αδυνατούσε να υπολογίσει από την (156) το x_5, εφόσον αυτό θα ήταν ακέραιος, διαφορετικά θα το υπολόγιζε κανονικά. Επομένως από τα παραπάνω συμπεραίνεται πως για να μπορούσε ο Prover να βρει κάποια x_5, r που να ικανοποιούσαν την (154), θα έπρεπε να είχε αρχικά επιλέξει τα x_3, x_4 με τέτοιο τρόπο, ώστε το x_3 να ήταν διαιρέτης των $x_4, \prod_{i=1}^{l} e_i$. Από την τελευταία εξίσωση προκύπτει πως

$$\prod_{i=1}^{l} e_i = x_5 \cdot x_3$$

και συνεπώς το x_5 θα ήταν διαιρέτης του $\prod_{i=1}^{l} e_i$.

Τα στοιχεία του δεδομένου συνόλου τιμών είναι τιμές που μπορεί να λάβει μόνο το συγκεκριμένο πεδίο του πιστοποιητικού και κανένα άλλο. Αυτό σημαίνει πως καθένας από τους πρώτους αριθμούς $e_1,..,e_l$ στους οποίους αντιστοιχίζονται οι τιμές αυτού του συνόλου, αντιστοιχεί σε μια τιμή που μπορεί να λάβει μόνο το συγκεκριμένο πεδίο και κανένα άλλο. Έτσι ο πρώτος αριθμός στον οποίο αντιστοιχίζεται η τιμή κάθε πεδίου διαφορετικού από το συγκεκριμένο δεν ανήκει στο σύνολο $\{e_1,..,e_l\}$. Το γινόμενο των πρώτων αριθμών που αντιστοιχούν στις τιμές όλων των πεδίων του πιστοποιητικού εκτός από το συγκεκριμένο είναι ίσο με

$$d = \frac{m_2}{v},$$

μια και ο πρώτος αριθμός που αντιστοιχεί στην τιμή του συγκεκριμένου πεδίου είναι το v. Εφόσον στο d δεν περιέχεται κανένα από τα $e_1,..,e_l$ ως πρώτος παράγοντάς του, τότε κανένα από αυτά δε θα το διαιρεί. Άρα σύμφωνα με την Πρόταση 1 το d θα είναι πρώτο με καθένα από αυτά και συνεπώς λόγω της Πρότασης 5.1 το d θα είναι πρώτο και με το γινόμενό τους $\prod_{i=1}^{l} e_i$. Επίσης αφού λόγω της αρχικής υπόθεσης η τιμή του συγκεκριμένου πεδίου δεν ανήκει στο δεδομένο σύνολο τιμών, τότε

$$v \notin \{e_1,..,e_l\}$$

και άρα το v δε θα περιέχεται ως πρώτος παράγοντας στο $\prod_{i=1}^{l} e_i$ και συνεπώς δε θα το διαιρεί. Έτσι από τη στιγμή που ο πρώτος v δεν είναι διαιρέτης του $\prod_{i=1}^{l} e_i$, σύμφωνα με την Πρόταση 1 τα $v, \prod_{i=1}^{l} e_i$ θα είναι πρώτοι μεταξύ τους. Επειδή όπως αποδείχτηκε προηγούμενα τα $d, \prod_{i=1}^{l} e_i$ είναι επίσης πρώτοι μεταξύ τους, τότε σύμφωνα με την Πρόταση 5.1 το $\prod_{i=1}^{l} e_i$ θα είναι πρώτο με το γινόμενο

$$d \cdot v = m_2 .$$

Δηλαδή οι μοναδικοί κοινοί διαιρέτες των $\prod_{i=1}^{l} e_i, m_2$ στο σύνολο $\mathbb{Z}^*$ θα είναι τα $-1,1$.

2.1. $x_3 \neq \pm \prod_{i=1}^{l} e_i$ **και** x_3 **διαιρέτης των** $x_4, \prod_{i=1}^{l} e_i$

Σε αυτήν την υποπερίπτωση ο Prover είχε αρχικά επιλέξει τα x_3, x_4 με τέτοιο τρόπο ώστε το x_3 να ήταν διαιρέτης των $x_4, \prod_{i=1}^{l} e_i$ και διαφορετικό από τα $-\prod_{i=1}^{l} e_i, \prod_{i=1}^{l} e_i$. Εφόσον το x_3 θα διαιρούσε τα $x_4, \prod_{i=1}^{l} e_i$, τότε όπως αναφέρθηκε προηγούμενα ο ίδιος θα μπορούσε να βρει κάποια x_5, r που θα ικανοποιούσαν την (154). Συγκεκριμένα, αφού το x_3 θα ήταν διαφορετικό από τα $-\prod_{i=1}^{l} e_i, \prod_{i=1}^{l} e_i$, το x_5 που θα υπολόγιζε από την (156) θα ήταν διαφορετικό από τα $-1,1$.

Θα δειχτεί ότι το x_5 δε θα ήταν διαιρέτης του m_2. Τίθεται ο ισχυρισμός πως θα ήταν. Εφόσον όπως προαναφέρθηκε το x_5 θα ήταν διαιρέτης του $\prod_{i=1}^{l} e_i$, τότε θα ήταν κοινός διαιρέτης των $\prod_{i=1}^{l} e_i, m_2$. Όπως προαναφέρθηκε οι μοναδικοί κοινοί διαιρέτες των $\prod_{i=1}^{l} e_i, m_2$ στο $\mathbb{Z}^*$ είναι τα $-1,1$ και επομένως οι δυνατές τιμές για το x_5 θα ήταν τα $-1,1$. Το τελευταίο συμπέρασμα καταλήγει σε άτοπο, αφού όπως αναφέρθηκε στην παρούσα υποπερίπτωση ισχύει $x_5 \neq \pm 1$. Έτσι ο προηγούμενος ισχυρισμός δεν αληθεύει και το x_5 δε θα ήταν διαιρέτης του m_2.

Λόγω του ότι $l_{g'} \neq 0$ η (153) ισοδυναμεί με

$$x_5 \cdot x_6 + m_2 = -l_{g'} \cdot (r \cdot x_6 + x_7) \Leftrightarrow r \cdot x_6 + x_7 = (x_5 \cdot x_6 + m_2) \cdot \frac{1}{-l_{g'}} \Leftrightarrow$$

$$x_7 = -(x_5 \cdot x_6 + m_2) \cdot \frac{1}{l_{g'}} - r \cdot x_6 \quad (157).$$

Στην (157) οι άγνωστες παράμετροι για τον Prover θα ήταν τα x_6, x_7 που θα ήθελε να βρει και το $l_{g'}$ το οποίο πάρα πολύ δύσκολα θα μπορούσε να υπολογίσει. Θα επέλεγε τυχαία κάποιο $x_6 \in \mathbb{Z}^*$ και θα προσπαθούσε να επιλύσει ως προς x_7 την (157). Επειδή το x_5 δε θα ήταν διαιρέτης του m_2, τότε για οποιαδήποτε τυχαία επιλογή του $x_6 \in \mathbb{Z}^*$ που θα έκανε ο Prover θα ίσχυε ότι

$$x_5 \cdot x_6 \neq -m_2$$

και άρα ισοδύναμα

$$-m_2 - x_5 \cdot x_6 \neq 0 \Leftrightarrow -\left(x_5 \cdot x_6 + m_2\right) \neq 0 .$$

Από τη στιγμή που πάρα πολύ δύσκολα θα μπορούσε να υπολογίσει και να μάθει το $l_{g'}$, τότε λόγω της τελευταίας σχέσης το γινόμενο

$$-\left(x_5 \cdot x_6 + m_2\right) \cdot \frac{1}{l_{g'}}$$

θα του ήταν επίσης άγνωστο με αποτέλεσμα να αδυνατούσε να επιλύσει την (157) ως προς x_7.

2.2. $x_3 = \pm\prod_{i=1}^{l} e_i$ **και** x_4 **ακέραιο πολλαπλάσιο του** $\prod_{i=1}^{l} e_i$

Σε αυτήν την υποπερίπτωση ο Prover είχε αρχικά επιλέξει τα x_3, x_4 με τέτοιο τρόπο έτσι ώστε το x_3 να ήταν ίσο με $-\prod_{i=1}^{l} e_i$ ή $\prod_{i=1}^{l} e_i$ και το x_4 ακέραιο πολλαπλάσιο του $\prod_{i=1}^{l} e_i$. Τότε το x_3 θα ήταν διαιρέτης των $x_4, \prod_{i=1}^{l} e_i$ και επομένως ο Prover θα μπορούσε να βρει κάποια x_5, r που θα ικανοποιούσαν την (154).

Συγκεκριμένα, για $x_3 = -\prod_{i=1}^{l} e_i$ θα ήταν λόγω της (156) $x_5 = -1$. Συνεπώς θα ισχύει

$$r = -\frac{x_4}{x_3} = -\frac{x_4}{-\prod_{i=1}^{l} e_i} \Leftrightarrow r = \frac{x_4}{\prod_{i=1}^{l} e_i}$$

και

$$x_5 \cdot x_6 + m_2 = (-1) \cdot x_6 + m_2 \Leftrightarrow x_5 \cdot x_6 + m_2 = m_2 - x_6 .$$

Αν ο Prover επέλεγε το x_6 έτσι ώστε $x_6 \neq m_2$, τότε προκύπτει από την τελευταία εξίσωση ότι

$$x_5 \cdot x_6 + m_2 = m_2 - x_6 \neq 0 .$$

Εφόσον πάρα πολύ δύσκολα θα μπορούσε να υπολογίσει και να μάθει το $l_{g'}$, τότε το γινόμενο

$$-\left(x_5 \cdot x_6 + m_2\right) \cdot \frac{1}{l_{g'}} = -\left(m_2 - x_6\right) \cdot \frac{1}{l_{g'}}$$

θα του ήταν επίσης άγνωστο με αποτέλεσμα να αδυνατούσε να επιλύσει την (157) ως προς x_7.

Αν επέλεγε το x_6 να ήταν ίσο με m_2, τότε ισχύει

$$x_5 \cdot x_6 + m_2 = m_2 - x_6 = 0$$

και έτσι η (157) γίνεται

$$x_7 = -0 \cdot \frac{1}{l_{g'}} - r \cdot x_6 = 0 - \frac{x_4}{\prod_{i=1}^{l} e_i} \cdot m_2 \Leftrightarrow x_7 = -\frac{x_4}{\prod_{i=1}^{l} e_i} \cdot m_2 .$$

Επομένως μία λύση που θα μπορούσε να βρει ο Prover για τα x_5, x_6, x_7, r θα ήταν η

$$(x_5, x_6, x_7, r) = \left(-1, m_2, -\frac{x_4}{\prod_{i=1}^{l} e_i} \cdot m_2, \frac{x_4}{\prod_{i=1}^{l} e_i} \right) \text{ (158).}$$

Για $x_3 = \prod_{i=1}^{l} e_i$ θα ήταν λόγω της (156) $x_5 = 1$. Επομένως θα ισχύει

$$r = -\frac{x_4}{x_3} \Leftrightarrow r = -\frac{x_4}{\prod_{i=1}^{l} e_i}$$

και

$$x_5 \cdot x_6 + m_2 = 1 \cdot x_6 + m_2 \Leftrightarrow x_5 \cdot x_6 + m_2 = m_2 + x_6 .$$

Αν ο Prover επέλεγε το x_6 έτσι ώστε $x_6 \neq -m_2$, τότε προκύπτει από την τελευταία εξίσωση ότι

$$x_5 \cdot x_6 + m_2 = m_2 + x_6 \neq 0 .$$

Εφόσον πάρα πολύ δύσκολα θα μπορούσε να υπολογίσει και να μάθει το $l_{g'}$, τότε το γινόμενο

$$-(x_5 \cdot x_6 + m_2) \cdot \frac{1}{l_{g'}} = -(m_2 + x_6) \cdot \frac{1}{l_{g'}}$$

θα του ήταν επίσης άγνωστο με αποτέλεσμα να αδυνατούσε να επιλύσει την (157) ως προς x_7.

Αν επέλεγε το x_6 να ήταν ίσο με $-m_2$, τότε ισχύει

$$x_5 \cdot x_6 + m_2 = m_2 + x_6 = 0$$

και έτσι η (157) γίνεται

$$x_7 = -0 \cdot \frac{1}{l_{g'}} - r \cdot x_6 = 0 - \left(-\frac{x_4}{\prod_{i=1}^{l} e_i} \right) \cdot (-m_2) \Leftrightarrow x_7 = -\frac{x_4}{\prod_{i=1}^{l} e_i} \cdot m_2 .$$

Επομένως μία δεύτερη λύση που θα μπορούσε να βρει ο Prover για τα x_5, x_6, x_7, r θα ήταν η

$$(x_5, x_6, x_7, r) = \left(1, -m_2, -\frac{x_4}{\prod_{i=1}^{l} e_i} \cdot m_2, -\frac{x_4}{\prod_{i=1}^{l} e_i} \right) \text{ (159).}$$

2.2.1. $x_3 = -\prod_{i=1}^{l} e_i$ **και** x_4 **ακέραιο πολλαπλάσιο του** $\prod_{i=1}^{l} e_i$

Σε αυτήν την υποπερίπτωση ο Prover είχε αρχικά επιλέξει τα x_3, x_4 με τέτοιο τρόπο ώστε το x_3 να ήταν ίσο με $-\prod_{i=1}^{l} e_i$ και το x_4 ακέραιο πολλαπλάσιο του $\prod_{i=1}^{l} e_i$. Τότε η αντίστοιχη λύση που θα έβρισκε για τα x_5, x_6, x_7, r θα ήταν η (158). Ο ίδιος θα έπρεπε μετά να υπολογίσει από τα x_5, r αυτής της λύσης το D σύμφωνα με την (149) και ύστερα να δοκιμάσει αν αυτό ικανοποιεί αφενός την (145) και αφετέρου μαζί με τα x_6, x_7 της ίδιας λύσης την (151). Η (149) γίνεται

$$D = \left(g^{x_5} \cdot g'^{r}\right) \bmod n \Rightarrow D = \left(g^{-1} \cdot g'^{\frac{x_4}{\prod_{i=1}^{l} e_i}} \right) \bmod n \quad (160).$$

Από την (160) συνεπάγεται ότι

$$D^{m_2} \equiv \left(g^{-1} \cdot g'^{\frac{x_4}{\prod_{i=1}^{l} e_i}} \right)^{m_2} \bmod n = \left(\left(g^{-1}\right)^{m_2} \cdot \left(g'^{\frac{x_4}{\prod_{i=1}^{l} e_i}} \right)^{m_2} \right) \bmod n \Rightarrow$$

$$D^{m_2} \equiv \left(g^{-m_2} \cdot g'^{\frac{x_4}{\prod_{i=1}^{l} e_i} \cdot m_2} \right) \bmod n \Rightarrow \left(D^{m_2} \cdot g^{m_2} \cdot g'^{-\frac{x_4}{\prod_{i=1}^{l} e_i} \cdot m_2} \right) \equiv 1 \bmod n \xrightarrow{(158)}$$

$$1 = \left(D^{x_6} \cdot g^{m_2} \cdot g'^{x_7}\right) \bmod n.$$

Από την τελευταία εξίσωση συμπεραίνεται πως το D που υπολογίζεται από τα x_5, r της λύσης (158) ικανοποιεί μαζί με τα x_6, x_7 της ίδιας λύσης την (151). Από την (160) συνεπάγεται ότι

$$D^{-\prod_{i=1}^{l} e_i} \equiv \left(g^{-1} \cdot g'^{\frac{x_4}{\prod_{i=1}^{l} e_i}} \right)^{-\prod_{i=1}^{l} e_i} \bmod n = \left(\left(g^{-1}\right)^{-\prod_{i=1}^{l} e_i} \cdot \left(g'^{\frac{x_4}{\prod_{i=1}^{l} e_i}} \right)^{-\prod_{i=1}^{l} e_i} \right) \bmod n \Rightarrow$$

$$D^{-\prod_{i=1}^{l} e_i} \equiv \left(g^{(-1)\cdot\left(-\prod_{i=1}^{l} e_i\right)} \cdot g'^{\frac{x_4}{\prod_{i=1}^{l} e_i}\cdot\left(-\prod_{i=1}^{l} e_i\right)} \right) \bmod n \Rightarrow D^{x_3} \equiv \left(g^{\prod_{i=1}^{l} e_i} \cdot g'^{-x_4} \right) \bmod n \Rightarrow$$

$$\left(D^{x_3} \cdot g'^{x_4}\right) \equiv g^{\prod_{i=1}^{l} e_i} \bmod n \xrightarrow{(135)} G = \left(D^{x_3} \cdot g'^{x_4}\right) \bmod n.$$

Από την τελευταία εξίσωση συμπεραίνεται πως το D που υπολογίζεται από τα x_5, r της λύσης (158) ικανοποιεί την (145).
Η (150) γίνεται

$$D' = \left(f^{x_5} \cdot f'^{s} \right) \bmod P \Rightarrow D' = \left(f^{-1} \cdot f'^{s} \right) \bmod P \quad (161).$$

Για τον υπολογισμό κάποιων $y_5, y_6, s \in \mathbb{Z}^*$ που θα έπρεπε να ικανοποιούν τη δεύτερη εξίσωση του συστήματος

$$\begin{cases} f = \left(G_1^{y_3} \cdot f'^{y_4} \right) \bmod P \\ f = \left(G_2^{y_5} \cdot f'^{y_6} \right) \bmod P \end{cases} \quad (152),$$

όπου

$$\begin{cases} G_1 = \left(D' \cdot f^{-1} \right) \bmod P \\ G_2 = \left(D' \cdot f \right) \bmod P \end{cases} \quad (134),$$

ο Prover θα ακολουθούσε τις παρακάτω συνεπαγωγές προκειμένου να συμπεράνει τη συνθήκη που θα έπρεπε να τηρούν, ξεκινώντας από την (161).

$$D' = \left(f^{-1} \cdot f'^{s} \right) \bmod P \Rightarrow \left(D' \cdot f \right) \equiv f'^{s} \bmod P \xrightarrow{(134)} G_2 \equiv f'^{s} \bmod P \Rightarrow$$

$$G_2^{y_5} \equiv \left(f'^{s} \right)^{y_5} \bmod P \Rightarrow G_2^{y_5} \equiv f'^{s \cdot y_5} \bmod P \Rightarrow$$

$$\left(G_2^{y_5} \cdot f'^{y_6} \right) \equiv \left(f'^{s \cdot y_5} \cdot f'^{y_6} \right) \bmod P \xrightarrow{(152)} f \equiv f'^{s \cdot y_5 + y_6} \bmod P \quad (162).$$

Σύμφωνα με την (65) που αναφέρεται στην υποενότητα 4.1, ισχύει

$$f' = f^{l_{f'}} \bmod P,$$

όπου το $l_{f'} \in \{2, .., P'-1\}$ κρατείται μυστικό από την Αρχή. Έτσι ο Prover δεν το ξέρει και πάρα πολύ δύσκολα θα μπορούσε να το υπολογίσει από την τελευταία εξίσωση λόγω του Πρώτου Ισχυρισμού Διακριτού Λογαρίθμου. Επίσης όπως αναφέρεται στην ίδια υποενότητα, η τάξη του f ως προς P είναι ίση με P'. Από την (65) συνεπάγεται πως

$$f'^{s \cdot y_5 + y_6} \equiv \left(f^{l_{f'}} \right)^{s \cdot y_5 + y_6} \bmod P \xrightarrow{(162)} f \equiv f^{l_{f'} \cdot (s \cdot y_5 + y_6)} \bmod P.$$

Σύμφωνα με την Πρόταση 15.2 και αφού η τάξη του f ως προς P είναι ίση με P', προκύπτει από την τελευταία ισοδυναμία πως

$$\left(l_{f'} \cdot \left(s \cdot y_5 + y_6 \right) - 1 \right) \equiv 0 \bmod P'.$$

Δηλαδή $\exists d_1 \in \mathbb{Z}$ ώστε

$$l_{f'} \cdot \left(s \cdot y_5 + y_6 \right) - 1 = P' \cdot d_1.$$

Από την τελευταία εξίσωση προκύπτει πως η συνθήκη που πρέπει να ικανοποιούν τα y_5, y_6, s είναι ότι το

$$l_{f'} \cdot \left(s \cdot y_5 + y_6 \right) - 1$$

θα πρέπει να είναι πολλαπλάσιο του P', το οποίο με τη σειρά του να σημειωθεί ότι είναι διάφορο του 0 αφού είναι πρώτος αριθμός. Επειδή ο Prover γνωρίζει το P', αφού όπως αναφέρθηκε στην υποενότητα 4.1 αυτό έχει δημοσιοποιηθεί από την εκδότρια Αρχή κατά τη φάση δημιουργίας παραμέτρων, τότε θα μπορούσε να υπολογίσει ένα οποιοδήποτε πολλαπλάσιό του και όχι μόνο το μηδενικό, ώστε αρχικά να το δοκιμάσει εάν θα μπορούσε να αποτελέσει τιμή του

$$l_{f'} \cdot \left(s \cdot y_5 + y_6 \right) - 1$$

και αν ναι μετά να δοκιμάσει αν τα y_5, y_6, s που θα είχε υπολογίσει ικανοποιούσαν τη δεύτερη εξίσωση της (152). Εφόσον $l_{f'} \in \{2, .., P'-1\}$, θα είναι $l_{f'} \neq 0$ και άρα για

οποιαδήποτε επιλογή του $d_1 \in \mathbb{Z}$ που θα έκανε ο Prover, η παραπάνω εξίσωση ισοδυναμεί με

$$l_{f'} \cdot (s \cdot y_5 + y_6) = P' \cdot d_1 + 1 \Leftrightarrow s \cdot y_5 + y_6 = \frac{1}{l_{f'}} \cdot (P' \cdot d_1 + 1) \Leftrightarrow$$

$$y_6 = \frac{1}{l_{f'}} \cdot (P' \cdot d_1 + 1) - s \cdot y_5 \text{ (163).}$$

Επειδή το P' είναι περιττός πρώτος αριθμός, θα είναι $P' \geq 3 > 0$. Τότε $\forall x \in \mathbb{Z}_+$ θα ισχύει

$$x \geq 0 \Rightarrow P' \cdot x \geq 0 \Rightarrow P' \cdot x + 1 \geq 1 > 0 \Rightarrow P' \cdot x + 1 \neq 0.$$

Επίσης $\forall x \in \mathbb{Z}_-^*$ θα ισχύει

$$\begin{cases} x \leq -1 \\ P' \geq 3 \end{cases} \Rightarrow \begin{cases} P' \cdot x \leq P' \cdot (-1) \\ -P' \leq -3 \end{cases} \Rightarrow P' \cdot x \leq -P' \leq -3 \Rightarrow P' \cdot x \leq -3 \Rightarrow$$

$$P' \cdot x + 1 \leq -2 < 0 \Rightarrow P' \cdot x + 1 \neq 0.$$

Επομένως $\forall x \in \mathbb{Z}$ ισχύει

$$P' \cdot x + 1 \neq 0$$

και έτσι για οποιαδήποτε επιλογή του $d_1 \in \mathbb{Z}$ που θα έκανε ο Prover θα ίσχυε

$$P' \cdot d_1 + 1 \neq 0.$$

Στην (163) οι άγνωστες παράμετροι για τον Prover θα ήταν τα y_5, y_6, s που θα ήθελε να βρει και το $l_{f'}$ το οποίο πάρα πολύ δύσκολα θα μπορούσε να υπολογίσει. Θα επέλεγε τυχαία κάποια $y_5, s \in \mathbb{Z}^*$ και θα προσπαθούσε να επιλύσει ως προς y_6 την (163). Επειδή αφενός για οποιαδήποτε επιλογή του $d_1 \in \mathbb{Z}$ που θα έκανε θα ίσχυε

$$P' \cdot d_1 + 1 \neq 0$$

και αφετέρου πάρα πολύ δύσκολα θα μπορούσε να υπολογίσει και να μάθει το $l_{f'}$, τότε το γινόμενο

$$\frac{1}{l_{f'}} \cdot (P' \cdot d_1 + 1)$$

θα του ήταν άγνωστο με αποτέλεσμα να αδυνατούσε να επιλύσει την (163) ως προς y_6.

Επομένως στην υποπερίπτωση που ο Prover επέλεγε το x_3 να ήταν ίσο με $-\prod_{i=1}^{l} e_i$ και το x_4 ακέραιο πολλαπλάσιο του $\prod_{i=1}^{l} e_i$, δε θα μπορούσε να υπολογίσει κάποια y_5, y_6, s που να τηρούσαν την παραπάνω συνθήκη ώστε μετά να δοκιμάσει αν αυτά ικανοποιούσαν τη δεύτερη εξίσωση της (152).

2.2.2. $x_3 = \prod_{i=1}^{l} e_i$ και x_4 ακέραιο πολλαπλάσιο του $\prod_{i=1}^{l} e_i$

Σε αυτήν την υποπερίπτωση ο Prover είχε αρχικά επιλέξει τα x_3, x_4 με τέτοιο τρόπο ώστε το x_3 να ήταν ίσο με $\prod_{i=1}^{l} e_i$ και το x_4 ακέραιο πολλαπλάσιο του $\prod_{i=1}^{l} e_i$. Τότε η αντίστοιχη λύση που θα έβρισκε για τα x_5, x_6, x_7, r θα ήταν η (159). Ο ίδιος θα

έπρεπε μετά να υπολογίσει από τα x_5, r αυτής της λύσης το D σύμφωνα με την (149) και ύστερα να δοκιμάσει αν αυτό ικανοποιεί αφενός την (145) και αφετέρου μαζί με τα x_6, x_7 της ίδιας λύσης την (151). Η (149) γίνεται

$$D = \left(g^{x_5} \cdot g'^{r}\right) \bmod n = \left(g^1 \cdot g'^{-\frac{x_4}{\prod_{i=1}^{l} e_i}}\right) \bmod n \Rightarrow D = \left(g \cdot g'^{-\frac{x_4}{\prod_{i=1}^{l} e_i}}\right) \bmod n \quad (164).$$

Από την (164) συνεπάγεται ότι

$$D^{-m_2} \equiv \left(g \cdot g'^{-\frac{x_4}{\prod_{i=1}^{l} e_i}}\right)^{-m_2} \bmod n = \left(g^{-m_2} \cdot \left(g'^{-\frac{x_4}{\prod_{i=1}^{l} e_i}}\right)^{-m_2}\right) \bmod n \Rightarrow$$

$$D^{-m_2} \equiv \left(g^{-m_2} \cdot g'^{\left(-\frac{x_4}{\prod_{i=1}^{l} e_i}\right)\cdot(-m_2)}\right) \bmod n \Rightarrow D^{-m_2} \equiv \left(g^{-m_2} \cdot g'^{\frac{x_4}{\prod_{i=1}^{l} e_i}\cdot m_2}\right) \bmod n \Rightarrow$$

$$\left(D^{-m_2} \cdot g^{m_2} \cdot g'^{-\frac{x_4}{\prod_{i=1}^{l} e_i}\cdot m_2}\right) \equiv 1 \bmod n \xrightarrow{(159)} 1 = \left(D^{x_6} \cdot g^{m_2} \cdot g'^{x_7}\right) \bmod n .$$

Από την τελευταία εξίσωση συμπεραίνεται πως το D που υπολογίζεται από τα x_5, r της λύσης (159) ικανοποιεί μαζί με τα x_6, x_7 της ίδιας λύσης την (151). Από την (164) συνεπάγεται ότι

$$D^{\prod_{i=1}^{l} e_i} \equiv \left(g \cdot g'^{-\frac{x_4}{\prod_{i=1}^{l} e_i}}\right)^{\prod_{i=1}^{l} e_i} \bmod n = \left(g^{\prod_{i=1}^{l} e_i} \cdot \left(g'^{-\frac{x_4}{\prod_{i=1}^{l} e_i}}\right)^{\prod_{i=1}^{l} e_i}\right) \bmod n \Rightarrow$$

$$D^{\prod_{i=1}^{l} e_i} \equiv \left(g^{\prod_{i=1}^{l} e_i} \cdot g'^{\left(-\frac{x_4}{\prod_{i=1}^{l} e_i}\right)\cdot\prod_{i=1}^{l} e_i}\right) \bmod n \Rightarrow D^{x_3} \equiv \left(g^{\prod_{i=1}^{l} e_i} \cdot g'^{-x_4}\right) \bmod n \Rightarrow$$

$$\left(D^{x_3} \cdot g'^{x_4}\right) \equiv g^{\prod_{i=1}^{l} e_i} \bmod n \xrightarrow{(135)} G = \left(D^{x_3} \cdot g'^{x_4}\right) \bmod n .$$

Από την τελευταία εξίσωση συμπεραίνεται πως το D που υπολογίζεται από τα x_5, r της λύσης (159) ικανοποιεί την (145).
Η (150) γίνεται

$$D' = \left(f^{x_5} \cdot f'^{s} \right) \bmod P = \left(f^{1} \cdot f'^{s} \right) \bmod P \Rightarrow D' = \left(f \cdot f'^{s} \right) \bmod P \quad (165).$$

Για τον υπολογισμό κάποιων $y_3, y_4, s \in \mathbb{Z}^*$ που θα έπρεπε να ικανοποιούν την πρώτη εξίσωση του συστήματος

$$\begin{cases} f = \left(G_1^{y_3} \cdot f'^{y_4} \right) \bmod P \\ f = \left(G_2^{y_5} \cdot f'^{y_6} \right) \bmod P \end{cases} \quad (152),$$

όπου

$$\begin{cases} G_1 = \left(D' \cdot f^{-1} \right) \bmod P \\ G_2 = \left(D' \cdot f \right) \bmod P \end{cases} \quad (134),$$

ο Prover θα ακολουθούσε τις παρακάτω συνεπαγωγές προκειμένου να συμπεράνει τη συνθήκη που θα έπρεπε να τηρούν, ξεκινώντας από την (165).

$$D' = \left(f \cdot f'^{s} \right) \bmod P \Rightarrow \left(D' \cdot f^{-1} \right) \equiv f'^{s} \bmod P \xrightarrow{(134)} G_1 \equiv f'^{s} \bmod P \Rightarrow$$

$$G_1^{y_3} \equiv \left(f'^{s} \right)^{y_3} \bmod P \Rightarrow G_1^{y_3} \equiv f'^{s \cdot y_3} \bmod P \Rightarrow$$

$$\left(G_1^{y_3} \cdot f'^{y_4} \right) \equiv \left(f'^{s \cdot y_3} \cdot f'^{y_4} \right) \bmod P \xrightarrow{(152)} f \equiv f'^{s \cdot y_3 + y_4} \bmod P \quad (166).$$

Ισχύει

$$f' = f^{l_{f'}} \bmod P \quad (65),$$

όπου το $l_{f'}$ είναι άγνωστο στον Prover και ο ίδιος πάρα πολύ δύσκολα θα μπορούσε να το υπολογίσει από την τελευταία εξίσωση λόγω του Πρώτου Ισχυρισμού Διακριτού Λογαρίθμου. Από την (65) συνεπάγεται πως

$$f'^{s \cdot y_3 + y_4} \equiv \left(f^{l_{f'}} \right)^{s \cdot y_3 + y_4} \bmod P \xrightarrow{(166)} f \equiv f^{l_{f'} \cdot (s \cdot y_3 + y_4)} \bmod P .$$

Σύμφωνα με την Πρόταση 15.2 και αφού η τάξη του f ως προς P είναι ίση με P', προκύπτει από την τελευταία ισοδυναμία πως

$$\left(l_{f'} \cdot \left(s \cdot y_3 + y_4 \right) - 1 \right) \equiv 0 \bmod P' .$$

Δηλαδή $\exists d_2 \in \mathbb{Z}$ ώστε

$$l_{f'} \cdot \left(s \cdot y_3 + y_4 \right) - 1 = P' \cdot d_2 .$$

Από την τελευταία εξίσωση προκύπτει πως η συνθήκη που πρέπει να ικανοποιούν τα y_3, y_4, s είναι ότι το

$$l_{f'} \cdot \left(s \cdot y_3 + y_4 \right) - 1$$

θα πρέπει να είναι πολλαπλάσιο του P', το οποίο με τη σειρά του να σημειωθεί ότι είναι διάφορο του 0 αφού είναι πρώτος αριθμός. Επειδή ο Prover γνωρίζει το P', αφού αυτό έχει δημοσιοποιηθεί από την εκδότρια Αρχή κατά τη φάση δημιουργίας παραμέτρων, τότε θα μπορούσε να υπολογίσει ένα οποιοδήποτε πολλαπλάσιό του και όχι μόνο το μηδενικό, ώστε αρχικά να το δοκιμάσει εάν θα μπορούσε να αποτελέσει τιμή του

$$l_{f'} \cdot \left(s \cdot y_3 + y_4 \right) - 1$$

και αν ναι μετά να δοκιμάσει αν τα y_3, y_4, s που θα είχε υπολογίσει ικανοποιούσαν την πρώτη εξίσωση της (152). Εφόσον είναι $l_{f'} \neq 0$, τότε για οποιαδήποτε επιλογή του $d_2 \in \mathbb{Z}$ που θα έκανε ο Prover, η παραπάνω εξίσωση ισοδυναμεί με

$$l_{f'} \cdot \left(s \cdot y_3 + y_4 \right) = P' \cdot d_2 + 1 \Leftrightarrow s \cdot y_3 + y_4 = \frac{1}{l_{f'}} \cdot \left(P' \cdot d_2 + 1 \right) \Leftrightarrow$$

$$y_4 = \frac{1}{l_{f'}} \cdot \left(P' \cdot d_2 + 1\right) - s \cdot y_3 \text{ (167).}$$

Όπως αποδείχτηκε στην υποπερίπτωση 2.2.1, $\forall x \in \mathbb{Z}$ ισχύει

$$P' \cdot x + 1 \neq 0 .$$

Έτσι για οποιαδήποτε επιλογή του $d_2 \in \mathbb{Z}$ που θα έκανε ο Prover θα ίσχυε

$$P' \cdot d_2 + 1 \neq 0 .$$

Στην (167) οι άγνωστες παράμετροι για τον Prover θα ήταν τα y_3, y_4, s που θα ήθελε να βρει και το $l_{f'}$ το οποίο πάρα πολύ δύσκολα θα μπορούσε να υπολογίσει. Θα επέλεγε τυχαία κάποια $y_3, s \in \mathbb{Z}^*$ και θα προσπαθούσε να επιλύσει ως προς y_4 την (167). Επειδή αφενός για οποιαδήποτε επιλογή του $d_2 \in \mathbb{Z}$ που θα έκανε θα ίσχυε

$$P' \cdot d_2 + 1 \neq 0$$

και αφετέρου πάρα πολύ δύσκολα θα μπορούσε να υπολογίσει και να μάθει το $l_{f'}$, τότε το γινόμενο

$$\frac{1}{l_{f'}} \cdot \left(P' \cdot d_2 + 1\right)$$

θα του ήταν άγνωστο με αποτέλεσμα να αδυνατούσε να επιλύσει την (167) ως προς y_4.

Επομένως στην υποπερίπτωση που ο Prover επέλεγε το x_3 να ήταν ίσο με $\prod_{i=1}^{l} e_i$ και το x_4 ακέραιο πολλαπλάσιο του $\prod_{i=1}^{l} e_i$, δε θα μπορούσε να υπολογίσει κάποια y_3, y_4, s που να τηρούσαν την παραπάνω συνθήκη ώστε μετά να δοκιμάσει αν αυτά ικανοποιούσαν την πρώτη εξίσωση της (152).

Από τα παραπάνω συμπεραίνεται πως ο Prover μόνο για δύο επιλογές του $\left(x_3, x_4\right) \in \left(\mathbb{Z}^*\right)^2$ θα μπορούσε να υπολογίσει κάποια $x_5, x_6, x_7, r \in \mathbb{Z}^*$ που να τηρούσαν τις δύο αντίστοιχες συνθήκες που τέθηκαν. Συγκεκριμένα το x_4 θα πρέπει να είναι και στις δύο επιλογές ακέραιο πολλαπλάσιο του $\prod_{i=1}^{l} e_i$, ενώ το x_3 ίσο με $-\prod_{i=1}^{l} e_i$ στην μία επιλογή και ίσο με $\prod_{i=1}^{l} e_i$ στην άλλη. Σε κάθεμια από τις δύο επιλογές του $\left(x_3, x_4\right)$, το D που θα υπολόγιζε ο Prover από τα αντίστοιχα x_5, r βάσει της (149), θα ικανοποιούσε αφενός την (145) και αφετέρου μαζί με τα αντίστοιχα x_6, x_7 την (151), εξασφαλίζοντας έτσι την επιτυχή για αυτόν εκτέλεση των δύο τελευταίων από τα πέντε συνολικά πρωτόκολλα. Στην μία επιλογή όπου $x_3 = -\prod_{i=1}^{l} e_i$ είναι $x_5 = -1$, ενώ στην άλλη όπου $x_3 = \prod_{i=1}^{l} e_i$ είναι $x_5 = 1$. Για κάθεμια από αυτές τις δύο τιμές του x_5 ο Prover θα μπορούσε επιλέγοντας τυχαία κάποιο $s \in \mathbb{Z}^*$ να υπολογίσει βάσει της (150) ένα D', εξασφαλίζοντας έτσι την επιτυχή για αυτόν εκτέλεση του πρώτου από τα πέντε συνολικά πρωτόκολλα. Όμως για $x_5 = -1$ δε θα μπορούσε να υπολογίσει

βάσει της (150) κάποιο D' όπως επίσης και κάποια $y_5, y_6 \in \mathbb{Z}^*$ ώστε αυτά τα τρία να ικανοποιούσαν τη δεύτερη εξίσωση της (152), με αποτέλεσμα να μην ήταν δυνατή η επιτυχής για αυτόν εκτέλεση του τρίτου από τα πέντε συνολικά πρωτόκολλα. Παρόμοια, για $x_5 = 1$ δε θα μπορούσε να υπολογίσει βάσει της (150) κάποιο D' όπως επίσης και κάποια $y_3, y_4 \in \mathbb{Z}^*$ ώστε αυτά τα τρία να ικανοποιούσαν την πρώτη εξίσωση της (152), με αποτέλεσμα να μην ήταν δυνατή η επιτυχής για αυτόν εκτέλεση του δεύτερου από τα πέντε συνολικά πρωτόκολλα. Έτσι από τη στιγμή που για κάθεμια από τις δύο τιμές του x_5 ο Prover δε θα μπορούσε να εκτελέσει επιτυχώς για αυτόν και τα δύο πρωτόκολλα γνώσης διακριτών λογαρίθμων modulo πρώτο αριθμό, το παρών πρωτόκολλο που εξετάζεται σε αυτήν την υποενότητα θα διακοπτόταν από τον Verifier είτε μετά το τέλος του δεύτερου είτε μετά το τέλος του τρίτου πρωτοκόλλου. Αυτό σημαίνει πως ο Prover δε θα μπορούσε να εκτελέσει με τον Verifier το τέταρτο και πέμπτο πρωτόκολλο, εκ των οποίων το τελευταίο είναι αυτό της γνώσης διακριτών λογαρίθμων του G ως προς τις βάσεις D, g'.

Επομένως σύμφωνα με όσα αναφέρθηκαν στην περίπτωση 2 συμπεραίνεται πως αν η τιμή του συγκεκριμένου πεδίου του πιστοποιητικού δεν ανήκει στο δεδομένο σύνολο τιμών και ο Prover επιλέξει να μην τηρήσει το πρωτόκολλο που εξετάζεται στην παρούσα υποενότητα, τότε δε θα καταφέρει να εκτελέσει επιτυχώς το πρωτόκολλο γνώσης διακριτών λογαρίθμων του G ως προς τις βάσεις D, g'.

Συνεπώς από την παρούσα απόδειξη προκύπτει πως μόνο όταν η τιμή του συγκεκριμένου πεδίου ανήκει στο δεδομένο σύνολο τιμών και το πρωτόκολλο τηρηθεί, ο Prover μπορεί να πείσει σίγουρα τον Verifier ότι γνωρίζει διακριτούς λογαρίθμους του του G ως προς τις βάσεις D, g'. Διαφορετικά η πιθανότητα να πειστεί ο Verifier είναι εξαιρετικά μικρή. Αυτό σημαίνει πως η απόδειξη γνώσης τέτοιων λογαρίθμων από τον Prover αποτελεί σχεδόν κατά 100% και απόδειξη ότι η τιμή του συγκεκριμένου πεδίου ανήκει στο δεδομένο σύνολο τιμών.

4. <u>Εμπιστευτικότητα πληροφορίας</u>

Η τιμή αυτού του πεδίου αποτελεί πληροφορία που δεν μπορεί να γίνει γνωστή στον Verifier. Από την μία δεν μαθαίνει άμεσα από τον Prover αυτήν την τιμή και από την άλλη δεν μπορεί να λάβει γνώση της έμμεσα από τον πρώτο αριθμό v στον οποίο αντιστοιχίζεται. Αν ήξερε αυτόν τον αριθμό θα μπορούσε να χρησιμοποιήσει τη δημοσιοποιημένη λίστα των κωδικών των τιμών των πεδίων της Αρχής προκειμένου μέσω αυτού να βρει την τιμή του συγκεκριμένου πεδίου. Όμως αφενός δεν τον μαθαίνει άμεσα από τον Prover και αφετέρου δεν μπορεί να τον πληροφορηθεί έμμεσα υπολογίζοντάς τον.

Από την μία, στην περίπτωση που ο ισχυρισμός του Prover είναι αληθής και το παρών πρωτόκολλο τηρηθεί, τότε όπως αναφέρθηκε στην παρούσα απόδειξη θα $\exists d' \in \mathbb{N}^*$ ώστε να ισχύει

$$\prod_{i=1}^{l} e_i = v \cdot d'$$

και το πρωτόκολλο γνώσης διακριτών λογαρίθμων του G ως προς τις βάσεις D, g' θα εκτελεστεί επιτυχώς. Αν ο Verifier επιχειρούσε να λύσει την προηγούμενη εξίσωση ως προς v, θα ήταν απαραίτητη η γνώση του d' την οποία δε θα είχε. Ο λόγος θα ήταν ότι κατά την επιτυχή εκτέλεση του προηγούμενου πρωτοκόλλου γνώσης διακριτών λογαρίθμων δεν είναι δυνατό να πληροφορηθεί τον λογάριθμο d' που ξέρει ο Prover ως προς τη βάση D.

Από την άλλη, στην περίπτωση που ο Verifier εκτελέσει με τον Prover επιτυχώς το πρωτόκολλο ισότητας διακριτών λογαρίθμων διαφορετικών modulo των D, D' ως προς τις βάσεις g, f με αναπαραστάσεις στις βάσεις g, g' σε $\bmod n$ και f, f' σε $\bmod P$ αντίστοιχα, δεν μπορεί να πληροφορηθεί τον κοινό λογάριθμο που ξέρει ο Prover ο οποίος είναι ο v.

Επίσης, αν προσπαθούσε να λύσει ως προς v μία εκ των δύο εξισώσεων του συστήματος

$$\begin{cases} P' \cdot x_1 + (v-1) \cdot y_1 = 1 \\ P' \cdot x_2 + (v+1) \cdot y_2 = 1 \end{cases} \quad (133),$$

με δεδομένο πως θα ήξερε το δημόσια γνωστό P' θα ήταν απαραίτητη η γνώση των x_1, y_1 ή των x_2, y_2 αν επιχειρούσε να επιλύσει την πρώτη ή τη δεύτερη εξίσωση αντίστοιχα. Όμως κανένα από αυτά τα δύο ζεύγη αριθμών δε θα μπορούσε να γνωρίζει. Από την μία, κατά τη διάρκεια και μετά το τέλος του παρόντος πρωτοκόλλου δεν πληροφορείται τα x_1, x_2. Από την άλλη, αν εκτελεστεί επιτυχώς το πρωτόκολλο γνώσης διακριτών λογαρίθμων modulo πρώτο αριθμό του f ως προς τις βάσεις G_1, f', τότε δεν είναι δυνατό να πληροφορηθεί τον λογάριθμο y_1 που ξέρει ο Prover ως προς τη βάση G_1. Επίσης, αν εκτελεστεί επιτυχώς το πρωτόκολλο γνώσης διακριτών λογαρίθμων modulo πρώτο αριθμό του του f ως προς τις βάσεις G_2, f', τότε δεν είναι δυνατό να πληροφορηθεί τον λογάριθμο y_2 που ξέρει ο Prover ως προς τη βάση G_2.

4.1. Ο ρόλος των παραμέτρων g', f' και των μεταβλητών r, s

Στην περίπτωση που το παρών πρωτόκολλο τηρηθεί ο Prover θα υπολογίσει κανονικά σύμφωνα με αυτό τις παραμέτρους D, D' από τις σχέσεις

$$D = \left(g^v \cdot g''^r\right) \bmod n \ (131), \ D' = \left(f^v \cdot f'^s\right) \bmod P \ (132).$$

Σε αυτήν την περίπτωση το D' θα συμμετέχει στο πρώτο πρωτόκολλο και το D σε τρία από τα πέντε συνολικά πρωτόκολλα και έτσι ο Verifier θα έχει πρόσβαση στις δύο αυτές παραμέτρους. Επομένως θα μπορούσε να προσπαθήσει να υπολογίσει το v από μία εκ των δύο παραπάνω σχέσεων.

Το v ανήκει σε ένα πεπερασμένο σύνολο πρώτων αριθμών. Το πλήθος αυτού του συνόλου είναι το πλήθος όλων των δυνατών τιμών που μπορεί να έχει το συγκεκριμένο πεδίο του πιστοποιητικού και άρα είναι μικρό. Αν δεν υπήρχαν η παράμετρος g' και η μεταβλητή r στην (131) και ίσχυε

$$D = g^v \bmod n,$$

τότε πολύ εύκολα ο Verifier θα μπορούσε να ανακαλύψει την τιμή του v. Αν v'' είναι μία μεταβλητή που παίρνει τιμές από το προηγούμενο μικρό σύνολο των πρώτων αριθμών, τότε θα έθετε κάθε έναν από όλους αυτούς τους πρώτους αριθμούς στην μεταβλητή v'' και θα δοκίμαζε αν ικανοποιούνταν η εξίσωση

$$D = g^{v''} \bmod n \ (168).$$

Αυτή η διαδικασία θα σταματούσε όταν θα έβρισκε εκείνον τον αριθμό που θα ικανοποιούσε την (168) και ο οποίος θα ήταν ο v. Εφόσον το πλήθος όλων αυτών των πρώτων αριθμών είναι μικρό, η αναζήτηση θα διαρκούσε λίγο. Η (168) με την προσθήκη της παραμέτρου g' ως βάση και της δεύτερης μεταβλητής r ως εκθέτης της μετασχηματίζεται στην εξίσωση

$$D = \left(g^{v''} \cdot g'^{r}\right) \bmod n \quad (169).$$

Με αυτόν τον τρόπο οι δυνατές τιμές του v'' για τις οποίες ισχύει η (169) μπορεί να είναι περισσότερες της μίας, καθώς είναι δυνατό να υπάρχουν ζεύγη (v'', r) με διαφορετικά v'' που να την ικανοποιούν. Αν οι τιμές που μπορούσε να λάβει το r ήταν σχετικά λίγες όπως και του v'', τότε η εύρεση ζευγών (v'', r) που θα ικανοποιούσαν την (169) θα ήταν και πάλι εύκολη, μόνο που αν ο Verifier έβρισκε περισσότερα του ενός τέτοια ζεύγη με το καθένα να έχει διαφορετική τιμή για το v'', δε θα ήξερε ποιο από αυτά τα ζεύγη είναι αυτό που επέλεξε ο Prover για τον υπολογισμό του D. Έτσι δε θα μπορούσε να αποφανθεί σχετικά με το ποιο είναι το v και άρα ποια είναι η τιμή του συγκεκριμένου πεδίου. Από τη στιγμή όμως που το r λαμβάνει τυχαία τιμές από όλο το $\mathbb{Z}^*$, η εύρεση του v δυσκολεύει εξαιρετικά πολύ. Αφενός η αναζήτηση ζευγών (v'', r) που ικανοποιούν την (169) γίνεται πάρα πολύ δύσκολη σύμφωνα με το Δεύτερο Ισχυρισμό Διακριτού Λογαρίθμου, αφετέρου είναι πολύ πιθανό να υπάρχουν περισσότερα τέτοια ζεύγη με διαφορετικές τιμές για το v''. Έτσι η προσθήκη στην (168) της παραμέτρου g' ως μια δεύτερη βάση και της δεύτερης μεταβλητής r η οποία λαμβάνει τιμές από όλο το $\mathbb{Z}^*$ ως εκθέτης της, δυσχεραίνουν εξαιρετικά πολύ την εύρεση του v. Επομένως σχεδόν σίγουρα θα αδυνατούσε ο Verifier να υπολογίσει το v από την (131).

Παρόμοια ανάλυση με αυτήν που παρουσιάστηκε σχετικά με τον ρόλο της παραμέτρου g' και της μεταβλητής r μπορεί να γίνει και για την παράμετρο f' και την μεταβλητή s. Οι δύο τελευταίες λαμβάνουν μέρος στον υπολογισμό της παραμέτρου D' σύμφωνα με την (132). Η μεταβλητή s όπως και η r λαμβάνει τυχαία τιμές από όλο το $\mathbb{Z}^*$. Το τελικό συμπέρασμα αυτής της ανάλυσης θα ήταν πως σχεδόν σίγουρα θα αδυνατούσε ο Verifier να υπολογίσει το v από την (132).

Μία άλλη δυνατότητα που θα είχε ο Verifier για να υπολογίσει το v θα ήταν να ακολουθούσε τη διαδικασία που αναφέρθηκε στην παράγραφο 4 της απόδειξης της υποενότητας 5.5. Όμως και με αυτόν τον τρόπο θα αδυνατούσε να το υπολογίσει, καθώς η συγκεκριμένη διαδικασία βασίζεται στη γνώση του m_2 την οποία δε θα μπορούσε να έχει.

Από την μία, όταν προηγουμένως στα πλαίσια της εκτέλεσης του πρωτοκόλλου εγκυρότητας πιστοποιητικού εκτέλεσε με τον Prover το πρωτόκολλο γνώσης διακριτών λογαρίθμων του Z ως προς τα A', R_1, R_2, S, δεν ήταν δυνατό να πληροφορηθεί τους διακριτούς λογαρίθμους που ξέρει ο Prover ως προς τις τέσσερις αυτές βάσεις, άρα και τον m_2 ως προς το R_2.

Από την άλλη, στην περίπτωση που εκτελέσει με τον Prover επιτυχώς το πρωτόκολλο ισότητας διακριτών λογαρίθμων των $Z, 1$ ως προς τις βάσεις R_2, g με αναπαραστάσεις στις βάσεις A', R_1, R_2, S και D, g, g' αντίστοιχα, δεν μπορεί να πληροφορηθεί τον κοινό λογάριθμο που ξέρει ο Prover και ο οποίος είναι ο m_2.

Αναφορές

[1] Patrik Bichsel, Carl Binding, Jan Camenisch, Thomas Groß, Tom Heydt-Benjamin, Dieter Sommer, Greg Zaverucha, 'Research Report Cryptographic Protocols of the Identity Mixer Library', ενότητα 2

[2] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, 'Handbook of

Applied Cryptography', σελίδες 65, 68, 69, 70

[3] Bruce Schneier, 'Applied cryptography', σελίδες 251, 261

[4] Σταύρος Γ. Παπασταυρίδης, 'Εισαγωγή στην Σύγχρονη Άλγεβρα και τις Εφαρμογές της, Τόμος Β, Θεωρία Πολυωνύμων, Θεωρία Ομάδων', σελίδα 271

[5] Stefan Brands, 'An Efficient Off-line Electronic Cash System Based On The Representation Problem', σελίδες 13, 15, 21

[6] Jan Camenisch, Thomas Groß, 'Efficient Attributes for Anonymous Credentials', υποενότητες 3.4, 4.3, 4.4, σελίδες 24, 26

[7] Jan Camenisch, Anna Lysyanskaya, 'A Signature Scheme with Efficient Protocols', υποενότητα 2.2

[8] Θεόφιλος Κανακάρης, Ιωάννης Σταματίου, 'Αποδεικτικά Πρωτόκολλα Μηδενικής Γνώσης στην Ηλεκτρονική Ψηφοφορία', Εργασία, ενότητα 6, υποενότητες 6.1, 6.3

[9] Jan Camenisch, Markus Michels, 'Separability and Efficiency for Generic Group Signature Schemes', υποενότητες 3.3, 3.4