2020

Διπλωματική Εργασία

ΑΝΑΛΥΣΗ ΤΕΧΝΟΛΟΓΙΩΝ PUF ΚΑΙ ΤΟΥ ΤΡΟΠΟΥ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ ΓΙΑ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ

ΔΕΥΤΕΡΑΙΟΣ ΠΑΥΛΟΣ – ΕΥΣΤΑΘΙΟΣ ΜΤΕ1711

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΞΕΝΑΚΗΣ ΧΡΗΣΤΟΣ

Περιεχόμενα

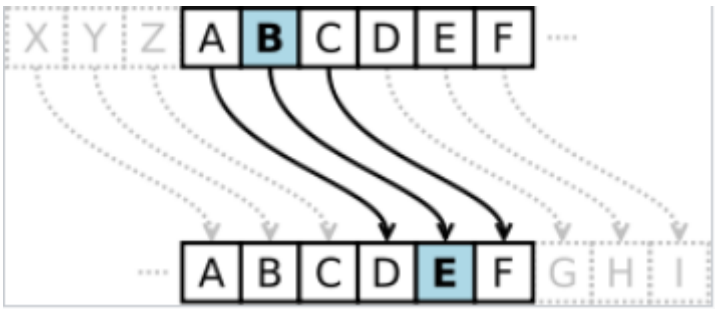
ΕΙΣΑΓΩΓΗ

Στις μέρες μας η ταχεία ανάπτυξη των ΤΠΕ έχει φανερώσει την ανάγκη για ανάπτυξη τεχνολογιών, ώστε να υπάρχει ασφάλεια στη διάδοση και στη μετάδοση των πληροφοριών. Τα κυριότερα θέματα που πρέπει να αντιμετωπιστούν είναι η ταυτοποίηση ενός χρήστη μέσω διαδικτύου και η ασφαλής μεταφορά μιας πληροφορίας μέσω ενός καναλιού που μπορεί να μην είναι ασφαλές.

Το θέμα της ταυτοποίησης στο διαδίκτυο αναφέρεται πλέον ως *αυθεντικοποίηση*. Ο πιο απλός τρόπος για την αυθεντικοποίηση ενός χρήστη είναι με την χρήση ενός ονόματος χρήστη και ενός συνθηματικού που το γνωρίζει μόνο ο ίδιος. Σε αυτήν την περίπτωση θα πρέπει να δίνεται ιδιαίτερη προσοχή στην πολυπλοκότητα του συνθηματικού, το οποίο θα πρέπει να αλλάζει τακτικά από τον χρήστη.

Για την αυθεντικοποίηση στις μέρες μας χρησιμοποιούνται κι άλλοι τρόποι, όπως έξυπνες κάρτες και βιομετρικά στοιχεία. Άλλες λύσεις για επιπλέον ασφάλεια είναι η αυθεντικοποίηση με *two factor off authentication*. Στην παρούσα εργασία θα πραγματευτούμε την αυθεντικοποίηση με την χρήση των *physical unclonable functions (PUFs).*

Η ασφαλής μεταφορά μιας πληροφορίας σε ένα κανάλι που δεν είναι ασφαλές προϋποθέτει τη συμφωνία ενός τρόπου επικοινωνίας που δεν είναι γνωστός σε έναν τρίτο που «ακούει» το κανάλι. Από τα πολύ παλιά χρόνια έχουμε τον κώδικα του Καίσαρα, στον οποίο κάθε γράμμα του κειμένου αντικαθίσταται από κάποιο άλλο γράμμα με σταθερή απόσταση κάθε φορά στο αλφάβητο. Στην παρακάτω εικόνα βλέπουμε τον κώδικα του Καίσαρα με μετατόπιση 3.



Εικόνα 1. Κώδικας Καίσαρα με μετατόπιση 3 [55]

Αυτός βέβαια είναι ένας απλοϊκός τρόπος κωδικοποίησης ο οποίος μπορεί να «σπάσει» ιδιαίτερα εύκολα γιατί το μόνο που χρειάζεται είναι να βρούμε μια λέξη του κειμένου.

Ιστορικά πρέπει να αναφερθεί και η χρήση της μηχανής Enigma από τους Γερμανούς, για ανταλλαγή μηνυμάτων κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου. Η λειτουργία της βασιζόταν στην κρυπτογράφηση συμμετρικού κλειδιού. Πιο συγκεκριμένα, στην αρχή της επικοινωνίας των χρηστών είναι απαραίτητο να ανταλλαχθεί ένα μυστικό κλειδί. Στη συνέχεια το κλειδί αυτό χρησιμοποιείται για την κρυπτογράφηση του μεταδιδόμενου μηνύματος. Ο «πατέρας» της Πληροφορικής Άλαν Τούρινγκ «έσπασε» τον κωδικό Enigma των Γερμανών και κατάφερε έτσι να δώσει ένα σημαντικό πλεονέκτημα στις Συμμαχικές δυνάμεις. [1]

Εικόνα 2. Συσκευή Enigma του Β' Παγκοσμίου Πολέμου [56]

Σήμερα χρησιμοποιείται σε μεγάλο βαθμό κρυπτογράφηση με χρήση συναρτήσεων κατακερματισμού (Hash Functions)[2]. Οι συναρτήσεις αυτές βασίζονται σε πολύπλοκα μαθηματικά προβλήματα και δίνουν μοναδική έξοδο (σύνοψη) για κάθε είσοδο. Μια ιδανική κρυπτογραφική συνάρτηση κατατεμαχισμού έχει τις παρακάτω ιδιότητες:

- Είναι εύκολο να υπολογιστεί η σύνοψη για οποιαδήποτε είσοδο.
- Δεν είναι εφικτό να βρεθεί η είσοδος από την σύνοψη.
- Δεν είναι εφικτό να τροποποιηθεί η είσοδος χωρίς να τροποποιηθεί η σύνοψη.

- Δεν είναι εφικτό να βρεθούν δύο διαφορετικές είσοδοι που δίνουν την ίδια σύνοψη.

Όσο αυξάνεται η υπολογιστική ισχύς των ηλεκτρονικών υπολογιστών τόσο πιο πιθανό είναι βρεθεί λύση στα λεγόμενα «άλυτα» προβλήματα. Επίσης οι hackers επενδύουν όλο και περισσότερο χρόνο και χρήμα για να βρουν κενά στα κρυπτογραφικά μοντέλα. Το αποτέλεσμα είναι κάποιες συναρτήσεις κατακερματισμού να είναι πια ακατάλληλες για χρήση σε κρυπτογραφικά μοντέλα και κάποιοι αλγόριθμοι κρυπτογράφησης που παλιά χρησιμοποιούνταν ευρέως, σήμερα να μην θεωρούνται ασφαλείς. Ένα χαρακτηριστικό παράδειγμα αποτελεί ο αλγόριθμος md5 ο οποίος πλέον δεν θεωρείται ασφαλής.

Στόχος της παρούσας εργασίας είναι να παρουσιαστεί η λειτουργία των διαφόρων τεχνολογιών PUF για την ανταλλαγή κρυπτογραφικών κλειδιών, να αναδειχθούν τα πλεονεκτήματα και τα μειονεκτήματα της κάθε τεχνολογίας, καθώς και να αναλυθούν τα μοντέλα επιθέσεων που είναι αποτελεσματικά ενάντια στα PUFs.

1. Τι είναι τα PUFs

Ένα PUF είναι στην ουσία το ανάλογο hardware μιας μονόδρομης μαθηματικής συνάρτησης, το οποίο δεν βασίζεται σε έναν συνηθισμένο μαθηματικό μετασχηματισμό κατακερματισμού, αλλά σε έναν περίπλοκο και μη αναπαραγώγιμο φυσικό μηχανισμό. Τα PUFs είναι κατασκευές οι οποίες χρησιμοποιούν την φυσική διαταραχή τυχαίων πρωτοφανών hardware νανοκλίμακας για την παραγωγή κλειδιών, χωρίς να χρειάζεται να κρατιέται κάπου η κρίσιμη πληροφορία. [3]

Η επιτυχία των επιθέσεων στις υλοποίησες των PUF εξαρτάται επιγραμματικά από τους παρακάτω τομείς:

- Την ικανότητα του επιτιθέμενου, την ταχύτητα, το κόστος και την ακρίβεια των εργαλείων και του εξοπλισμού
- Την γνώση σχετικά με την υλοποίηση του PUF
- Την διαρροή πληροφοριών από το PUF

Software Implementations

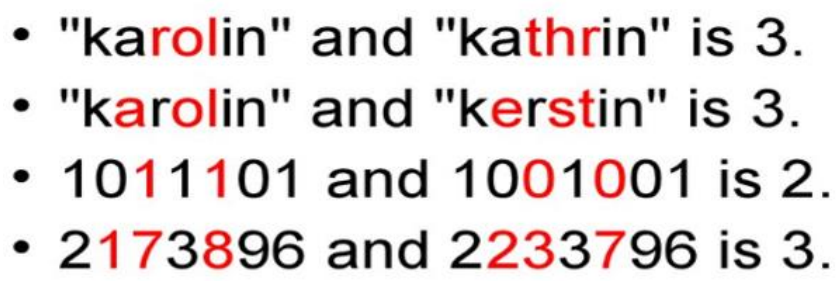
Ενώ οι λύσεις ασφάλειας που βασίζονται στο software είναι πιο εύκολες στην εγκατάσταση, συντήρηση και αναβάθμιση, έχουν ένα βασικό μειονέκτημα. Αυτό είναι η παραδοχή ότι υπάρχει επαρκής φυσική προστασία των μέσων που έχουν εγκατασταθεί, το οποίο δεν μπορεί να διασφαλιστεί πάντα με βεβαιότητα. Στις λύσεις software η ασφάλεια βασίζεται σε ένα δυσεπίλυτο μαθηματικό πρόβλημα με την υπόθεση ενός «ασφαλούς» κλειδιού. Η αποθήκευση αυτού του κλειδιού σε μια σταθερή μνήμη είναι η αχίλλειος πτέρνα πολλών συστημάτων και ιδιαίτερα πολλών έξυπνων συσκευών. Όπως πολύ εύστοχα έχει σχολιάσει ο Ron Rivest «η ονομασία μιας ακολουθίας bit μυστικό κλειδί, δεν το κάνει ασφαλές αλλά μάλλον δείχνει ότι είναι ένας ενδιαφέρον στόχος για έναν επιτιθέμενο».

2. Ταυτοποίηση

Κατά την ταυτοποίηση ένα γνωστό ID δίνεται σε μια άγνωστη οντότητα. Για κάθε οντότητα δίνεται ένα μοναδικό ID. Όταν αναφερόμαστε σε μικροηλεκτρονικές συσκευές και PUF το ID αυτό δίνεται σε ένα τσιπ [5]. Αυτό είναι πολύ σημαντικό για να αποφεύγονται λανθασμένες ταυτοποιήσεις [6].

Όταν τα PUF χρησιμοποιούνται στα συστήματα ταυτοποίησης αντικαθιστούν τη διαδικασία παραγωγής του ID εξωτερικά καθώς και την non-volatile memory (NVM) που θα χρησιμοποιούταν ώστε να αποθηκευτεί το ID. Αν η εγκατάσταση NVM μπορεί να αντικατασταθεί από την χρήση PUF το κόστος για κάθε συσκευή αυθεντικοποίησης μπορεί να μειωθεί σημαντικά. Επομένως, τα PUFs μπορούν να μειώσουν την πολυπλοκότητα παραγωγής και με το να παρέχουν το ID χρησιμοποιώντας τις εσωτερικές ιδιότητες του τσιπ. [7]

Οι έξοδοι όμως των συστημάτων PUF έχουν θόρυβο. Αυτό σημαίνει ότι ένα σύστημα ταυτοποίησης που στηρίζεται στα PUF θα πρέπει να έχει ανοχή στα λάθη. Το μέτρο για την μέτρηση αντοχής στα δυαδικά συστήματα ονομάζεται Hamming distance. Στην παρακάτω εικόνα βλέπουμε κάποια παραδείγματα Hamming distance. [8]



Εικόνα 3. Παραδείγματα Hamming distances [54]

Όταν χρησιμοποιούνται τα PUF για την ταυτοποίηση υπάρχει η φάση εγγραφής των ID σε μια βάση. Σε μια τυπική διαδικασία ταυτοποίησης το PUF διαβάζεται ξανά. Λόγω των λαθών που παράγουν τα PUF είναι απίθανο να υπάρξει πλήρης αντιστοίχηση της εξόδου και της καταχώρησης στη βάση. Υπάρχουν 2 τρόποι για τον χειρισμό της ανοχής του συστήματος.

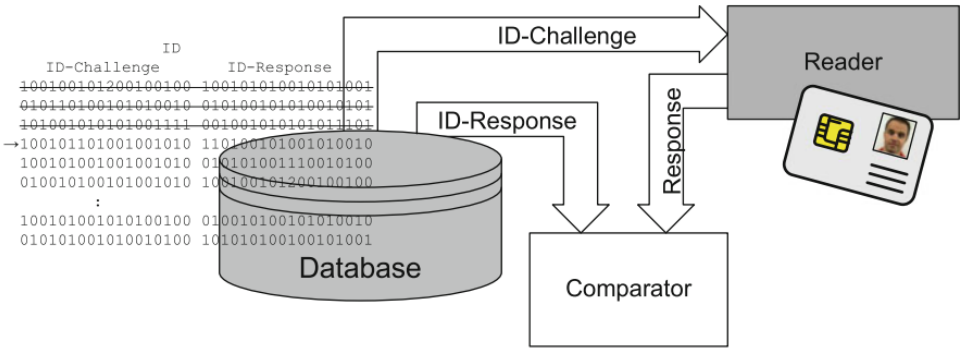
- Επιλέγεται το σύνολο δεδομένων που έχει την μικρότερη απόσταση από τα IDs που λήφθηκαν. Το μειονέκτημα αυτής της μεθόδου είναι ότι καταχωρούνται στη βάση ελαττωματικά τσιπς ή τσιπς που δεν χρειάζεται να γίνουν register στη βάση.
- Ορίζεται ένας αριθμός από λάθος bit που είναι αποδεκτά. IDs που είναι μέσα σε αυτόν το σύνολο λαθών θεωρούνται έγκυρα.

2.1 Αυθεντικοποίηση

Αυθεντικοποίηση είναι η διαδικασία κατά την οποία επιβεβαιώνεται σε ένα chip μια συγκεκριμένη οντότητα. Μια διακεκριμένη ιδέα που χρησιμοποιείται για αυθεντικοποίηση βασίζεται σε ζευγάρια πρόκλησης - απάντησης (challenge – response). Στην πληροφορική ένα πρωτόκολλο αυθεντικοποίησης που χρησιμοποιεί αυτήν την τεχνολογία ονομάζεται Challenge Handshake Authentication Protocol (CHAP) [9].

2.1.1 Αυθεντικοποίηση με ζευγάρια πρόκλησης – απάντησης και PUFs

Η ιδέα της αυθεντικοποίησης με ζευγάρια πρόκλησης – απάντησης είναι απλή. Όταν μια οντότητα θέλει να αυθεντικοποιηθεί για παράδειγμα σε έναν server της στέλνεται μια ερώτηση από τον server (πρόκληση). Ο server στο παράδειγμα μας έχει αποθηκευμένη την απάντηση σε μια βάση δεδομένων . Η οντότητα επιστρέφει την απάντηση. Ο server επιβεβαιώνει ότι η απάντηση ταιριάζει με αυτήν που έχει αποθηκευμένη και τότε η οντότητα αυθεντικοποείται. Στην παρακάτω φωτογραφία βλέπουμε πώς λειτουργεί η συγκεκριμένη διαδικασία. [10]

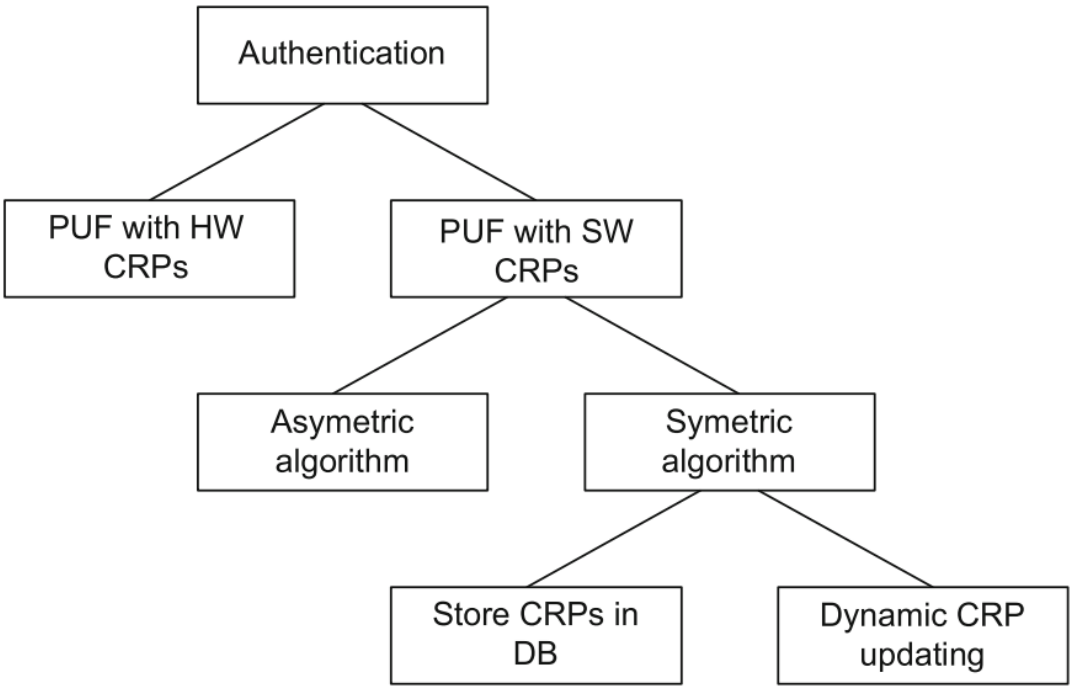


Εικόνα 4. Παράδειγμα αυθεντικοποίησης με Challenge – Response pairs [10]

Όταν γίνεται η χρήση PUF για την αυθεντικοποίηση λόγω των λαθών που παράγονται μπορεί η οντότητα να μην αυθεντικοποιηθεί ακόμα κι αν είναι η σωστή. Υπάρχουν 2 τρόποι που παράγονται οι απαντήσεις στο challenge – response στα PUF.

1. Τα PUF που στηρίζονται στο hardware. Σε αυτήν την περίπτωση τα PUF κελιά πρέπει να μπορούν να παράγουν διαφορετική έξοδο ανάλογα με την είσοδο. Πέρα από την διόρθωση των λαθών μπορούν να χρησιμοποιηθούν PUF που έχουν ανοχή σε λάθη.
2. Σε περίπτωση που οι απαντήσεις βασίζονται στο software τότε δεν υπάρχει ανοχή στα λάθη. Σε αυτήν την περίπτωση θα πρέπει να γίνει διόρθωση των σφαλμάτων.

Στο παρακάτω σχήμα βλέπουμε την ταξινόμηση της αυθεντικοποίησης με χρήση των PUFs.



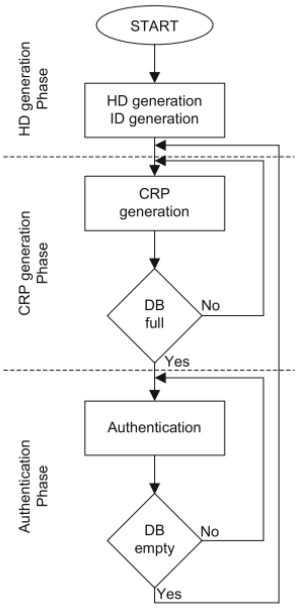
Εικόνα 5. Ταξινόμηση της αυθεντικοποίησης με χρήση PUFs [10]

2.2 Κύκλος ζωής της προσέγγισης CRP

Στο σχήμα 1 παρουσιάζεται ένας κύκλος ζωής της διαδικασίας πιστοποίησης με CRPs. Στην πρώτη φάση, η οποία ονομάζεται φάση εγγραφής, πρέπει να καταχωρηθεί το τσιπ σε μια βάση δεδομένων. Σε περιπτώσεις όπου δεν υπάρχει NVM στο τσιπ και η διόρθωση σφάλματος είναι απαραίτητη, τα βοηθητικά δεδομένα πρέπει να δημιουργηθούν στο τσιπ και να μεταδοθούν στη βάση δεδομένων. Επιπλέον, ένα αναγνωριστικό του τσιπ πρέπει να αποθηκευτεί στη βάση δεδομένων. Αυτό το αναγνωριστικό θα χρησιμοποιηθεί κατά τη διάρκεια της διαδικασίας επαλήθευσης ταυτότητας.

Στη συνέχεια, αρχίζει η φάση παραγωγής CRP. Κατά τη διάρκεια αυτής της φάσης, ένας ορισμένος αριθμός CRP δημιουργείται και αποθηκεύεται στη βάση δεδομένων. Ο αριθμός των αποθηκευμένων ζευγών εξαρτάται από τον εκτιμώμενο αριθμό διαδικασιών επαλήθευσης ταυτότητας του τσιπ.

Η τελευταία φάση είναι η φάση της αυθεντικοποίησης. Κατά τη διάρκεια αυτής της φάσης, το πιστοποιημένο αναγνωριστικό επαληθεύεται από το σύστημα. Μια νέα CRP είναι απαραίτητη για κάθε διαδικασία επαλήθευσης ταυτότητας. Αυτό είναι σημαντικό προκειμένου να καταστεί δυνατή η επαναχρησιμοποίηση των εγγεγραμμένων ζευγών πρόκλησης-απόκρισης.



Σχήμα 1. Διάρκεια ζωής αυθεντικοποίησης με την χρήση CRPs [10]

Θετικά και αρνητικά της αυθεντικοποίησης με χρήση CRPs:

+ Είναι πολύ δύσκολο να υπάρξει επίθεση στο σύστημα

- Όταν τελειώσουν τα ζευγάρια CRPs θα πρέπει να ξαναγίνει η φάση εγγραφής η οποία μπορεί να γίνει μόνο μέσα σε ένα έμπιστο και ασφαλές περιβάλλον

2.3 Γενικά θέματα ασφάλειας

Είναι σημαντικό για την ασφάλεια των μοντέλων αυθεντικοποίησης με ζεύγη πρόκλησης απάντησης (από εδώ και πέρα CRP) να έχουν αρκετά μεγάλο μέγεθος CRPs. Σήμερα το τυπικό μέγεθος του challenge είναι από 128 bits και πάνω. Αυτό βέβαια μπορεί να αλλάξει όσο αυξάνεται η επεξεργαστική ισχύς των υπολογιστών. Επίσης, το challenge πρέπει να είναι τυχαία νούμερα. Αν ένας επιτιθέμενος μπορεί να προβλέψει μελλοντικά challenges, τότε θα μπορεί με την χρήση των μελλοντικών challenges να κλωνοποιήσει μερικώς ένα τσιπ. [10]

2.4 Σκέψη για δυνατότητες αποφυγής της φάσης εγγραφής

Η συγκεκριμένη παράγραφος περιλαμβάνει μια προσωπική πρόταση – σκέψη για το πώς θα μπορούσε να αποφευχθεί η επανάληψη της διαδικασίας εγγραφής. Έστω ότι μια οντότητα ζητάει αυθεντικοποίηση. Στέλνεται το challenge από τον server κι η οντότητα δίνει το response. Το response που πρέπει να δοθεί είναι γνωστό και στους 2. Έστω ότι το μέγεθος του response που πρέπει να δοθεί είναι καταχωρημένο και είναι 256 bits. Η οντότητα παράγει την απάντηση και στέλνει τα 128 bits για την αυθεντικοποίηση. Τα 128 bits που απομένουν (από εδώ και στο εξής spare bits) τα περνάει από μια hush function και έπειτα τα χρησιμοποιεί για να δημιουργήσει ένα νέο challenge. Η απάντηση του νέου challenge κρυπτογραφείται και στέλνεται ξεχωριστά στον server. Για την αποκρυπτογράφηση απαιτούνται τα 128 bits τα οποία είναι ήδη αποθηκευμένα στον server. Στην συνέχεια τα bits αυτά περνάνε από μια hush function στο τσιπ και στο server ώστε να παραχθούν τα spare 128 bits.

2.5 Αυθεντικοποίηση με χρήση CRPs βασισμένα σε Hardware

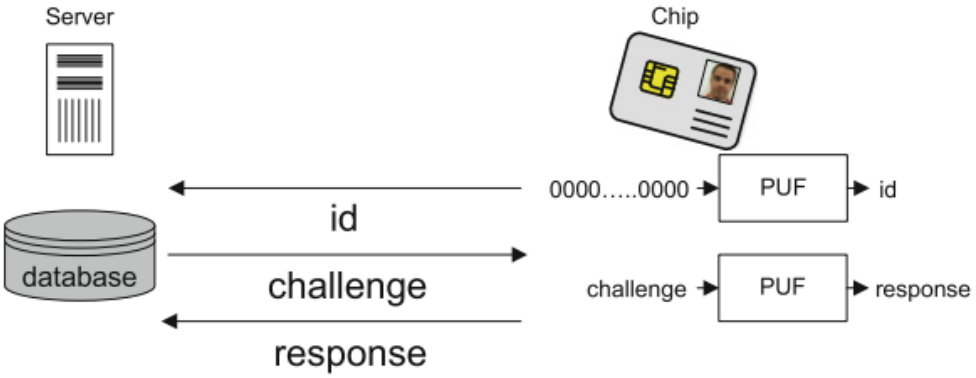
Μια βασισμένη στο υλικό CRP βασίζεται σε κυψέλες PUF, η έξοδος των οποίων εξαρτάται από μια είσοδο PUF: out = f (in). Τέτοια PUFs λειτουργούν με κάποιο τρόπο σαν συναρτήσεις κατακερματισμού. [11] Έτσι, οι παρακάτω ιδιότητες είναι σημαντικές:

• Ντετερμινιστικές: εκτός από τον πιθανό θόρυβο στην έξοδο, πρέπει να παραδίδεται πάντα η ίδια έξοδος για την ίδια είσοδο.

• Ομοιογένεια: κάθε πιθανή τιμή εξόδου πρέπει να δημιουργείται με την ίδια πιθανότητα.

• Πρόβλεψη: η έξοδος του PUF δεν πρέπει να είναι προβλέψιμη εάν η είσοδος ή άλλοι συνδυασμοί εισόδου-εξόδου είναι γνωστοί.

Αν όλες οι παραπάνω συνθήκες ικανοποιούνται, τότε λέμε ότι ένα PUF είναι κατάλληλο για σκοπούς αυθεντικοποίησης. Η ιδέα πίσω από την παραγωγή CRP βασισμένη στο υλικό απεικονίζεται στο σχήμα 2. Πρώτα απ' όλα, ο διακομιστής πρέπει να γνωρίζει την ταυτότητα του τσιπ. Για παράδειγμα, αυτό μπορεί να γίνει με την ανάγνωση ενός προκαθορισμένου ζεύγους CRP: ο μηδενικός φορέας μπορεί να χρησιμοποιηθεί ως είσοδος στο PUF. Η παραγόμενη απάντηση ορίζεται ως η ταυτότητα του τσιπ. Συνήθως, η επιστρεφόμενη απάντηση είναι θορυβώδης. Επομένως, ο διακομιστής πρέπει να συγκρίνει το αναγνωριστικό που έλαβε με τα αναγνωριστικά στις βάσεις δεδομένων. Αν η απόσταση Hamming σε ένα από τα αναγνωριστικά στη βάση δεδομένων είναι μικρότερη από μια ορισμένη προκαθορισμένη τιμή, το τσιπ αναγνωρίζεται. Μετά από αυτό, ο διακομιστής στέλνει μία πρόκληση των αποθηκευμένων CRP στο τσιπ. Η απόκριση παράγεται από το PUF και επιστρέφεται στον εξυπηρετητή. Εάν η απόκριση ταιριάζει σε ένα CRP με μια συγκριμένη ανοχή, τότε το τσιπ αυθεντικοποιείται.



Σχήμα 2: Αυθεντικοποίηση με Hardware-Based PUFs [10]

Πλεονεκτήματα (+) και μειονεκτήματα (-):

+ Δεν απαιτείται NVM.

+ Δεν απαιτείται διόρθωση σφάλματος.

+ Απλή προσέγγιση.

- Το υλικό PUF με CRP είναι δύσκολο να υλοποιηθεί.

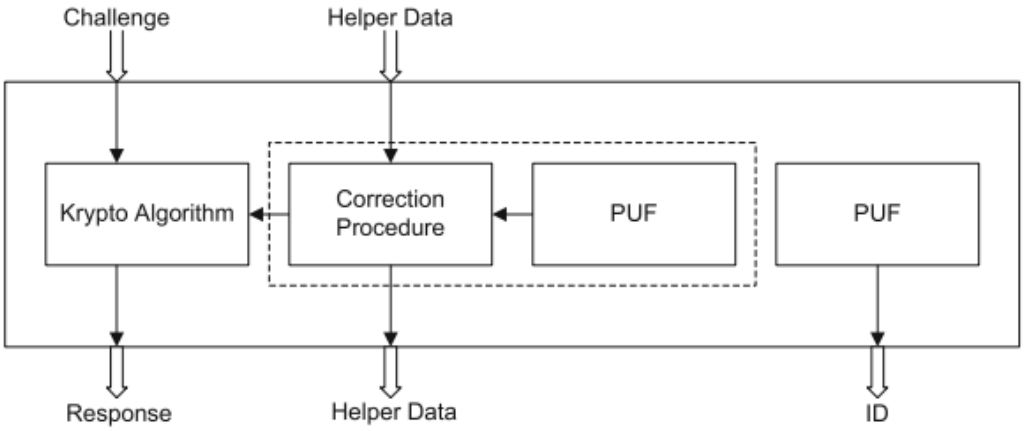
- Τα PUF είναι συγκριτικά μεγάλα σε μέγεθος.

- Ορισμένα CRPs πρέπει να αποθηκεύονται στο διακομιστή.

- Τα CRP πρέπει να παραχθούν σε αξιόπιστο περιβάλλον.

3. Αυθεντικοποίηση με CRPs βασισμένα σε Software

Η βασική ιδέα πίσω από αυτή την προσέγγιση είναι ότι η πρόκληση αντιστοιχίζεται σε μια απάντηση μέσω ενός αλγορίθμου κρυπτογράφησης. Στο σχέδιο 3 απεικονίζεται η βασική ιδέα. Διάφοροι αλγόριθμοι κρυπτογράφησης είναι κατάλληλοι. Ένα κλειδί χωρίς λάθη είναι που απαιτείται για την παραγωγή μιας ίδιας εξόδου για όλους αυτούς τους αλγορίθμους [12]. Σχετικά με τα PUFs αυτή η απαίτηση συνεπάγεται ότι πρέπει σε κάθε περίπτωση να γίνει διόρθωση σφάλματος.



Σχήμα 3: Αυθεντικοποίηση με Software – Based PUFs [10]

Στο παραπάνω σχήμα ένα σταθερό κλειδί επιστρέφεται από τα PUF. Οι διαφορετικές διαδικασίες για τη σταθεροποίηση της εξόδου ενός PUF περιγράφονται στη συνέχεια. Πρώτον, πρέπει να παραχθεί η ταυτότητα της οντότητας που πρέπει να επικυρωθεί. Αυτό μπορεί να γίνει με διάφορους τρόπους:

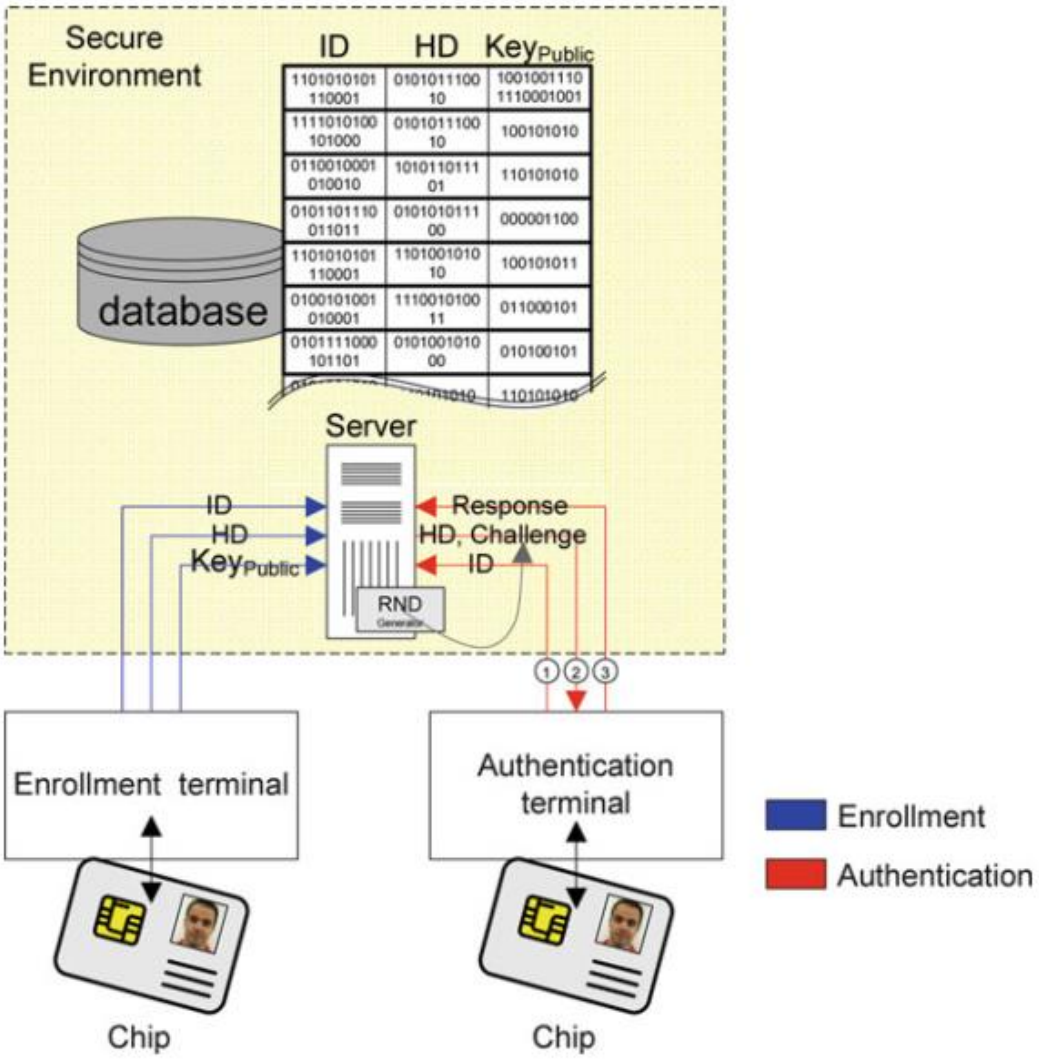
- Το αναγνωριστικό αποθηκεύεται εκτός του τσιπ και πρέπει να εισαχθεί σε ένα επιπλέον βήμα.
- Το αναγνωριστικό αποθηκεύεται στο τσιπ.
- Το αναγνωριστικό δημιουργείται χρησιμοποιώντας ένα δεύτερο PUF στο τσιπ.

Στη συνέχεια η οντότητα αυθεντικοποιείται ή όχι ανάλογα με τα δεδομένα που είναι αποθηκευμένα στον server.

Η κρυπτογράφηση δημόσιου κλειδιού και συμμετρικού κλειδιού μπορεί να χρησιμοποιηθεί για τη δημιουργία της απάντησης. Και οι δύο διαδικασίες εξηγούνται στις ακόλουθες ενότητες.

Κρυπτογράφηση δημόσιου κλειδιού

Όταν χρησιμοποιείται κρυπτογράφηση δημόσιου κλειδιού για την παραγωγή CRP, η εισερχόμενη πρόκληση είναι κρυπτογραφημένη με τη βοήθεια ενός ιδιωτικού κλειδιού στο τσιπ. Το αποτέλεσμα επιστρέφεται ως η απάντηση. Στη συνέχεια, η απόκριση μπορεί να αποκρυπτογραφηθεί στο διακομιστή με χρήση ενός δημόσιου κλειδιού. Εάν η αποκρυπτογραφημένη απόκριση ταιριάζει με την πρόκληση, η ταυτότητα του τσιπ επικυρώνεται. Για να επιτρέπεται η επαλήθευση ταυτότητας μιας οντότητας, κατά τη διάρκεια της αρχικής φάσης εγγραφής, το τσιπ πρέπει να καταχωρηθεί στο σύστημα.[10] Αργότερα, κατά τη διάρκεια της φάσης ελέγχου ταυτότητας, η ταυτότητα του τσιπ μπορεί να επαληθευτεί. Η όλη διαδικασία παρουσιάζεται στην εικόνα 6 και περιγράφεται στις ακόλουθες παραγράφους.



Εικόνα 6. Software – Based CRPs με χρήση κρυπτογράφησης δημόσιου κλειδιού [10]

Φάση εγγραφής:

- Πρέπει να δημιουργηθεί και να αποθηκευτεί στο διακομιστή ένα αναγνωριστικό του τσιπ. Το αναγνωριστικό χρησιμοποιείται για να βρεθεί το σωστό σύνολο δεδομένων στη βάση δεδομένων και επίσης να εντοπιστεί το τσιπ αργότερα.
- Το PUF παράγει δεδομένα εξόδου και βοηθητικά δεδομένα για μεταγενέστερη διόρθωση σφάλματος. Τα βοηθητικά δεδομένα (HD) μπορούν να αποθηκευτούν είτε εξωτερικά σε ένα διακομιστή είτε σε ένα εσωτερικό NVM,

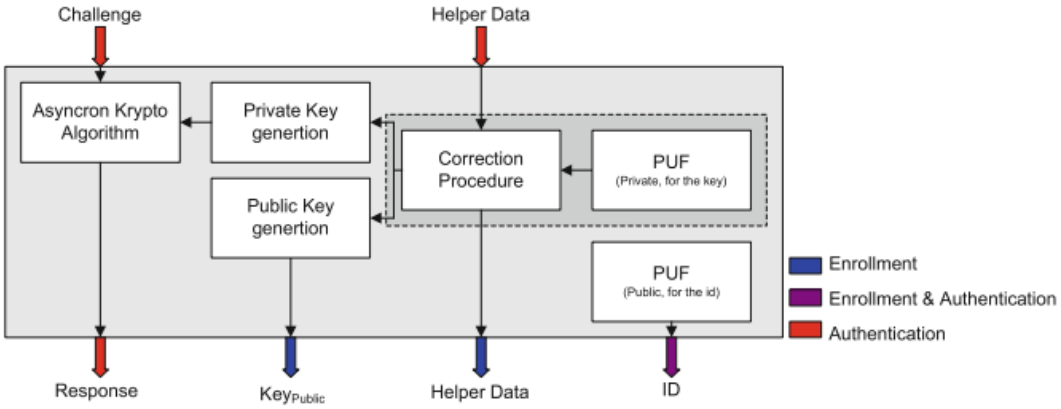
εάν υπάρχει. Στην εικόνα 6 τα HD μεταφέρονται στο διακομιστή και εισάγονται στη βάση δεδομένων.

- Το δημόσιο και το ιδιωτικό κλειδί προέρχονται από την παραγωγή του PUF. Τα παραγόμενα δημόσια κλειδιά αποστέλλονται στο διακομιστή όπου είναι αποθηκευμένα στη βάση δεδομένων. Η παραγωγή του δημόσιου κλειδιού πρέπει να γίνει για το τσιπ για λόγους ασφαλείας. Η έξοδος του PUF δεν πρέπει ποτέ να αφήσει το τσιπ.

Φάση αυθεντικοποίησης:

- Ως πρώτο βήμα, το αναγνωριστικό αποστέλλεται στο διακομιστή.
- Στη συνέχεια, ο διακομιστής στέλνει το HD στο τσιπ, αν είναι απαραίτητο. Επιπροσθέτως, ένας τυχαίος αριθμός δημιουργείται στο διακομιστή. Αυτός ο αριθμός παρέχεται ως πρόκληση για το τσιπ.
- Το PUF παράγει μια έξοδο χωρίς σφάλματα χρησιμοποιώντας τα βοηθητικά δεδομένα.
- Το τσιπ παράγει το ιδιωτικό κλειδί από την έξοδο του PUF.
- Η απόκριση παράγεται από το τσιπ. Αυτό γίνεται με την κρυπτογράφηση των λαμβανόμενων προκλήσεων με την χρήση του ιδιωτικού κλειδιού.
- Η απάντηση αποστέλλεται πίσω στο διακομιστή.
- Η απάντηση αποκρυπτογραφείται χρησιμοποιώντας το δημόσιο κλειδί.
- Αν τα δεδομένα ταιριάζουν, το τσιπ είναι αυθεντικοποιημένο.

Στην παρακάτω εικόνα βλέπουμε ένα διάγραμμα του τσιπ:



Εικόνα 7. Παραγωγή CRPs με χρήση κρυπτογράφησης δημόσιου κλειδιού [10]

Πλεονεκτήματα (+) και Μειονεκτήματα (-):

+ Τα PUF για την υλοποίηση είναι απλά και μικρά.

+ Τα CRPs δεν χρειάζεται να αποθηκεύονται σε ένα διακομιστή.

+ Τα CRPs δεν χρειάζεται να δημιουργούνται κατά τη φάση εγγραφής.

+ Οι απαιτήσεις ασφαλείας δεν είναι πολύ περιοριστικές.

+ Διανείμεται εύκολα η βάση δεδομένων (σε διαφορετικούς σταθμούς ελέγχου ταυτότητας).

- Η κρυπτογράφηση δημόσιου κλειδιού είναι πολύπλοκη από την άποψη της υπολογιστικής ισχύος. Ειδικά σε τσιπ, όπου οι πόροι (χρόνος, υλικό, ενέργεια) είναι περιορισμένοι, αυτό μπορεί να είναι ένα σοβαρό πρόβλημα.

- Πολλά PUF bits είναι απαραίτητα για να επιτευχθεί ένα αποδεκτό επίπεδο ασφάλειας.

3.2 Κρυπτογράφηση συμμετρικού κλειδιού

Υπάρχουν διάφοροι τρόποι χρήσης αλγορίθμων συμμετρικού κλειδιού για τον έλεγχο ταυτότητας τσιπ.[13] Υπάρχουν προσεγγίσεις όπου το μυστικό του PUF εγκαταλείπει το τσιπ. Αυτό δεν συνιστάται δεδομένου ότι η εγγενής παραγωγή του μυστικού είναι ένα από τα βασικά χαρακτηριστικά των PUF και θα πρέπει να χρησιμοποιείται για την αύξηση του επιπέδου ασφαλείας. Για τον λόγο αυτό τέτοιες προσεγγίσεις δεν λαμβάνονται υπόψη στην παρούσα διπλωματική εργασία.

Υπάρχουν διαφορετικά πλεονεκτήματα της κρυπτογράφησης συμμετρικού κλειδιού σε σύγκριση με ασύμμετρες προσεγγίσεις. Ένα από αυτά είναι ότι έχουν λιγότερες απαιτήσεις σε υπολογιστική ισχύ. Αυτό έχει ως αποτέλεσμα το χρησιμοποιούμενο μήκος κλειδιού να είναι μικρότερο. Για παράδειγμα το τυπικό μήκος κλειδιού του ασύμμετρου RSA είναι 1,024 bit. Το μήκος κλειδιού του συμμετρικού AES είναι μεταξύ 128 bit και 256 bit. Έτσι, ο σχεδιασμός των τσιπ είναι

λιγότερο πολύπλοκος σε σύγκριση με προσεγγίσεις οι οποίες χρησιμοποιούν κρυπτογράφηση δημόσιου κλειδιού.

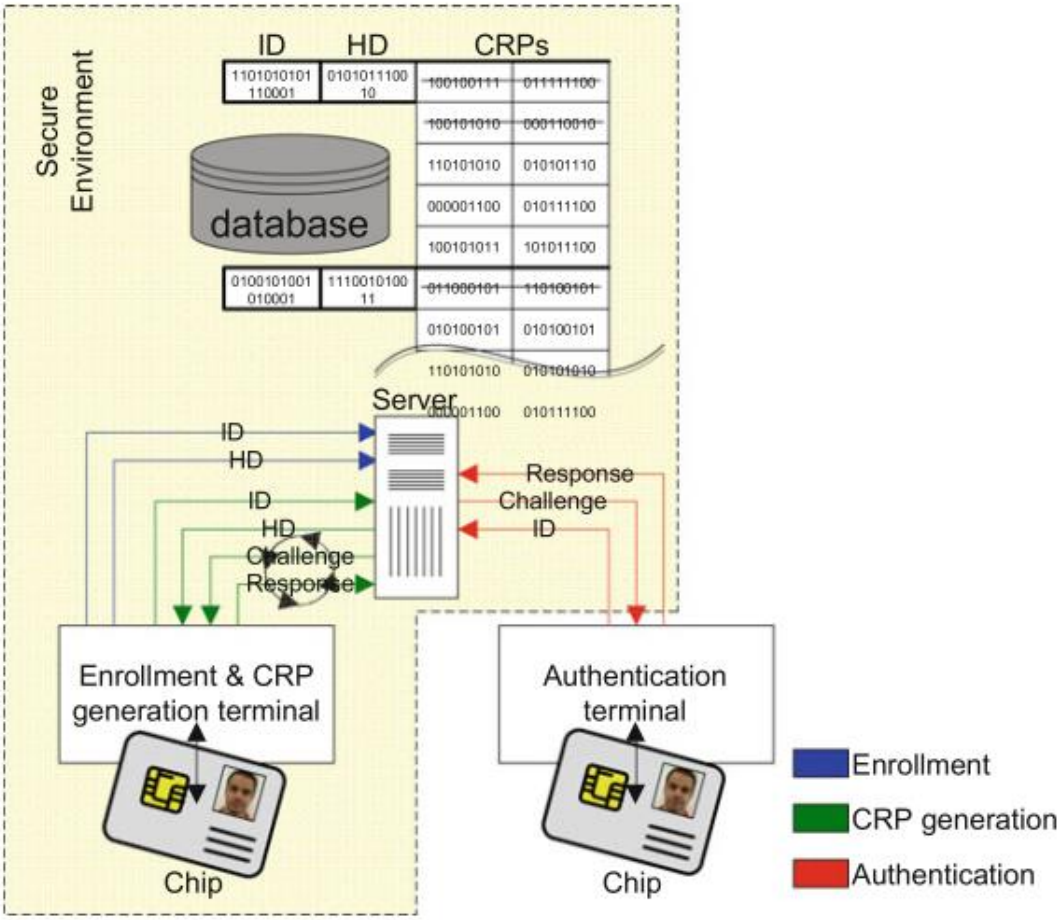
Στην παρούσα διπλωματική εργασία θα αναλυθούν δυο διαφορετικές υλοποίησες. Στην $1^{η}$ ένα σύνολο από CRPs αποθηκεύεται στον server. Στην $2^{η}$ εφαρμόζεται μια ιδέα για δυναμική ενημέρωση των CRPs.

3.2.1 Αποθήκευση Λίστας των CRPs στη Βάση Δεδομένων

Η όλη διαδικασία μπορεί να φανεί στην εικόνα 8. [10] Χωρίζεται σε τρεις φάσεις:

1. **Φάση εγγραφής:** Το τσιπ καταχωρείται στη βάση δεδομένων.
2. **Δημιουργία CRPs:** Ενημερώνεται η βάση δεδομένων των CRPs.
3. **Έλεγχος ταυτότητας:** Τα τσιπ επικυρώνονται χρησιμοποιώντας τα δεδομένα από τη βάση δεδομένων.

Οι τρεις αυτές φάσεις περιγράφονται λεπτομερέστερα παρακάτω.



Εικόνα 8. Συσκευές στη CRP προσέγγιση [10]

Φάση Εγγραφής

Η φάση εγγραφής φαίνεται στις μπλε γραμμές της εικόνας 8. Κατά την φάση εγγραφής :

1. Το PUF παράγει μια έξοδο και τα απαραίτητα βοηθητικά δεδομένα. Αυτά τα βοηθητικά δεδομένα μπορεί να αποθηκευτούν εξωτερικά σε ένα διακομιστή ή σε ένα εσωτερικό NVM.
2. Ένα αναγνωριστικό του τσιπ πρέπει επίσης να αποθηκευτεί στο διακομιστή. Η δημιουργία του αναγνωριστικού μπορεί να γίνει χρησιμοποιώντας ένα δεύτερο PUF ή μια προκαθορισμένη πρόκληση (zero-vector).

Δημιουργία CRPs

Η φάση δημιουργίας CRPs φαίνεται στις πράσινες γραμμές της εικόνας 8. Σε αυτήν την φάση έχουμε τα εξής βήματα:

1. Τα ζεύγη πρόκλησης-απόκρισης παράγονται σε ένα ασφαλές περιβάλλον. Συνήθως ο διακομιστής δημιουργεί μια πρόκληση η οποία στη συνέχεια αποστέλλεται στο τσιπ. Το τσιπ επιστρέφει την αντίστοιχη απόκριση.
2. Αυτά τα δεδομένα CRP αποθηκεύονται σε μια βάση δεδομένων. Για κάθε έλεγχο ταυτότητας ένα CRP χρησιμοποιείται. Συνεπώς, ο αριθμός των αποθηκευμένων CRP εξαρτάται από την εφαρμογή και τη συχνότητα της επαλήθευσης ταυτότητας.
3. Εάν χρησιμοποιηθούν όλα τα CRPs, η βάση δεδομένων μπορεί να ξαναγεμίσει με νέα CRPs με τον ίδιο τρόπο και πάλι σε ασφαλές περιβάλλον.

Φάση Αυθεντικοποίησης

Η φάση αυθεντικοποίησης φαίνεται με κόκκινες γραμμές στην εικόνα 8. Κατά την φάση αυτή:

1. Στο πρώτο βήμα ο server λαμβάνει ένα αναγνωριστικό από το τσιπ.
2. Στο δεύτερο βήμα ο server στέλνει ένα challenge στο τσιπ.
3. Στο τρίτο βήμα το τσιπ παράγει την απάντηση με βάση το εσωτερικό κλειδί που έχει παραχθεί από το PUF. Η απάντηση στέλνεται στον server.
4. Στο τέταρτο βήμα συγκρίνεται η απάντηση που στάλθηκε με αυτήν που είναι αποθηκευμένη στον server. Αν ταιριάζει τότε το τσιπ αυθεντικοποιείται.

Οι δημοφιλείς αλγόριθμοι για αυτήν την προσέγγιση είναι ο AES (με χρήση συμμετρικού κλειδιού) ο MD5 και ο SHA-1 (και οι δύο με χρήση συναρτήσεων κατακερματισμού).

Πλεονεκτήματα (+) και Μειονεκτήματα (-)

+ Ο αλγόριθμος είναι υπολογιστικά λιγότερο περίπλοκος από τις προσεγγίσεις του δημόσιου κλειδιού.

+ Η υλοποίηση είναι απλή.

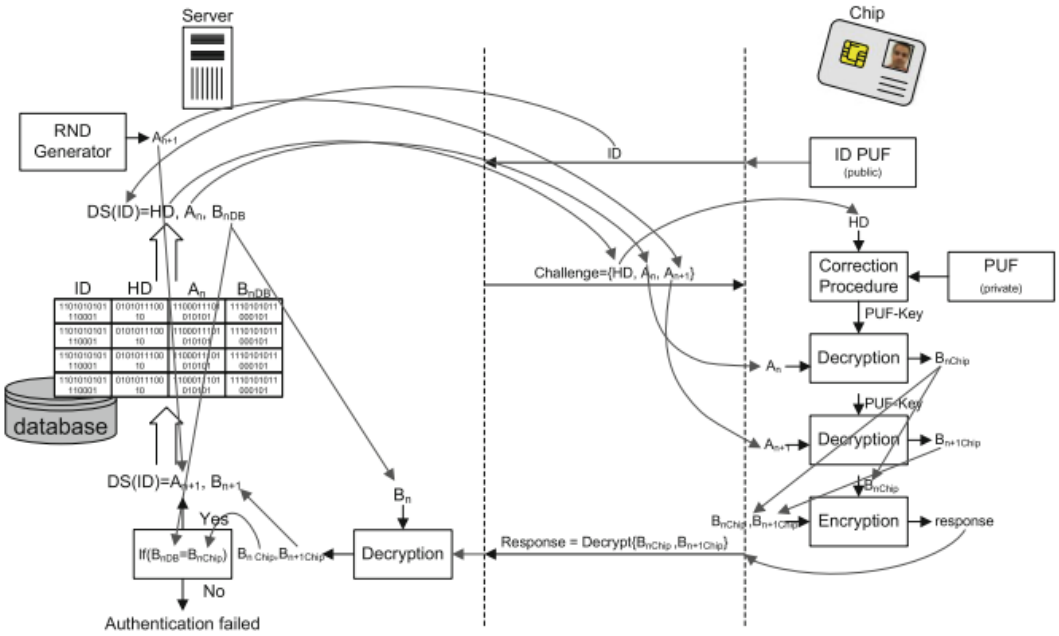
- Λόγω της θορυβώδους εξόδου των PUF απαιτείται η χρήση ενός αλγορίθμου για την διόρθωση λαθών.

- Πρέπει να αποθηκεύονται τα CRPs στον server.

- Όταν όλα τα CRPs χρησιμοποιηθούν θα πρέπει να ξαναπαραχθούν.

3.3 Δυναμική Ενημέρωση των CRPs

Το πλεονέκτημα της δυναμικής ενημέρωσης CRP είναι ότι μόνο ένα CRP είναι αποθηκευμένο στη βάση δεδομένων κάθε φορά. Ένα νέο CRP δημιουργείται κατά τη διάρκεια κάθε ανάγνωσης. Έτσι, δεν υπάρχει περιορισμός όσον αφορά τον αριθμό των αυθεντικοποιήσεων ανάλογα με τα CRPs που είναι αποθηκευμένα, καθώς αυτά παράγονται δυναμικά. Η υλοποίηση φαίνεται στην εικόνα 9.



Εικόνα 9. Δυναμική ενημέρωση CRP, Φάση Αυθεντικοποίησης [10]

Δεν απαιτείται ειδική φάση παραγωγής CRP. Η φάση εγγραφής είναι σχεδόν ίδια με την προηγούμενη προσέγγιση. Επιπλέον, ένα CRP αποθηκεύεται στη βάση δεδομένων.

Φάση Εγγραφής

Τα βήματα της φάσης εγγραφής είναι:

1. Το PUF παράγει έξοδο και τα απαραίτητα βοηθητικά δεδομένα. Αυτά τα βοηθητικά δεδομένα μπορεί να αποθηκευτούν σε έναν server εξωτερικά ή σε εσωτερικό NVM.
2. Ένα αναγνωριστικό του τσιπ πρέπει επίσης να αποθηκευτεί στο server. Η δημιουργία του αναγνωριστικού μπορεί να γίνει χρησιμοποιώντας ένα δεύτερο PUF ή μια προκαθορισμένη πρόκληση (zero-vector).
3. Σε ένα ασφαλές περιβάλλον δημιουργείται ένα ζευγάρι απόκρισης πρόκλησης. Το B_n (εικόνα 9) πρέπει να είναι διαθέσιμο και στις δύο πλευρές για την κρυπτογράφηση / αποκρυπτογράφηση των δεδομένων που

αποκτήθηκαν. Ο zero-vector μπορεί να χρησιμοποιηθεί κατά τη διάρκεια της φάσης εγγραφής. Το CRP θα αποθηκευτεί στη βάση δεδομένων.

Φάση Αυθεντικοποίησης

Η φάση αυθεντικοποίησης περιλαμβάνει τα εξής βήματα:

1. Στο πρώτο βήμα ο διακομιστής λαμβάνει το αναγνωριστικό από το τσιπ.
2. Ο διακομιστής στέλνει τα βοηθητικά δεδομένα, την πραγματική πρόκληση A_n και μια νέα πρόκληση A_{n+1} που προέρχεται από ένα RNG (random number generator) στο τσιπ.
3. Το τσιπ παράγει μια απάντηση μέσω του εσωτερικού κλειδιού που δημιουργήθηκε από το PUF. Και οι δύο προκλήσεις αποκρυπτογραφούνται ξεχωριστά. Μετά από αυτό, οι δύο απαντήσεις B_n,chip και B_{n+1},chip συγχωνεύονται και κρυπτογραφούνται με την πρώτη απάντηση B_n,chip. Τα κρυπτογραφημένα δεδομένα αποστέλλονται στο διακομιστή.
4. Στο διακομιστή, το κλειδί κρυπτογράφησης είναι γνωστό, δεδομένου ότι είναι η απόκριση B_n στην πρώτη πρόκληση A_n. Έτσι, τα ληφθέντα δεδομένα αποκρυπτογραφούνται χρησιμοποιώντας αυτήν την απάντηση. Αν τα δεδομένα από το τσιπ είναι σωστά, τα αποκρυπτογραφημένα δεδομένα αποτελούνται από την απάντηση στην πρώτη πρόκληση B_n,chip και η απάντηση στη δεύτερη πρόκληση B_{n+1},chip . Ως εκ τούτου, το τσιπ πιστοποιείται από την απάντηση στην πρώτη πρόκληση. Η απάντηση στη δεύτερη πρόκληση αποθηκεύεται στο διακομιστή ως η πρώτη πρόκληση για την επόμενη διαδικασία ελέγχου ταυτότητας.

Ένας αλγόριθμος προσαρμογής για αυτήν την προσέγγιση είναι ο συμμετρικός block AES.

Πλεονεκτήματα (+) και Μειονεκτήματα (-)

+ Ο αλγόριθμος είναι υπολογιστικά λιγότερο περίπλοκος από τις προσεγγίσεις του δημόσιου κλειδιού.

+ Δεν χρειάζεται να αποθηκεύονται πολλά CRPs στον server.

- Απαιτείται η χρήση αλγόριθμου διόρθωσης.

- Η όλη προσέγγιση είναι κάπως περίπλοκη.

4. Συγκριτική Μελέτη των Διαφορετικών Τεχνολογιών PUFs

Στη συνέχεια παρουσιάζονται οι διαφορετικές τεχνολογίες PUFs που έχουν αναπτυχθεί και αναλύονται τα πλεονεκτήματα και τα μειονεκτήματα τους. Πριν από αυτό είναι σημαντικό να εξεταστούν οι παράγοντες που επηρεάζουν την αποδοτικότητα των PUFs.[14] Επίσης πρέπει να καθοριστούν τα χαρακτηριστικά που ξεχωρίζουν τα PUFs μεταξύ τους, για να συγκριθούν PUFs που έχουν παρόμοιες τεχνολογίες. Τέτοια παραδείγματα μπορεί να είναι:

- Κοινά PUF
- PUF που συμπεριλαμβάνουν προεπεξεργασία
- PUF που περιλαμβάνουν διόρθωση σφαλμάτων.

Επιπλέον, είναι σημαντικό να προσδιοριστούν εκ των προτέρων οι περιβαλλοντικές συνθήκες στις οποίες τα PUFs ελέγχονται. Ειδικά, το εύρος θερμοκρασίας επηρεάζει την εμφάνιση σφαλμάτων και λαμβάνεται σοβαρά υπόψιν κατά την διενέργεια ελέγχων.

Υπάρχουν δύο εναλλακτικές λύσεις για τον έλεγχο ενός PUF: μπορεί είτε να δοκιμαστεί το πλακίδιο ή μετά τη συσκευασία. Το πλεονέκτημα της δοκιμής των πλακιδίων είναι τα τεράστια ποσά δεδομένων που μπορούν να συλλεχθούν. Έτσι, μπορούν να αξιολογηθούν ακριβή στατιστικά στοιχεία. Ακόμα κι αν η μέτρηση γίνει μέσα στο πακέτο, το PUF δείχνει ακριβώς τη συμπεριφορά που θα έχει αργότερα στο πεδίο. Επιπλέον, η ανάλυση μπορεί να γίνει σε οποιοδήποτε εργαστήριο που διευκολύνει την διαδικασία. Μπορούν να ελεγχθούν τουλάχιστον οι βασικές λειτουργίες και οι παράμετροι απόδοσης (π.χ. κατανάλωση).

4.1 Βασικές Παράμετροι Αποδοτικότητας PUFs

Hamming Distance

Η Hamming Distance έχει αναλυθεί και παραπάνω οπότε εδώ απλά θα δώσουμε έναν ποσοτικό ορισμό για την μέτρηση της Hamming Distance (HD) . [15] Έστω ότι έχουμε δύο string που είναι 8 bits και διαφέρουν μεταξύ τους σε 4 bits. Η HD τους είναι:

$$HD(String1, String2) = 0.5 \; or \; 50\%$$

Διωνυμική Κατανομή

Εάν τα στοιχεία των bit string είναι τυχαίες μεταβλητές, τα HD μεταξύ διαφορετικών συμβολοσειρών καταλήγουν σε διωνυμική κατανομή. Η διωνυμική κατανομή ορίζεται ως:

$$\binom{n}{k} p^k (1-p)^{n-k}$$

όπου n είναι ο αριθμός των δυαδικών ψηφίων στο string, k ο αριθμός των "1" και p η πιθανότητα εμφάνισης "1."

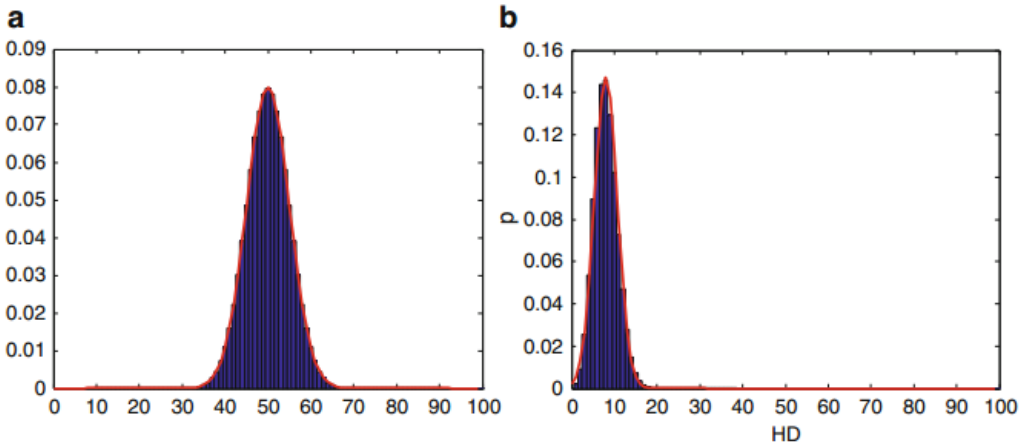
Εάν ο αριθμός των δυαδικών ψηφίων είναι μεγάλος, η κανονική κατανομή είναι μια καλή προσέγγιση για την διωνυμική κατανομή. Οι εξισώσεις στο (4.1) δείχνουν την μετατροπή μιας διωνυμικής διανομής σε Gaussian διανομή:

$$\mu = np$$

$$\sigma^2 = npq$$

Σε ορισμένες περιπτώσεις, αυτή η μετατροπή είναι πολύ χρήσιμη. Στο Σχήμα 4.2 βλέπουμε δύο παραδείγματα διωνυμικών κατανομών για n = 100 (μ = 50, σ = 5, μ = 8, σ = 2.713). Οι κόκκινες καμπύλες δείχνουν τις κατάλληλες κατανομές Gaussian.

(4.1) Διωνυμική κατανομή: η = 100, p = 0,5, q = 0,5 (μπλε ράβδους). Gaussian διανομή: μ = 50, σ = 5 (κόκκινη καμπύλη). (b) Διωνυμική κατανομή: η = 100, p = 0,08, q = 0,92 (μπλε ράβδοι). Gaussian κατανομή: μ = 8, σ = 2.713 (κόκκινη καμπύλη) [10]



Είναι εύκολο να προσδιοριστούν οι τιμές p και q για έναν ορισμένο αριθμό N διωνύμου σε κατανεμημένα σύνολα δεδομένων DS. n είναι ο αριθμός των δυαδικών ψηφίων σε κάθε σύνολο δεδομένων. Ο μέσος όρος όλων των δυαδικών ψηφίων μ_{all} σε όλα τα σύνολα δεδομένων καθορίζεται σε ένα πρώτο βήμα:

$$(4.2): \mu_{all} \approx \frac{\#\ \tau\omega\nu\ 1s\ \sigma\varepsilon\ \acute{o}\lambda\alpha\ \tau\alpha\ DS}{n*N}$$

Το p μπορεί να υπολογιστεί από το (4.2):

$$p = \frac{\mu_{all}}{n}$$

$$q = 1\text{-}p$$

4.2 Προδιαγραφές Παραμέτρων

Για να χαρακτηρίσουν οι ιδιότητες του υλικού ενός PUF προτείνεται να ληφθούν υπόψιν οι ακόλουθες παράμετροι:

- Μέση τιμή
- Ποσοστό σφαλμάτων
- Συσχέτιση μεταξύ των δυαδικών ψηφίων
- Συσχέτιση μεταξύ των τσιπ
- Κατανάλωση Ενέργειας

Οι παραπάνω παράμετροι θα αναλυθούν λεπτομερώς στη συνέχεια.

4.2.1 Το ιδανικό PUF

Στον πίνακα 1 βλέπουμε τις ιδιότητες του ιδανικού PUF. Οι τιμές που αναφέρονται αφορούν τις ιδανικές ιδιότητες οι οποίες είναι αδύνατον να ικανοποιηθούν. Για παράδειγμα δεν γίνεται να έχουμε ένα ποσοστό σφαλμάτων bit 0% και κατανάλωση ενέργειας 0 pj/bit.

Property	Identifier	Value
Mean value	μ	$0.5, \sigma = \frac{\sqrt{N}}{2}$
Error rate	$HD_{intra(120C)}$	0 %
Corr. between bits	R_{xx}	$0, \sigma = \frac{1}{2\sqrt{N}}$
Corr. between chips	HD_{inter}	$50, \% \sigma = 100\% \frac{\sqrt{N}}{2}$
Power consumption	E/bit	0 pJ/bit

Πίνακας 1: Ιδιότητες του ιδανικού PUF [10]

4.2.2 Μέση Τιμή

Η έξοδος ενός PUF δεν πρέπει να είναι προβλέψιμη. Έτσι, στην έξοδο οι τιμές "1" και "0" πρέπει να κατανέμονται εξίσου. Κοιτάζοντας την έξοδο του τσιπ, η αριθμητική μέση τιμή x των 4,096 κελιών θα πρέπει να είναι περίπου 0,5, όπου το x ορίζεται ως:

$$\mathbf{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \qquad (1)$$

όπου n είναι ο αριθμός των κελιών και x_i η πραγματική έξοδος. Από τα αποτελέσματα των δέκα δοκιμών τα τσιπ διανέμονται διμερώς, τα διαφορετικά x τοποθετούνται στην κορυφή της πιθανότητας (pd f) μιας διωνυμικής κατανομής (μπλε καμπύλη). Το αποτέλεσμα μπορεί να είναι όπως φαίνεται στο σχήμα 2. Όλα τα x βρίσκονται γύρω στο 0,5. Αυτό είναι το αναμενόμενο αποτέλεσμα. Ωστόσο, μια μικρή τάση προς το "1" μπορεί να παρατηρηθεί. Αυτή η τάση οφείλεται σε στατιστικά λάθη. Έτσι, η τάση δεν επηρεάζει σημαντικά την προβλεψιμότητα. Το ποσό της μεροληψίας που μπορεί να γίνει αποδεκτή εξαρτάται έντονα από την εφαρμογή για ποιους σκοπούς χρησιμοποιούνται τα δεδομένα.

Το εμπιστευτικό διάστημα (CI) μπορεί να χρησιμοποιηθεί για να καθοριστεί αν τα δεδομένα βρίσκονται εντός ενός αναμενόμενου εύρους. Για παράδειγμα, εάν υπάρχει ένα διάστημα εμπιστοσύνης 95% και χρησιμοποιείται το κανονικό διάστημα προσέγγισης, το CI μπορεί να προσδιοριστεί ως:

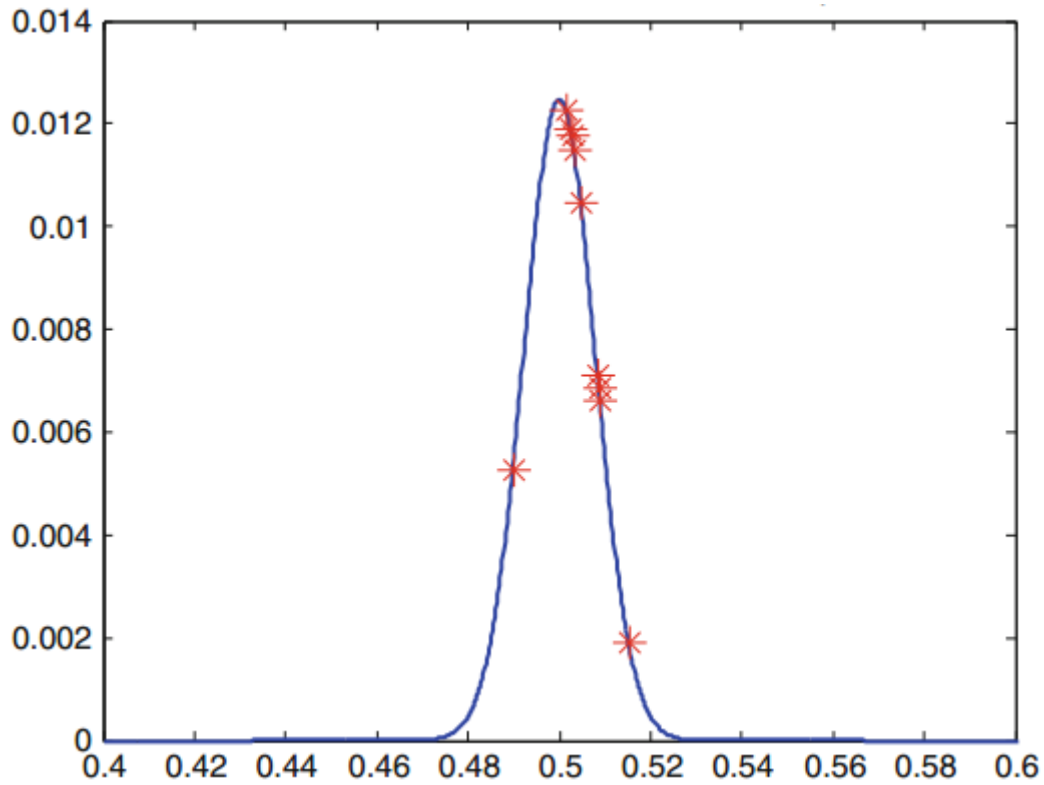
$$\mathbf{CI} = \mathbf{p} \pm z\sqrt{\frac{p(1-p)}{n}} \qquad (2)$$

όπου p είναι η πιθανότητα εμφάνισης, n είναι ο αριθμός των bits εξόδου και z είναι το 1 - α / 2 εκατοστημόριο, α είναι το εκατοστημόριο σφάλματος. Στην περίπτωση αυτή α = 5% 1 - α / 2 = 0,975 και z (0,975) = 1,96. Σύμφωνα με το p = 0,5, η (2) γίνεται:

$$\mathbf{CI = 0.5 \pm 1.96\sqrt{\frac{0.25}{4.096}} = 0.4846 \text{ και } 0.5154}$$

Επομένως, όλα τα x των δοκιμαστικών τσιπς βρίσκονται μέσα στο εμπιστευτικό διάστημα.

Αριστερά: Μέση Τιμή Διαφορετικών Τσιπ



Κάτω: Μέση Τιμή

Σχήμα 2: Μετρούμενες μέσες τιμές στην κορυφή μιας διωνυμικής κατανομής [10]

4.2.3 Συχνότητα Εμφάνισης Σφαλμάτων

Η έξοδος ενός PUF θα πρέπει να παραμείνει σταθερή εντός μιας προκαθορισμένης περιοχής λειτουργίας. Παρουσιάζονται σφάλματα, εάν τα bits αλλάζουν τις τιμές εξόδου μεταξύ διαφορετικών διαδρομών. Η συχνότητα εμφάνισης λαθών (Bit error rate-BER) μπορεί να μετρηθεί χρησιμοποιώντας την απόσταση Hamming (HD) που έχει ήδη αναλυθεί σε προηγούμενη ενότητα.

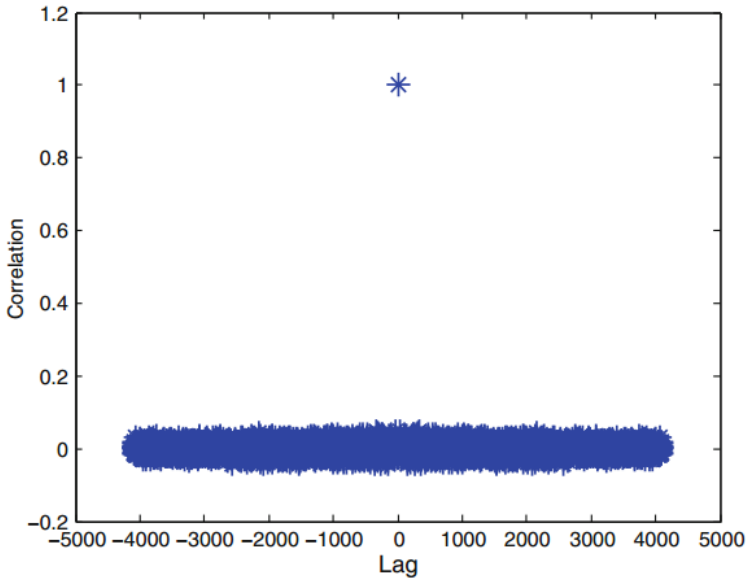
Για να προσδιοριστεί το ποσοστό σφάλματος ενός PUF, το HD του προσδιορίζεται με ένα διάνυσμα αναφοράς και υπολογίζεται η πραγματική έξοδος. Σε αυτή την περίπτωση η Hamming απόσταση ονομάζεται HD intra-chip (HD_{intra}). Σε ένα ιδανικό PUF αυτή η τιμή είναι 0. Λόγω της επίδρασης του θορύβου, της θερμοκρασίας, της μεταβολής της παροχής ενέργειας και της διακύμανσης του ρεύματος αυτή η τιμή υπερβαίνει το 0.

4.2.4 Συσχέτιση μεταξύ των δυαδικών ψηφίων

Τα γειτονικά κελιά δεν πρέπει να αλληλεπιδρούν μεταξύ τους για την αποφυγή ζητημάτων ασφάλειας. [16] Συσχέτιση μεταξύ των κελιών θα μπορούσε να μειώσει τον αριθμό των πιθανών συνδυασμών και έτσι θα αυξανόταν ο κίνδυνος επιτυχούς επίθεσης με brute-force. Για να ελεγχθεί αν υπάρχει συσχέτιση στο τσιπ δοκιμής, χρησιμοποιείται η λειτουργία αυτόματης συσχέτισης με χρήση της συνάρτησης R_{xx}:

$$\boldsymbol{R_{xx}\,(J) = \int_n x_n x_{n-j}\,,} \quad \textbf{(3)}$$

όπου το Rxx αξιολογείται με την υστέρηση j. Για Rxx (j) = 1 και Rxx (j) = -1 τα δεδομένα στην υστέρηση j είναι πλήρως συσχετισμένα. Για το Rxx (j) = 0, τα δεδομένα είναι εντελώς άσχετα. Το αποτέλεσμα μέτρησης του τσιπ δοκιμής φαίνεται στο σχήμα 4.6. Τα δεδομένα συσχετίζονται μόνο στην υστέρηση j = 0. Η συσχέτιση είναι αμελητέα για καθυστερήσεις διαφορετικές από 0, και έτσι το δοκιμαστικό τσιπ πληροί τις απαιτήσεις.



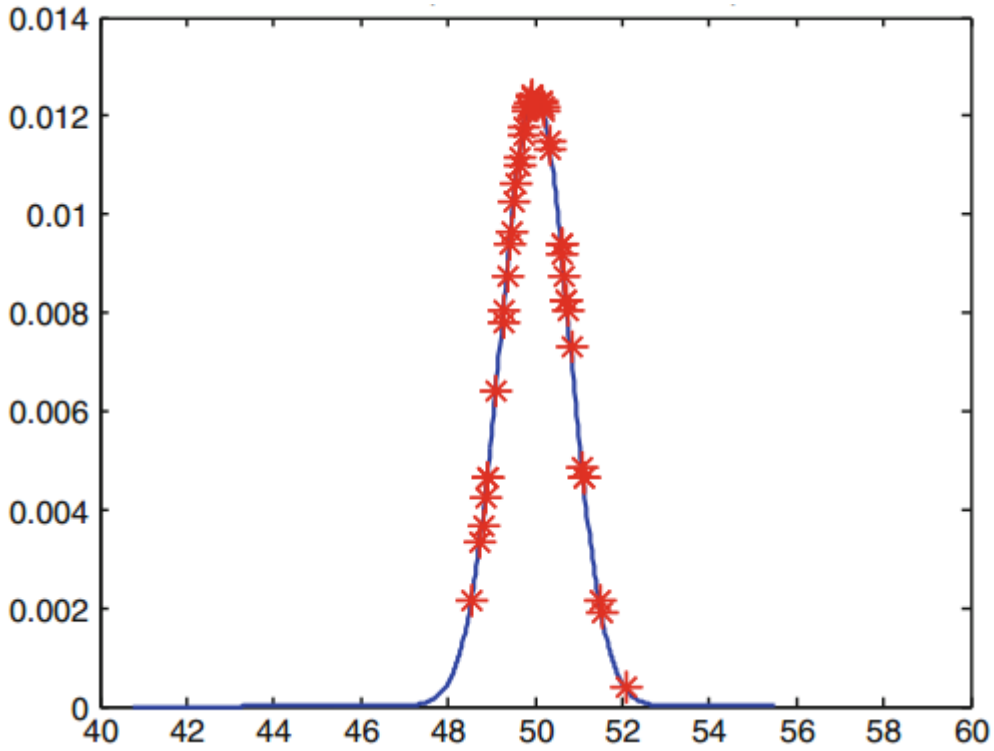
Σχήμα 3. Αυτοσυσχέτιση του PUF [10]

Αν η διάταξη δεν γίνει με προσοχή, είναι πιθανό να εξαρτάται η έξοδος των κελιών από τη θέση στη διάταξη. Εάν συμβαίνει αυτό, τα συγκεκριμένα κελιά τείνουν να έχουν κάποια τιμή. Αυτό το αποτέλεσμα οδηγεί σε ζητήματα ασφάλειας, καθώς από τη στιγμή που γνωρίζουμε την παραγωγή ενός τσιπ είναι ευκολότερο να προβλεφθεί η έξοδος άλλων τσιπ. Όπως και στην περίπτωση του ποσοστού σφαλμάτων, η συσχέτιση μεταξύ διαφορετικών τσιπ μπορεί να προσδιοριστεί χρησιμοποιώντας την απόσταση Hamming. Υπό αυτές τις συνθήκες το HD ονομάζεται απόσταση μεταξύ των τσιπ (inter-chip) HD (HD_{inter}) και πρέπει να είναι περίπου 50%. Εάν ο μέσος συντελεστής HD_{inter} όλων των συνδυασμών των τσιπ είναι 50%, δεν υπάρχει συσχέτιση μεταξύ των τσιπ της διάταξης. Η υποκείμενη κατανομή είναι η διωνυμική κατανομή.

Στο σχήμα 4 βλέπουμε τις τιμές HD_{inter} που μετρήθηκαν σε δέκα τσιπ δοκιμής. Και πάλι, τα αποτελέσματα τοποθετούνται σε διωνυμική κατανομή. Η μέση τιμή όλων των HD_{inter} είναι 50.0271% που είναι κοντά στη βέλτιστη τιμή του 50%.

Άξονας y: Inter-Chip των 10 τσιπ δοκιμής

Άξονας x: HD%



Σχήμα 4. Inter-Chip Hamming από δέκα τσιπ δοκιμής στη διωνυμική κατανομή[10]

4.2.5 Ισχύς και Κατανάλωση Ενέργειας

Εάν το PUF χρησιμοποιείται σε συσκευές όπως ετικέτες RFID, η κατανάλωση ενέργειας παίζει σημαντικό ρόλο. Αλλά και η κατανάλωση ενέργειας έχει συχνά ενδιαφέρον. Στην περίπτωση του τσιπ της δοκιμής η μέση κατανάλωση ρεύματος είναι περίπου 290 μA. Για V_{DD} = 1,35 V η ισχύς γίνεται:

$$\mathbf{P = 290\mu A * 1.35V = 391.5\mu W} \qquad \mathbf{(4)}$$

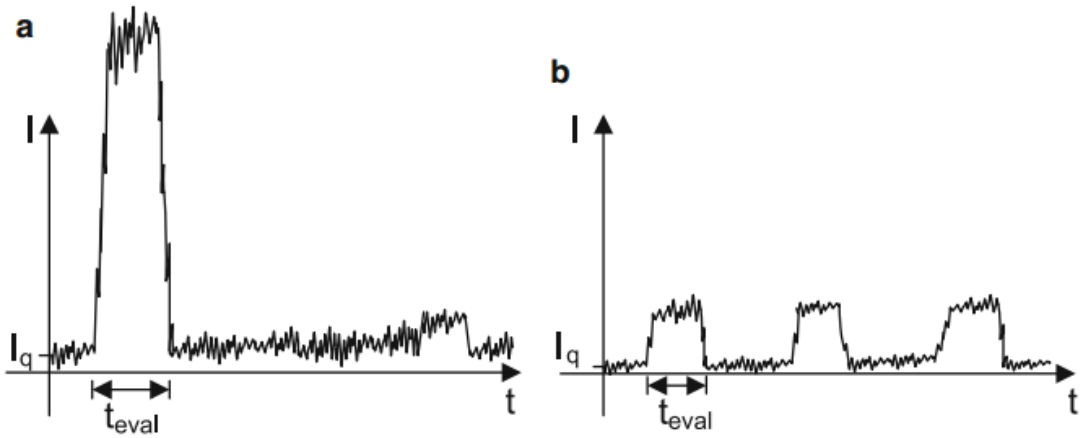
Χρησιμοποιώντας μια συχνότητα ρολογιού 1 Mhz και μία έξοδο bit ανά κύκλο, η κατανάλωση ενέργειας ανά κελί υπολογίζεται:

$$\mathbf{Ebit = 391.5\mu W * 1}\ \frac{\boldsymbol{\mu s}}{\boldsymbol{bit}}\ \mathbf{= 391.5}\ \frac{\boldsymbol{Pj}}{\boldsymbol{bit}} \quad \mathbf{(5)}$$

Σε σύγκριση με άλλες προσεγγίσεις, αυτή είναι μια αρκετά υψηλή τιμή. Μία ελάχιστη τιμή 1.6 $\frac{Pj}{bit}$ δημοσιεύθηκε στο [18].

Δεδομένου ότι η κατανάλωση ενέργειας δεν αποτελούσε κριτήριο σχεδιασμού, εξακολουθεί να υπάρχει περιθώριο βελτίωσης. Ένα απλό παράδειγμα θα ήταν η αύξηση της συχνότητας του ρολογιού.

Εάν η κατανάλωση ενέργειας είναι ανησυχητική, ένας τρόπος διανομής της ενέργειας με την πάροδο του χρόνου φαίνεται στο σχήμα 5. Απεικονίζεται η διαφορά της κατανάλωσης ισχύος μεταξύ παράλληλης (parallel) και σειριακής (serial) ανάγνωσης (read-out). Η ενσωματωμένη ενέργεια είναι σχεδόν η ίδια. Στο σχήμα 5a τα κελιά διαβάζονται παράλληλα ταυτόχρονα. Σε αυτή την περίπτωση, κελιά μπορούν να διαβαστούν πολύ γρήγορα. Το μειονέκτημα αυτής της προσέγγισης είναι η κορυφή της τρέχουσας κατανάλωσης. Ολόκληρη η ενέργεια για την αξιολόγηση ($t_{eval)}$ πρέπει να είναι διαθέσιμη σε σύντομο χρονικό διάστημα. Στο σχήμα 5b η ανάγνωση πραγματοποιείται σειριακά (απεικονίζεται η ανάγνωση των τριών κελιών). Στην περίπτωση αυτή η κατανάλωση ενέργειας αιχμής είναι πολύ μικρότερη, αλλά εμφανίζεται αρκετές φορές. Η συνολική κατανάλωση ενέργειας εξαπλώνεται σε μεγαλύτερο χρονικό διάστημα. Το μειονέκτημα αυτής της προσέγγιση είναι η αύξηση του χρόνου αξιολόγησης. Η σειριακή ανάγνωση είναι χρήσιμη για εφαρμογές περιορισμένης μέγιστης ισχύος.



Σχήμα 5: Κατανάλωση ισχύος: α) Παράλληλη ανάγνωση β) Σειριακή ανάγνωση [10]

4.3 Εναλλακτικές Συγκρίσιμες Ιδιότητες

Στην παρακάτω ενότητα θα ασχοληθούμε με εναλλακτικές μεθόδους και πρόσθετες ιδιότητες οι οποίες χαρακτηρίζουν ένα τσιπ PUF.

4.3.1 Μέγεθος

Το μέγεθος του PUF μπορεί να χαρακτηριστεί από την περιοχή ανά bit ($\frac{m^2}{bit}$). Δεδομένου ότι το μέγεθος εξαρτάται σε μεγάλο βαθμό από την τεχνολογία, είναι ευεργετικός ο γενικός προσδιορισμός περιοχής μεγέθους.[17] Σε αυτήν την περίπτωση η περιοχή εκφράζεται σε $\frac{f^2}{bit}$, όπου το f^2 είναι το ελάχιστο μέγεθος χαρακτήρων. Είναι το τετράγωνο του ελάχιστου μήκους καναλιού. F^2 = 8.100 nm^2 σε διεργασία 90 nm. Για παράδειγμα, ένα κοινό 6T-SRAM κελί έχει F^2 140.

4.3.2 Συσχέτιση μεταξύ των τσιπ: Εναλλακτική μέθοδος

Η μέθοδος που εισήχθη στην Ενότητα. 4.2.4 (HD_{inter}) είναι η προτιμώμενη προσέγγιση για την ανίχνευση της συσχέτισης μεταξύ τσιπ.[10] Ωστόσο, χρησιμοποιώντας HD_{inter} ένα μόνο μπιτ ενδέχεται να παρέχει τη ίδια έξοδο σε κάθε τσιπ, πράγμα το οποίο δεν μπορεί να ανιχνευθεί. Εάν υπάρχει η πιθανότητα ορισμένα κελιά να παράγουν πάντοτε την ίδια έξοδο (π.χ., λόγω προβλημάτων σχεδίου), πρέπει να επιλεγεί μια διαφορετική υλοποίηση. Μια εφικτή προσέγγιση είναι να υπολογιστεί ο μέσος όρος κάθε κυψέλης πάνω από όλα τα διαθέσιμα τσιπ:

$$\boldsymbol{\mu(j) = \frac{1}{N}\sum_{i=1}^{n} x_{ji}, \ (6)}$$

όπου N είναι ο συνολικός αριθμός των τσιπ, και j είναι το αναγνωριστικό κυψέλης. Για να είναι επαρκή τα αποτελέσματα, πρέπει να μετρηθεί ένας επαρκής αριθμός τσιπ.

4.3.3 Ταχύτητα

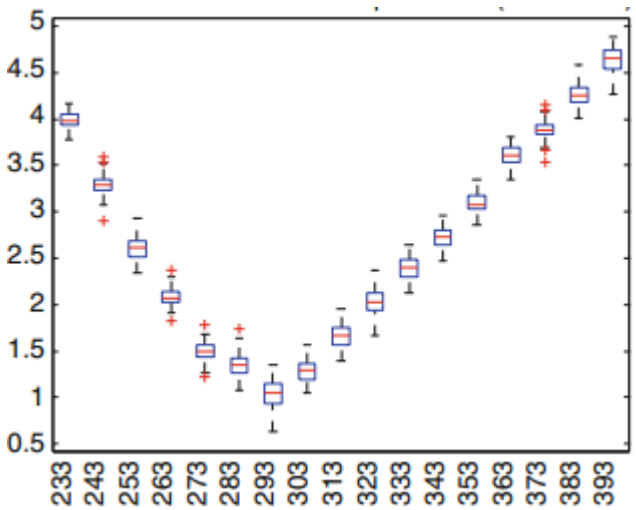
Ένα άλλο κριτήριο αξιολόγησης των PUF είναι η ταχύτητα. Η ταχύτητα μπορεί να αποτελεί ανησυχία σε ορισμένα κυκλώματα. Εάν η κατανάλωση ρεύματος παίζει κάποιο ρόλο σε αυτό, ορισμένα κυκλώματα μπορεί να υπερβούν κάποιους χρονικούς περιορισμούς πριν από την παροχή της εξόδου. Η μονάδα μέτρησης της ταχύτητας είναι $\frac{bit}{sec}$. Ο τρόπος προσδιορισμού της ταχύτητας ανάγνωσης εξαρτάται από τα κελιά που διαβάζονται παράλληλα ή σειριακά. Στην περίπτωση του παραδειγματικού τσιπ δοκιμής, η συχνότητα ανάγνωσης είναι 1 MHz. Δεδομένου ότι τα κελιά διαβάζονται σειριακά, η ανάγνωση των 4.096 κυψελών παίρνει t= $\frac{4096}{1MHZ}$=4096μs. Οπότε η ταχύτητα είναι 10E6$\frac{bits}{sec}$.

4.3.4 Ποσοστά Σφάλματος από Αλλαγές Θερμοκρασίας

Εξετάζοντας το σχήμα 6 μπορεί να παρατηρηθεί μια σχεδόν γραμμική σχέση μεταξύ της θερμοκρασίας και των σφαλμάτων. Εάν υποτεθεί μια γραμμική σχέση, προκαλείται ο ρυθμός σφάλματος (e_{temp}) που οφείλεται σε μετατοπίσεις θερμοκρασίας και μπορεί να εκφραστεί ως εξής:

$$\mathbf{e_{temp}} = \frac{E_T - E_N}{\Delta T}, \quad \mathbf{(7)}$$

όπου E_T είναι το ποσοστό σφαλμάτων στην θερμοκρασία T, και E_N είναι το ποσοστό σφαλμάτων στην ιδανική θερμοκρασία και ΔT = T-N. Η μονάδα μέτρησης είναι [$\frac{\%}{c}$]

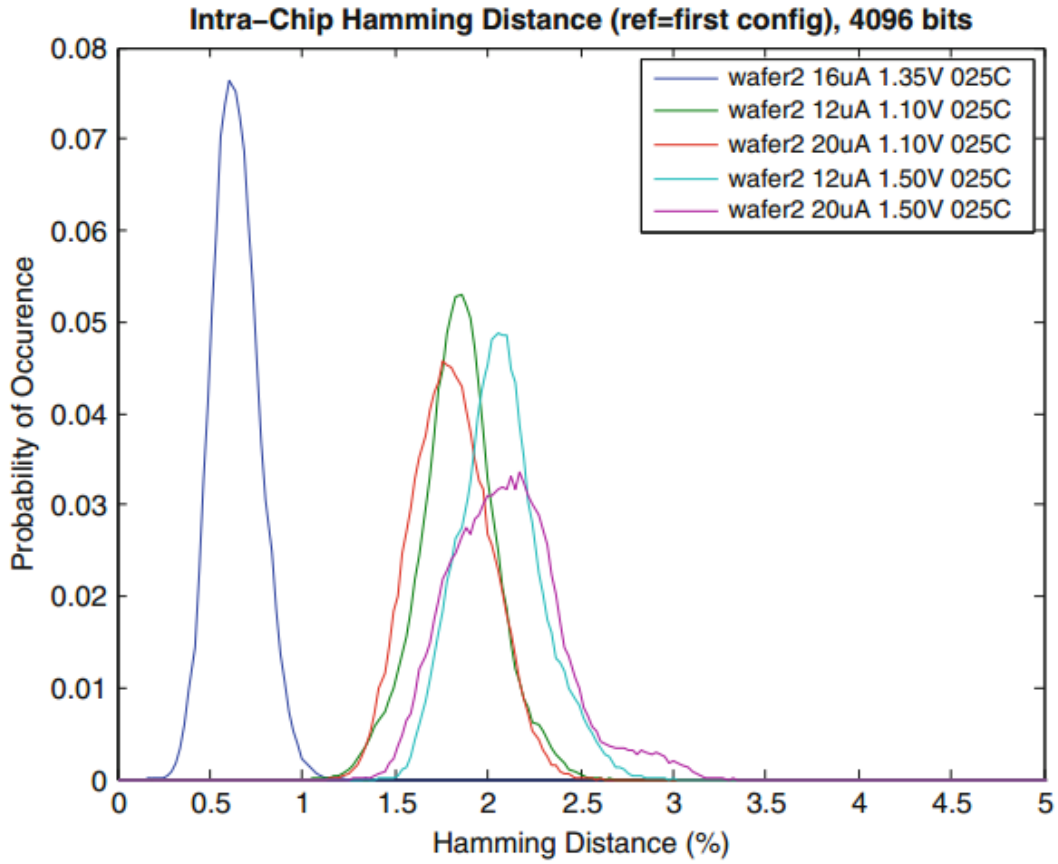


Σχήμα 6. Ποσοστό λαθών σε διαφορετικές θερμοκρασίες [10]
Άξονας y: Ποσοστό λαθών, Άξονας x: Θερμοκρασία σε K

4.3.5 Ρυθμός Σφαλμάτων από Παραλλαγές Ρεύματος και Τάσης

Η έξοδος των PUFs εκτός από την επιρροή της θερμοκρασίας, μπορεί επίσης να εξαρτάται από τις μεταβολές της τάσης τροφοδοσίας ή του ρεύματος εισόδου.[10] Η επίδραση αυτών των παραμέτρων, αν υπάρχουν, εξαρτάται έντονα από το κύκλωμα PUF. Στην περίπτωση του υποδειγματικού PUF, αλλαγές στις δύο παραμέτρους επηρεάζουν την έξοδο του PUF. Το αποτέλεσμα μπορεί να φανεί στο Σχήμα 7: το ρεύμα ποικίλει μεταξύ 12 και 20 μA, η τάση ρυθμίστηκε στα 1,1 V και 1,5 V. Η αναφορά καθορίστηκε σε I_{BIAS} = 16 μA και 1.35 V.

Το Σχήμα 7 δείχνει ότι οι μεταβολές στην τάση τροφοδοσίας και τα ρεύματα εισόδου έχουν σημαντικές επιπτώσεις στην έξοδο. Το ποσοστό σφάλματος αυξάνεται κατά περίπου 2%.



Σχήμα 7. Επιρροή διαφορετικών ρευμάτων και τάσεων [10]

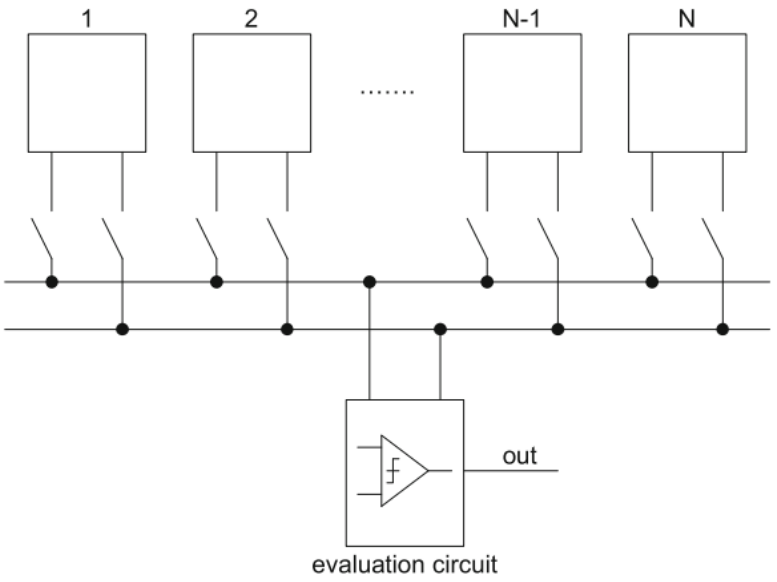
Όσον αφορά τα κυκλώματα PUF είναι ιδιαίτερα σημαντικό οι αλλαγές στη λειτουργία να είναι όσο το δυνατόν μικρότερες. Για να σταθεροποιηθεί η έξοδος, τα PUF θα πρέπει να λειτουργούν κάτω από τις ίδιες συνθήκες.

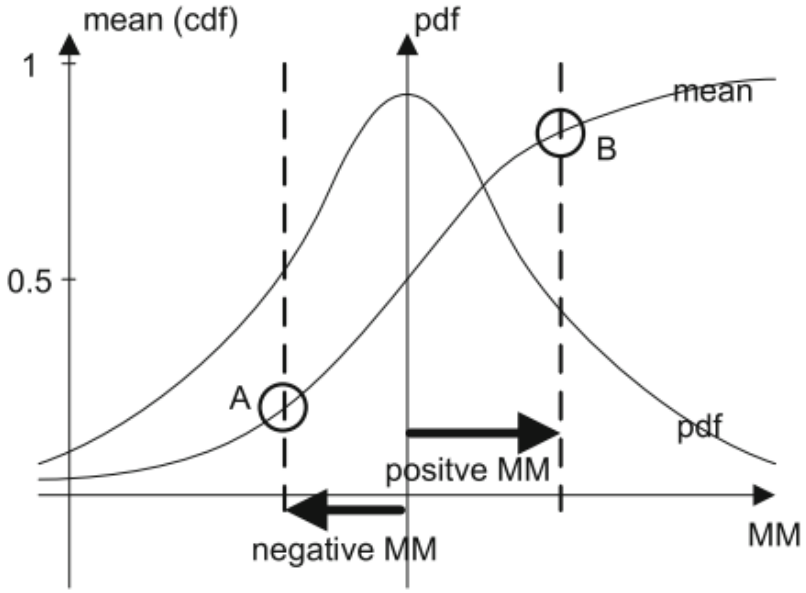
4.3.6 Συσχέτιση μεταξύ των δυαδικών ψηφίων: Ανάλυση μπλοκ

Σε μερικά σχήματα PUF, όπου δημιουργούνται ειδικές δομές στη διάταξη κυψελών ή κοινόχρηστων εξαρτημάτων, απαιτείται περαιτέρω ανάλυση των συσχετισμών. Για παράδειγμα, ένα PUF που περιλαμβάνει ένα κοινόχρηστο αισθητήρα απεικονίζεται στο σχήμα 8. Εμφανίζει N PUF κελιά που μοιράζονται ένα κύκλωμα αισθητήρων. Σε μια τέτοια περίπτωση, μια αναντιστοιχία στην κοινόχρηστη μονάδα επηρεάζει την έξοδο όλων των κυψελών. Αυτό το φαινόμενο μπορεί να φανεί στο Σχήμα 9. Η επίδραση μιας αρνητικής αναντιστοιχίας (MM) και η επίδραση μιας

θετικής αναντιστοιχίας παρουσιάζεται σε αυτό. Στην ιδανική περίπτωση η μέση απόδοση ισούται με 0,5. Εάν εισάγεται αρνητικό ΜΜ (A), η μέση απόδοση είναι μειωμένη. Εάν εισάγεται θετική αναντιστοιχία (B), η μέση παραγωγή αυξάνεται. Επομένως, στην έξοδο υπάρχουν περισσότερα μηδενικά. Στην πράξη, μια προκατάληψη στην έξοδο είναι ασφαλής, καθώς ο αριθμός πιθανών συνδυασμών μειώνεται.

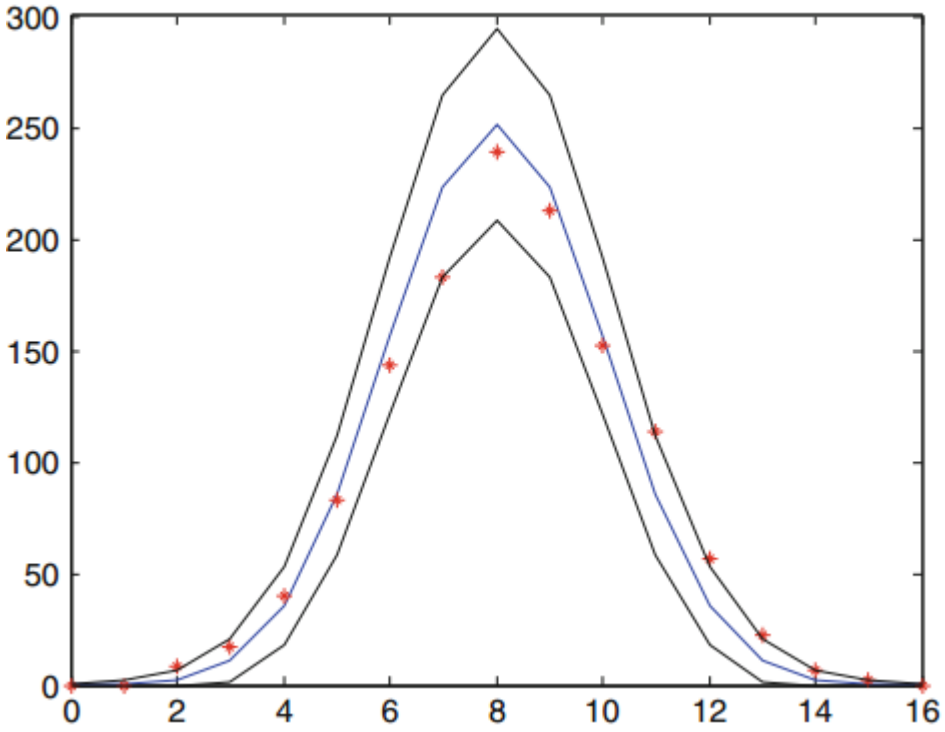
Σχήμα 7. Κυψέλες με κοινό κύκλωμα αισθητήρα [10]





Σχήμα 8. Αντίκτυπος της προκατάληψης στη μέση τιμή εξόδου [10]
Το cdf τοποθετείται στην κορυφή του PUF

Η ακόλουθη έννοια μέτρησης μπορεί να χρησιμοποιηθεί για την εύρεση προκαθορισμένων αποτελεσμάτων σε διαφοροποιήσεις τάσης σε διάφορα μέρη του κυκλώματος: Εάν τα N κελιά είναι συνδεδεμένα σε ένα ενισχυτή αισθητήρα, ολόκληρη η έξοδος είναι επίσης ομαδοποιημένη σε μπλοκ του N. Στη συνέχεια, προσδιορίζεται ο μέσος όρος κάθε μπλοκ. Δεδομένου ότι υπάρχει διωνυμική κατανομή για τις μέσες τιμές τέτοιων μπλοκ, τα αποτελέσματα μπορούν να τοποθετηθούν στην κορυφή αυτής της διανομής. Ένα παράδειγμα φαίνεται στο σχήμα 9. Το άνω και το κάτω μέρος των καμπυλών απεικονίζει το CI του 3σ (99,7%). Η επίδραση των προκαταλήψεων μπορεί να φανεί καθαρά. Κοντά ο μέσος όρος των τιμών τείνει να βρίσκεται κάτω από την αναμενόμενη τιμή. Σε αντάλλαγμα, για τις τιμές σε στις εξωτερικές περιοχές, οι μετρούμενες τιμές τείνουν να υπερβαίνουν τις τιμές προσδοκίας.



y: Συχνότητα, x: Αριθμός από «1»

Σχήμα 9. Κατανομή μέσης τιμής μπλοκ από 16 κελιά [10]

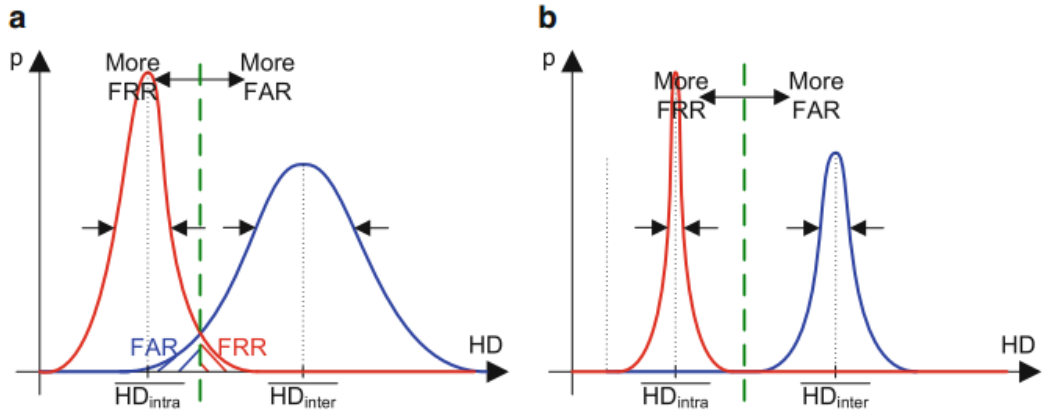
Για να έχουμε αριθμητικά αποτελέσματα, είναι λογικό να υπολογίσουμε κατά προσέγγιση την διωνυμική κατανομή με κανονική κατανομή. Ως εκ τούτου, η

αναμενόμενη τυπική απόκλιση σ_{ideal} και η πραγματική απόκλιση σ_{real} μπορούν να υπολογιστούν. Στο παράδειγμα (N = 16) οι δύο τιμές είναι σ_{ideal}= 2 και σ_{real} = 2.488 (εκτίμηση μέγιστης πιθανότητας).

4.3.7 FAR και FRR

Το αποδεκτό ποσοστό λαθών (false acceptance rate, στο εξής FAR) και το μη αποδεκτό ποσοστό λαθών (false rejection rate, στο εξής FRR) συμβάλλουν στην αναγνώριση της απόδοσης ενός συστήματος.[19][20] Όταν χρησιμοποιούνται PUFs, ο ρυθμός σφαλμάτων των τσιπ και ο αριθμός των bits εξόδου ορίζουν αυτή την απόδοση. Αυτό σημαίνει ότι τα FAR και FRR ορίζουν επίσης τη συνολική απόδοση του PUF.

Παράδειγμα: τα αναγνωριστικά των τσιπ αποθηκεύονται σε μια βάση δεδομένων σε ένα διακομιστή. Κατά τη διάρκεια της φάσης ταυτοποίησης, ένα τσιπ στέλνει το αναγνωριστικό του στο διακομιστή. Αν η απόσταση Hamming για μια καταχώρηση στη βάση δεδομένων είναι κάτω από μια προκαθορισμένη τιμή, εκχωρείται το αναγνωριστικό που έχει ληφθεί σε αυτήν την καταχώρηση από το διακομιστή. Μπορούν να συμβούν σφάλματα είτε αν το τσιπ δεν έχει εκχωρηθεί στο αναγνωριστικό (ψευδής απόρριψη) ή αν έχει ταυτοποιηθεί ένα άγνωστο τσιπ (ψευδής αποδοχή). Διαφορετικά μέτρα ορίζονται στη βιβλιογραφία: στο [19] αναλύεται το ποσοστό λανθασμένου συναγερμού και χρησιμοποιείται το ποσοστό ψευδούς ανίχνευσης (FDR). Στο [20] αναλύονται το ψεύτικο ποσοστό αποδοχής και το ποσοστό ψευδούς απόρριψης (FRR) που χρησιμοποιούνται ως κοινά μέτρα στη βιομετρία. Επομένως, προτιμώνται οι FAR και FRR για τον υπολογισμό. Στο σχήμα 10 Εμφανίζονται οι δύο παράμετροι.



Σχήμα 10. FAR και FRR: (a) Μικρός αριθμός κελιών PUF (b) Μεγάλος αριθμός κελιών PUF [10]

Η πράσινη τεθλασμένη γραμμή απεικονίζει τον μέγιστο αριθμό εσφαλμένων δυαδικών ψηφίων (HD_{MAX}) η οποία εξακολουθεί να επιτρέπεται να δεχτεί το ληφθέν αναγνωριστικό. Αν το HD_{MAX} είναι μεγάλο, το FRR είναι χαμηλό αλλά ο αριθμός των ψεύτικων αποδοχών είναι υψηλός. Εάν το FAR είναι υψηλό, η αλλαγή για την αποδοχή οποιουδήποτε αναγνωριστικού (π.χ., που αποστέλλεται από έναν εισβολέα) γίνεται υψηλότερη. Και αντίστροφα: αν επιλέγεται το HD_{MAX} μικρά, ψεύτικα αναγνωριστικά μπορεί να μην γίνονται αποδεκτά αλλά αυξάνεται και ο αριθμός των απορρίψεων.

Τα δύο μέτρα ορίζονται μαθηματικά ως εξής:

False Acceptance Rate:

$$\mathbf{FAR} = \frac{NFA}{NAA} * 100\%, \quad \mathbf{(8)}$$

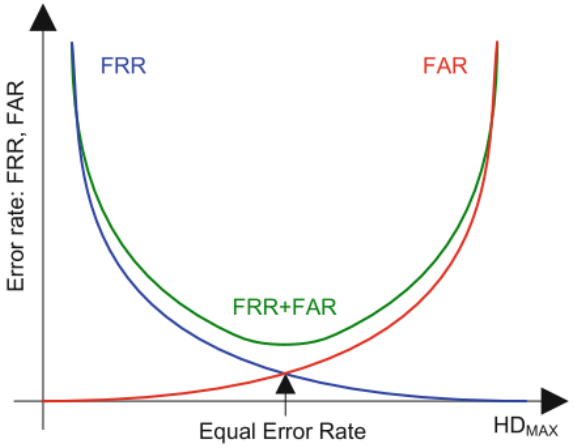
όπου NFA είναι ο αριθμός των αποδεκτών αποτυχημένων προσπαθειών και NAA είναι ο αριθμός των προσπάθειες ενός επιτιθέμενου.

False Rejection Rate:

$$\mathbf{FRR} = \frac{NFR}{NIA} * 100\% \ , \mathbf{(9)}$$

όπου NFR είναι ο αριθμός των ψευδών απορρίψεων και η NIA είναι ο αριθμός των αποπειρών ταυτοποίησης.

Η σχέση μεταξύ FRR και FAR φαίνεται παρακάτω σχήμα. Μια ισορροπία μεταξύ FRR και FAR πρέπει να βρεθεί ανάλογα με την εφαρμογή.



Σχήμα 11. Σχέση μεταξύ FAR και FRR [10]

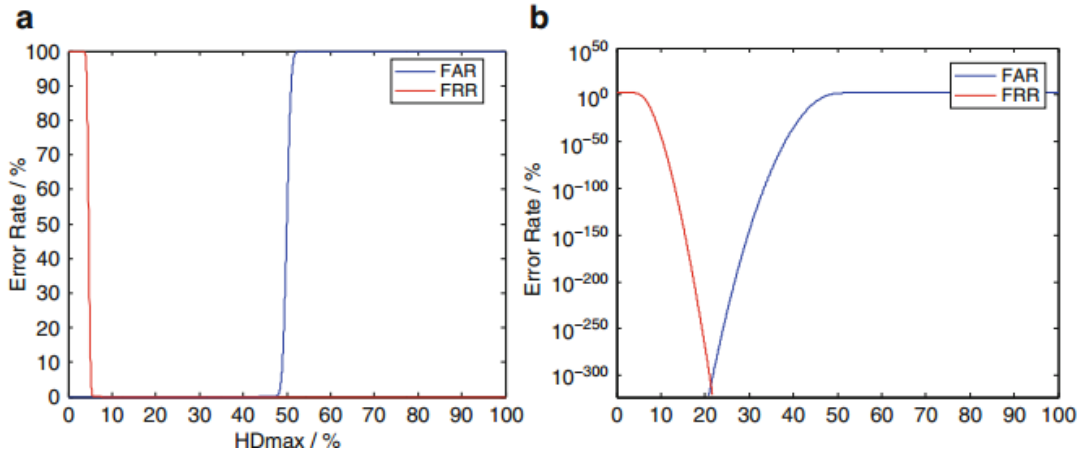
Είναι δυνατό να προσδιοριστεί στατιστικά το FRR και το FAR. Εάν οι διανομές στο Σχήμα 12 θεωρείται ότι είναι Gaussian, μπορεί να προκύψει η ακόλουθη παράμετρος: $HD_{intra} = \mu_{intra}$, σ_{intra}, $HD_{inter} = \mu_{inter}$, σ_{inter} και HD_{MAX}.

Το FRR μπορεί να εκφραστεί ως εξής:

$$\mathbf{FRR} = \frac{1}{\sigma\sqrt{2\pi}} \int_{HD_{MAX}}^{\infty} e^{-\frac{1}{2}\left(\frac{x-\mu_{intra}}{s_{intra}}\right)} \mathbf{dx * 100\% , (10)}$$

Το FAR μπορεί να εκφραστεί ως εξής:

$$\mathbf{FAR} = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{HD_{MAX}} e^{-\frac{1}{2}\left(\frac{x-\mu_{intra}}{s_{intra}}\right)} \mathbf{dx * 100\% , (11)}$$



Σχήμα 12. FAR και FRR ανάλογα με το HDMAX (a) Γραμμική κλίμακα. (b) Λογαριθμική κλίμακα [10]

Στην περίπτωση του υποδειγματικού τσιπ δοκιμής μ_{intra} = 4.6392%, σ_{intra} = 13.46, μ_{inter} = 50% και σ_{inter} = 32. Τα αποτελέσματα για FRR και FAR σε σχέση με το το HD_{MAX} απεικονίζονται στο σχήμα 12. Η γραμμική κλίμακα του σχήματος 12 a δεν είναι κατάλληλη. Θα πρέπει να προτιμάται μια λογαριθμική κλίμακα (Σχήμα 12b).

Για HDMAX = 10% FRR γίνεται περίπου ≈ 10E-40. Το FAR είναι μικρότερο από 10E-500.

4.3.8 Σύνοψη

Για να συνοψίσουμε αυτήν την ενότητα, οι μετρήσεις προκύπτουν από το υποδειγματικό τσιπ δοκιμής και παρουσιάζονται στον Πίνακα 2. Η μέση τιμή x, ο συσχετισμός μεταξύ των δυαδικών ψηφίων (R_{xx}), και η συσχέτιση μεταξύ των τσιπ (HD_{inter}) αποδεικνύονται πολύ καλά. Όλα αυτά τα μέτρα μέτρησης είναι εντός των στατιστικών επιθυμητών περιοχών. Η απόσταση Hamming μεταξύ των τσιπ (HD_{intra}) παραμένει επίσης μικρή, όσο η θερμοκρασία δεν αλλάζει. Ως εκ τούτου, η απόδοση του θορύβου είναι επίσης ικανοποιητική. Η εξάρτηση από την θερμοκρασία αποδεικνύει ότι αποτελεί μεγαλύτερο ζήτημα. Ένα ποσοστό σφάλματος 5% είναι πολύ υψηλό για λογικούς κώδικες διόρθωσης σφαλμάτων. Έτσι, στις μελλοντικές εφαρμογές πρέπει να δοθεί έμφαση στο πρόβλημα αυτό. Όπως ήδη αναφέρθηκε παραπάνω, η κατανάλωση ενέργειας είναι επίσης πολύ υψηλή, αλλά δεν έχουν πρώτιστη σημασία.

Property	Identifier	Test Chip
Mean value	$\bar{x}$	0.5046
Error rate	$HD_{intra120°C}$	4.6392 %
Corr. between bits	R_{xx}	≈ 0
Corr. between chips	HD_{inter}	50.0271 %
Power consumption	$\frac{E}{bit}$	391.5 $\frac{pJ}{bit}$

Πίνακας 2. Σύνοψη αποτελεσμάτων υποδειγματικών τσιπ [10]

5. Βασικές Αρχές

Το PUF με βάση το πυρίτιο προτάθηκε για πρώτη φορά από τους Gassend et al. [21] ως φυσική τυχαία λειτουργία το 2002. Περίπου την ίδια εποχή έγινε η εισαγωγή του οπτικού PUF από τον Pappu et al. [22] στο πλαίσιο της έννοιας της φυσικής μονόδρομης λειτουργίας. Ο όρος PUF στις μέρες μας χρησιμοποιείται συνήθως για να περιγράψει μια ποικιλία από τοπολογίες κυκλωμάτων που αναπτύσσονται για την εξαγωγή των παραμετρικών αναντιστοιχιών από τις παραλλαγές της διαδικασίας κατασκευής των συσκευών πυριτίου για τη συσκευή πιστοποίησης ταυτότητας και δημιουργία μυστικού κλειδιού [23]. Ένα φυσικό PUF μπορεί να οριστεί τυπικά ως ένα φυσικό σύστημα που χαρτογραφεί πιθανοτικά μια διεγερτική πρόκληση c που επιλέγεται από ένα πεπερασμένο σύνολο C = {0, 1} k σε απόκριση εξόδου r σε πεπερασμένο χώρο R = {0, 1} l σύμφωνα με τις ενδογενείς στοχαστικές του ιδιότητες k που προκαλείται από τη διαδικασία κατασκευής της συσκευής ως εξής:

$$\mathbf{PUF_k : C \rightarrow R \ (10)}$$

Η λειτουργία της δημιουργίας μιας απόκρισης r € R που δίνεται στην πρόκληση c € C μπορεί επίσης να εκφραστεί μαθηματικά ως:

$$\mathbf{r \leftarrow PUF_{ak}(c) \ (11)}$$

Παρόλο που δεν υπάρχει γενική συμφωνία για την κοινή ασφάλεια με συγκεκριμένες ιδιότητες για την πιστοποίηση PUFs, τα ακόλουθα επιθυμητά χαρακτηριστικά θεωρούνται ευρέως αποδεκτά από την ακαδημαϊκή κοινότητα στο σχεδιασμό των PUF.

Αξιόπιστο (Reliability): Ένα PUF είναι αξιόπιστο αν η απάντησή του στην ίδια πρόκληση μπορεί να αναπαραχθεί με την πάροδο του χρόνου και σε ένα ευρύ φάσμα συνθηκών λειτουργίας.

Απρόβλεπτο (Unpredictability): Η απάντηση σε μια αυθαίρετη πρόκληση που παράγεται από ένα PUF δεν μπορεί να προβλεφθεί από τα ζεύγη Challenge - Response (CRPs) άλλων στιγμιότυπων PUF ή με την χρήση CRP της ίδιας μορφής PUF.

Αδυναμία κλωνοποίησης (Unclonability): Η αντιστοίχιση CRP ενός PUF είναι μοναδική και δεν μπορεί να κλωνοποιηθεί φυσικά ή μαθηματικά. Αυτό ισχύει ακόμη και για τον αρχικό κατασκευαστή του PUF.

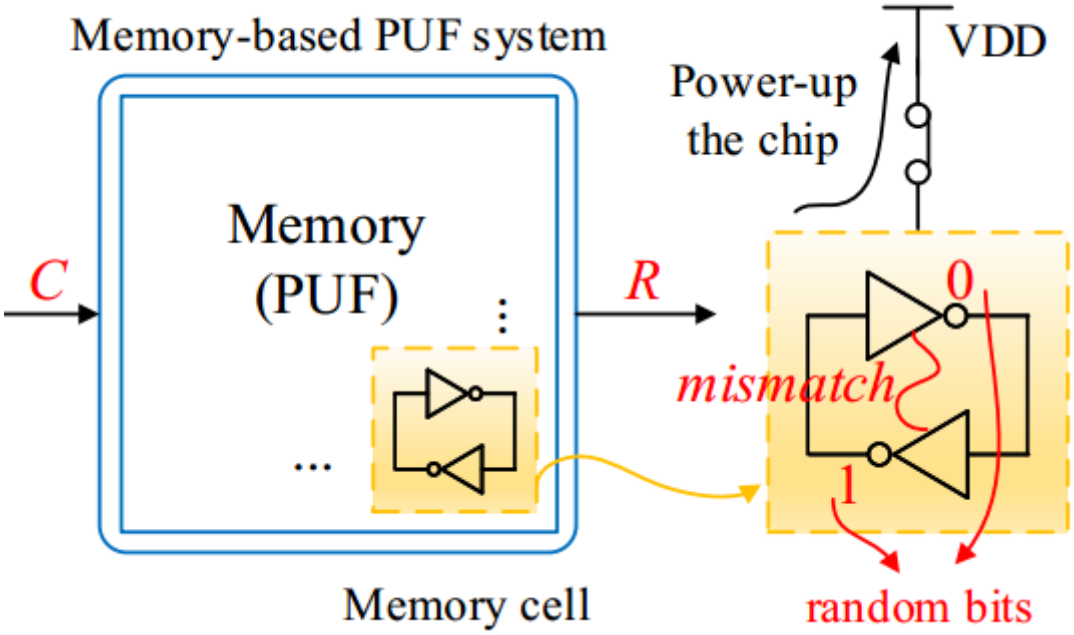
Φυσική Ανθεκτικότητα (Physical Unbreakability): Ένα PUF είναι φανερά κατασκευασμένο με τέτοιο ώστε οποιαδήποτε σωματική προσπάθεια να τροποποιηθεί κακόβουλα θα έχει ως αποτέλεσμα δυσλειτουργία ή μόνιμη ζημιά στο τσιπ.

Παραδείγματα αδύναμων PUF αποτελούν τα περισσότερα PUF με βάση τη μνήμη (memory – based) και τα puff με επικάλυψη PUF (coating Puff) [24]. Φυσιολογικά το PUF που βασίζεται στη μνήμη εκμεταλλεύεται τις μετασταθείσες καταστάσεις των αντιστροφέων με σταυροειδείς δεσμούς οι οποίοι δημιουργούν τυχαία δυαδικά ψηφία κατά την επαναφορά [25]. Όπως φαίνεται στο Σχήμα 13, το δυαδικό ψηφίο απόκρισης καθορίζεται από το ποια από τις δύο μετατροπείς όμοιου μεγέθους σε μια κυψέλη μνήμης στην οποία απευθύνεται το bit πρόκλησης φτάνει στο σημείο εκκίνησης πιο γρήγορα. Παραλλαγές PUFs με βάση την μνήμη έχουν αναπτυχθεί τα τελευταία χρόνια, όπως σύρτης (latch) PUF, πεταλούδα (butterfly) PUF, SRAM PUF, D flipflop PUF και bus keeper PUF. Η δομή κυψέλης του κάθε τύπου μπορεί να είναι μοναδική αλλά η παραγόμενη τυχαία απόκριση bit εξακολουθεί να διαβάζεται ξεχωριστά από κάθε κελί της συστοιχίας όταν αντιμετωπίζεται η πρόκληση. Η μνήμη PUF είναι εύκολη στον σχεδιασμό, έχει χαμηλή επιφάνεια και δεν υπάρχουν αμοιβαία συσχετισμένα bits απόκρισης. Όντας ασθενές PUF, ο χώρος CRP του μπορεί να διερευνηθεί πλήρως με ασήμαντη προσπάθεια [26], γεγονός που θέτει σε κίνδυνο την ασφάλειά του. Αυτό έχει ως αποτέλεσμα να χρησιμοποιείται μόνο σαν λύση αυθεντικοποίησης χαμηλού κόστους.

Ένα ισχυρό PUF, από την άλλη πλευρά, χαρακτηρίζεται από ένα τεράστιο αριθμό CRP, ο οποίος αναπτύσσεται εκθετικά ανάλογα με τον αριθμό των

συμμετρικών blocks που χρησιμοποιούνται για τη δημιουργία του PUF. Αυτή η ιδιότητα καθιστά πρακτικά ανέφικτο να υπολογιστούν εξαντλητικά όλες οι προκλήσεις σε ρεαλιστικό χρόνο. Λόγω της φυσικά κρυμμένης δομής και των σύνθετων συνδυασμών των αναντιστοιχιών των συνιστωσών, η πιθανότητα σωστής πρόβλεψης της απάντησης σε μια τυχαία επιλεγμένη άγνωστη πρόκληση είναι πολύ χαμηλή, ακόμη και με τη γνώση πολλών άλλων CRP.

Τα χαρακτηριστικά των ασθενών και δυνατών PUF θα τα δούμε εκτενέστερα στην επόμενη παράγραφο.



Σχήμα 12. Μηχανισμός δημιουργίας δυαδικών ψηφίων δομής και απόκρισης Memory-based PUF [57]

Ένα PUF λέγεται ότι είναι ανθεκτικό εάν τα CRP του παρουσιάζουν καλή τυχαιότητα, μοναδικότητα και αξιοπιστία. Οι περισσότερες τεχνικές που αναφέρονται στη βιβλιογραφία βελτιώνουν την ανθεκτικότητα του PUF έναντι μεταβολών στη θερμοκρασία και την τάση. Το φαινόμενο της γήρανσης είναι ένα θέμα το οποίο έχει σε μεγάλο βαθμό παραμεληθεί. Η γήρανση επιδεινώνεται από φαινόμενα όπως είναι η αστάθεια θερμοκρασίας αρνητικής απόκλισης (NBTI), hot-carrier injection (HCI), η εξαρτώμενη από τη θερμοκρασία διηλεκτρική διάσπαση (TDDB) και η ηλεκτρομεταφορά. Διαφορετική από τη χρονική επιρροή που προκαλείται από

διακυμάνσεις της θερμοκρασίας ή της τάσης, η γήρανση προκαλεί μη αναστρέψιμη επιδείνωση της απόδοσης του κυκλώματος με την πάροδο του χρόνου.

Η γήρανση και η πρόκληση της αλλαγής της απόδοσης του PUF έχει μελετηθεί όλο και περισσότερο τα τελευταία χρόνια. Από τη στιγμή που η γήρανση στο πεδίο απαιτεί πολύ χρόνο για να δημιουργήσει αισθητά αποτελέσματα, η ταχεία γήρανση χρησιμοποιείται ως αποτελεσματική μέθοδος εκτίμησης των επιπτώσεων. Βομβαρδίζοντας την συσκευή με υπερβολικά υψηλή θερμοκρασία, τάση κ.λπ., μπορεί να προχωρήσει η κανονική διαδικασία γήρανσης γρηγορότερα. Διαπιστώθηκε ότι η γήρανση υποβαθμίζει κατά κύριο λόγο την αξιοπιστία του PUF, αλλά έχει αμελητέο αντίκτυπο στην τυχαιότητα [27].

Έχουν προταθεί διάφορα αντίμετρα για την άμβλυνση της γήρανσης όπως το ζεύγος ταλαντωτή δακτυλίων (RO) με μεγαλύτερη διαφορά συχνότητας, παράλληλη κλίση / ρυθμός γήρανσης στο RO PUF [27][28] και απενεργοποίηση του κυκλώματος PUF όταν δεν χρησιμοποιείται [29], [30]. Από την άλλη πλευρά, η σκόπιμη γήρανση μπορεί επίσης να χρησιμοποιηθεί επωφελώς για την ενίσχυση της απόδοσης PUF. Στο [31], η γήρανση μπορεί είτε να αντιστρέψει είτε να αυξήσει την τάση διαφοράς κατωφλίου των δύο τρανζίστορ PMOS πυρήνα σε ένα στοιχείο SRAM για επίτευξη μεγαλύτερης ομοιομορφίας ή αξιοπιστίας για το SRAM PUF. Παρόμοια ιδέα καταδείχθηκε επίσης στο [32].

5.1 Αδύναμα Εναντίον Δυνατών PUF

Προτάθηκαν πολλές νέες και διαφορετικές υλοποιήσεις των PUFs, ώστε να αξιοποιηθεί η εντροπία κατά την διαδικασία κατασκευή τους. Γίνεται όλο και πιο δύσκολο να κατηγοριοποιηθούν οι διαφορετικοί τύποι PUF με βάση αναλογικές παραμέτρους (π.χ. καθυστέρηση, ισχύς, τάση, ρεύμα κ.λπ.) ή τις τοπολογίες κυκλωμάτων τους (π.χ. παρατήρησης, μνήμη, ταλαντωτής δακτυλίου (RO) κ.λπ.). Καθώς το μέγεθος του χώρου CRP έχει άμεση συνέπεια σχετικά με τις εφαρμογές και το μοντέλο απειλής τους, τα υπάρχοντα PUFs είναι συχνά διχοτομημένα σε αδύναμα PUF και ισχυρά PUF [33], [34].

Χαρακτηριστικά αδύναμων PUFs

- Τα αδύναμα PUFs έχουν περιορισμένα CRPs. Πιο συγκεκριμένα, ο αριθμός των CRPs αυξάνεται γραμμικά ή πολυωνυμικά ανάλογα με τον αριθμό των βασικών κυψελών ή μπλοκ συμμετρικών συνιστωσών που καταλήγουν να σχηματίσουν το PUF, και στη χειρότερη περίπτωση, υπάρχει μόνο μία CRP για ένα ολόκληρο PUF [35].
- Οι CRPs ενός ασθενούς PUF με πεπερασμένο φυσικό μέγεθος μπορούν να μετρηθούν εξαντλητικά μέσα σε πολυωνυμικό χρόνο.
- Η περιφερειακή διασύνδεση ενός ασθενούς PUF πρέπει να προστατεύεται με την ενσωμάτωσή του σε έναν ασαφή εκχυλιστή (Fuzzy Extractor (FE)) για να περιορίζεται η άμεση πρόσβαση στην αρχική απόκριση που παράγεται εσωτερικά από το φυσικό PUF.

Χαρακτηριστικά δυνατών PUFs

- Τεράστιος αριθμός CRP. Αυτός ο αριθμός αυξάνεται εκθετικά με τον αριθμό συμμετρικών στοιχείων που χρησιμοποιούνται για τη δημιουργία του PUF.
- Η φυσική συγκεχυμένη δομή και οι σύνθετοι συνδυασμοί των αναντιστοιχιών των συστατικών, καθιστούν την πιθανότητα σωστής πρόβλεψης της απόκρισης σε μια τυχαία επιλεγμένη άγνωστη πρόκληση πολύ χαμηλή ακόμη και με τη γνώση πολλών άλλων CRPs.
- Δεν χρειάζεται να ενσωματώνει μια δομή μετα-επεξεργασίας για να αποφευχθεί η εξωτερική πρόσβαση στα αρχικά δημιουργούμενα ψηφία απόκρισης.

Παραδείγματα ασθενών PUF

- PUF που βασίζονται στην μνήμη (Memory-based PUFs)
- PUF με επικάλυψη χρώματος (Coating PUFs)

Η χρήση αδύναμων PUF είναι ανεπαρκής για τον έλεγχο ταυτότητας, εκτός εάν χρησιμοποιείται μαζί με μια συνάρτηση κατακερματισμού και την χρήση ενός μυστικού κλειδιού.

Παραδείγματα δυνατών PUF

- Οπτικό PUF (Optical PUF)
- PUF που βασίζονται σε παρατήρηση (Arbiter – based PUF)

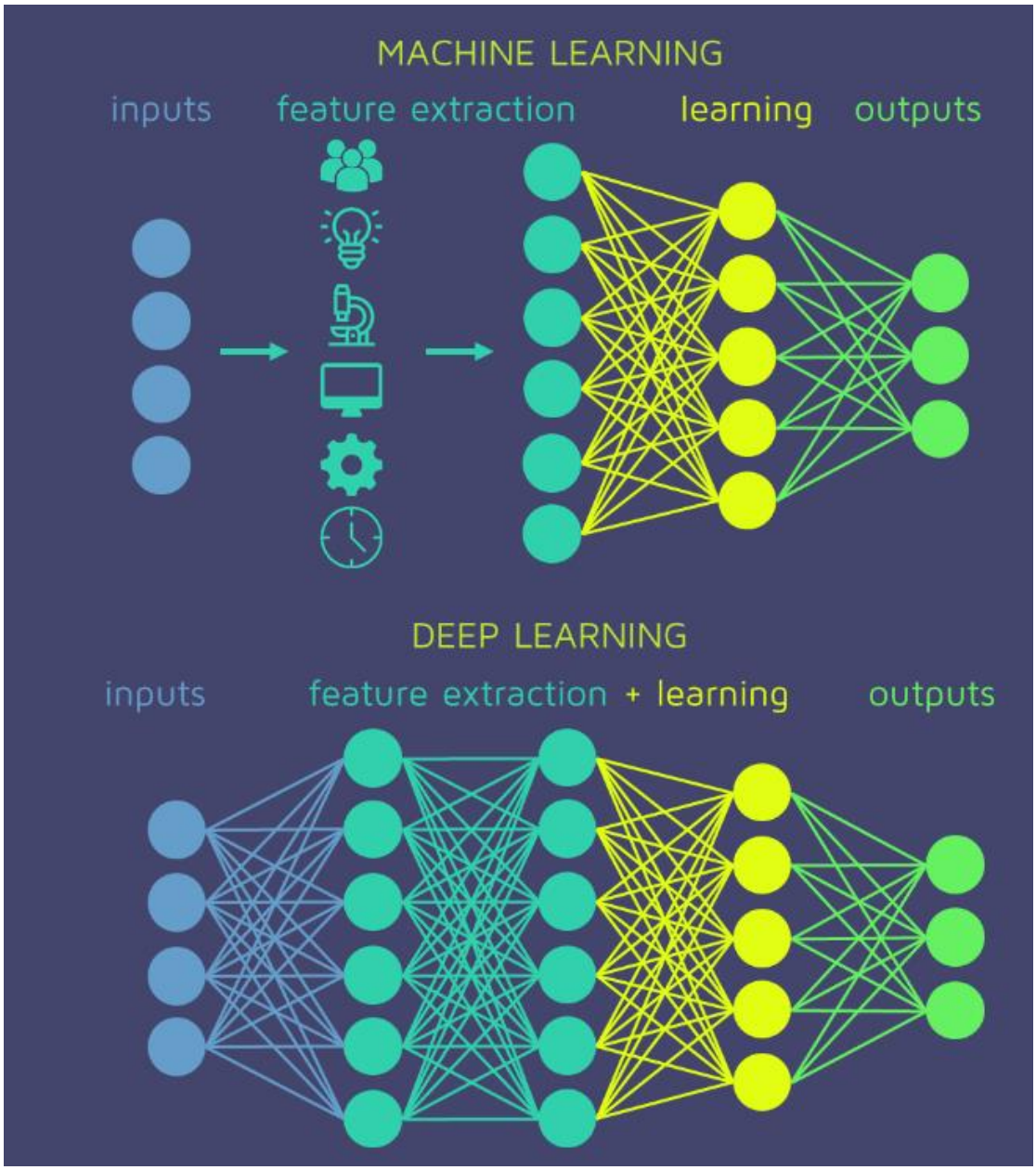
5.2. Μηχανισμοί επίθεσης σε PUFs

Το PUF έχει εξαλείψει με επιτυχία την ανάγκη της παρουσίας μυστικού κλειδιού στη NVM του τσιπ, με αποτέλεσμα την μείωση του κινδύνου των επιθέσεων backdoor, όπως γίνεται σε κρυπτοσυστήματα με "ασφαλές κλειδί". Δεδομένου ότι η συσκευή πρέπει να είναι ενεργοποιημένη για να απαντήσει στην πρόκληση πριν από την μέτρηση της απόκρισης, τα PUF είναι εγγενώς απαραβίαστα. Οποιαδήποτε επεμβατική επίθεση ή φυσική επαφή θα ανατρέψει την απόκριση σε και την παραγωγή CRP και θα καταστήσει το PUF ακατάλληλο. Ωστόσο, πολλά PUFs δεν χρησιμοποιούνται αυτόνομα. Ένας επιτιθέμενος, ενώ μπορεί να είναι δύσκολο να στοχεύσει το PUF άμεσα, μπορεί να επιτεθεί με διαρροή με χρήση πλευρικών διαύλων μέσω εξαρτημάτων που είναι κατασκευασμένα γύρω από τη διεπαφή σήματος εισόδου / εξόδου. Πολλά πρόσφατα πειράματα και ερευνητικά έργα έχουν δείξει ότι ορισμένες ισχυρές δομές PUF μπορεί επίσης να μοντελοποιούνται μαθηματικά και να είναι ευάλωτα σε επιθέσεις που βασίζονται σε ML (Machine Learning) αλγορίθμους. Οι επιθέσεις αυτές εξετάζονται σε αυτή την ενότητα.

5.3 Επιθέσεις μοντελοποίησης Αλγόριθμων Μηχανικής Μάθησης

Αυτό το είδος επιθέσεων απευθύνεται σε ισχυρά PUF με μεγάλο αριθμό CRP [36]. Οι επιθέσεις μοντελοποίησης συνήθως υλοποιούνται εξάγοντας ένα μοντέλο αριθμητικής προσομοίωσης του PUF. Ένας αλγόριθμος ML χρησιμοποιείται στη συνέχεια για να προβλέψει τις αποκρίσεις εξόδου του PUF σε άγνωστες προκλήσεις με την κατάρτιση του μαθητευόμενου μηχανήματος με ένα υποσύνολο γνωστών CRP. Αυτά τα CRPs μπορούν είτε να συλλεχθούν από την άμεση πρόσβαση

στο PUF ή από την υποκλοπή του κατά την παρακολούθηση του πρωτοκόλλου challenge – response.



Σχήμα 13. Παράδειγμα εκπαίδευσης αλγορίθμου μηχανικής μάθησης [37]

Ως αντιστάθμισμα κατά των επιθέσεων ML, μπορεί να προστεθεί μη γραμμικό αποτέλεσμα. Για παράδειγμα, περνώντας από XORing τις απαντήσεις με χρήση πολλαπλών PUFs παρατήρησης. Διεξήχθη μελέτη [38] ως πρότυπο επίθεσης, XOR, LW και παρατήρησης PUF από διαφορετικούς αλγόριθμους ML που εκπαιδεύονται

χρησιμοποιώντας προσομοιωμένο θόρυβο, δωρεάν υποσύνολο CRP, καθώς και πραγματικά δεδομένα πυριτίου(silicon) από τους δύο πρώτους τύπους PUF. Βρέθηκε ότι ενώ τα ισχυρά PUF είναι γενικά ανασφαλή έναντι των προχωρημένων επιθέσεων ML, η πολυπλοκότητα των επιθέσεων μπορεί εύκολα να αυξηθεί αυξάνοντας τον αριθμό των σταδίων, τον αριθμό των αλυσίδων PUF παρατήρησης ή προσθέτοντας νέα μη γραμμικά στοιχεία. Για παράδειγμα, για το ML η αντίσταση αυξάνεται πολυωνυμικά με τον αριθμό των σταδίων (ή ισοδύναμα, μήκος bits πρόκλησης) αλλά εκθετικά με τον αριθμό των αλυσίδων παρατηρητών PUFs XOR και LW παρατηρητών. Η αποτελεσματικότητα του αλγόριθμου επιθέσεων επί του τελευταίου είναι χαμηλή. Ένας παρατηρητής XOR 512 βαθμίδων PUF με 8 αλυσίδες παρατηρητών βρέθηκε να επιτυγχάνει μια καλή ισορροπία μεταξύ του αριθμού των θορυβωδών απαντήσεων και της πριμοδότησης πυριτίου για την αποτελεσματική παρεμπόδιση από ML επιθέσεις μοντελοποίησης [38].

Μια άλλη ευρέως σχεδιασμένη προσέγγιση για την αντιμετώπιση των επιθέσεων ML είναι η απόκρυψη των άμεσων απαντήσεων και η μετάδοση είτε των βοηθητικών δεδομένων ή υποσέλιδων \ padded υποσέλιδων της απάντησης μέσω του πρωτόκολλου ελέγχου ταυτότητας, όπως υποδεικνύεται από το PUF (RFEP) [39] και το λεπτό PUF (SLPUF) πρωτόκολλο [40]. Ωστόσο, η υπόθεση ότι οι επιθέσεις ML μπορούν να διεξαχθούν με επιτυχία μόνο με τη γνώση των αρχικών CRPs είναι φανταστική. Ο Becker [41] κατέδειξε ότι η στρατηγική εξέλιξης (ES) που βασίζεται στην ML τεχνική είναι σε θέση να αποκομίσει ένα ακριβές μοντέλο PUF από αναξιόπιστες πληροφορίες οι οποίες διέρρευσαν από τα βοηθητικά δεδομένα και τις συναφείς προκλήσεις από την γεννήτρια προκλήσεων LFSR για να σπάσει με επιτυχία τα RFEP και SLPUF πρωτόκολλα.

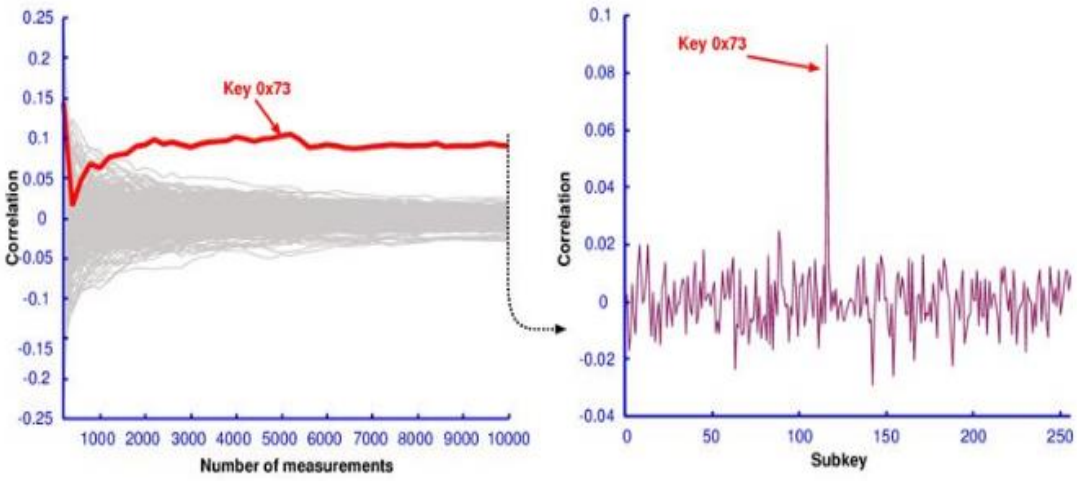
5.4 Επιθέσεις πλευρικών καναλιών (Side-Channel)

Οι Side-Channel attacks αναφέρονται σε μια ομάδα τεχνικών επίθεσης που εκμεταλλεύονται τις μετρήσιμες παραμέτρους της φυσικής εφαρμογής (σε αντίθεση με τις brute force επιθέσεις ή τις θεωρητικές αδυναμίες) ενός κρυπτογραφικού αλγορίθμου ή πρωτοκόλλου για την εξαγωγή του μυστικού κλειδιού. Οι πληροφορίες από τα πλευρικά κανάλια μπορεί να είναι διασπορά ισχύος,

χρονισμού, θερμοκρασίας, ηλεκτρομαγνητικών εκπομπών, εκπομπών οπτικών σημάτων, ακουστικών σημάτων ή οποιουδήποτε συνδυασμού αυτών [42]. Οι προσπάθειες για διατήρηση της αρχέγονης ασφάλειας του υλικού ως μαύρο κουτί για να αντισταθούν στην κρυπτανάλυση έχουν αποδειχθεί αναποτελεσματικές καθώς μερικές επιθέσεις πλευρικού καναλιού μπορούν να πετύχουν ακόμη και χωρίς να γνωρίζουν το κύκλωμα και τις εσωτερικές λειτουργίες του.

Side-Channel Attacks

- Εξοικονόμηση ενέργειας
- Συγχρονισμός
- Θερμοκρασία
- Ηλεκτρομαγνητικές εκπομπές
- Οπτικές εκπομπές σήματος
- Ακουστικά σήματα
- Συνδυασμός των παραπάνω



Σχήμα 14. Παράδειγμα Side-Channel Attack [43]

Χωρίς χρήση τεχνικών ML, ένα PUF παρατήρησης μπορεί επίσης να μοντελοποιηθεί χρησιμοποιώντας απλώς επαναληψιμότητα μέτρησης[44]. Η βασική ιδέα είναι να εκμεταλλευτεί το αποτέλεσμα των μη αναπαραγώγιμων χρονικών θορύβων σε

αναπαραγώγιμες μετρήσεις δομικών στοιχείων μεταβλητότητας για τον χαρακτηρισμό της αναλογικής μεταβλητότητας χρονισμού που είναι υπεύθυνη για τη δημιουργία δυαδικών ψηφίων.

5.5 Συνδυασμός επιθέσεων ML και Side-Channel

Οι επιθέσεις των πλευρικών καναλιών μπορούν επίσης να αυξήσουν την αποτελεσματικότητα των αλγορίθμων ML όταν γίνεται υπολογιστικά μη πρακτικό να μοντελοποιηθούν πιο εξελιγμένες ενισχυμένες ισχυρές δομές PUF [45]. Μια υβριδική επίθεση [46] που συνδυάζει το πλευρικό κανάλι ισχύος με ML δοκιμάστηκε με επιτυχία εναντίον του PUF παρατήρησης XOR και LW PUF σε περισσότερα από 64 στάδια με έως και εννέα παράλληλες αλυσίδες παρατηρητών. Αν και τα αποτελέσματα των μεμονωμένων παρατηρητών παραμένουν ανεξήγητα, οι πληροφορίες πλευρικών καναλιών είναι χρήσιμες για την ανίχνευση αυτών των "καλών" CRP όταν οι έξοδοι όλων των παρατηρητών είναι «0» ή «1». Με αυτόν τον τρόπο ο κάθε παρατηρητής PUF μπορεί μοντελοποιηθεί ξεχωριστά αποκαλύπτοντας αυτά τα "καλά" CRPs. Υποθέτοντας ότι οι έξοδοι των παράλληλων παρατηρητών k κατανέμονται εξίσου, η πιθανότητα εμφάνισης "καλών" CRPs είναι 2^{1-k}. Αν το k είναι μικρό στην πράξη, η επίθεση είναι πολύ αποτελεσματική και εξαιρετικά βιώσιμη.

6. Διάφορα Είδη PUF

Καθώς προχωράει η τεχνολογία και στην προσπάθεια να γίνουν πιο ανθεκτικά τα PUF στις επιθέσεις έχουν προταθεί διάφορα μοντέλα PUF. Σε αυτή την ενότητα θα δούμε ενδεικτικά κάποια μοντέλα PUF.

6.1 FinFET PUF

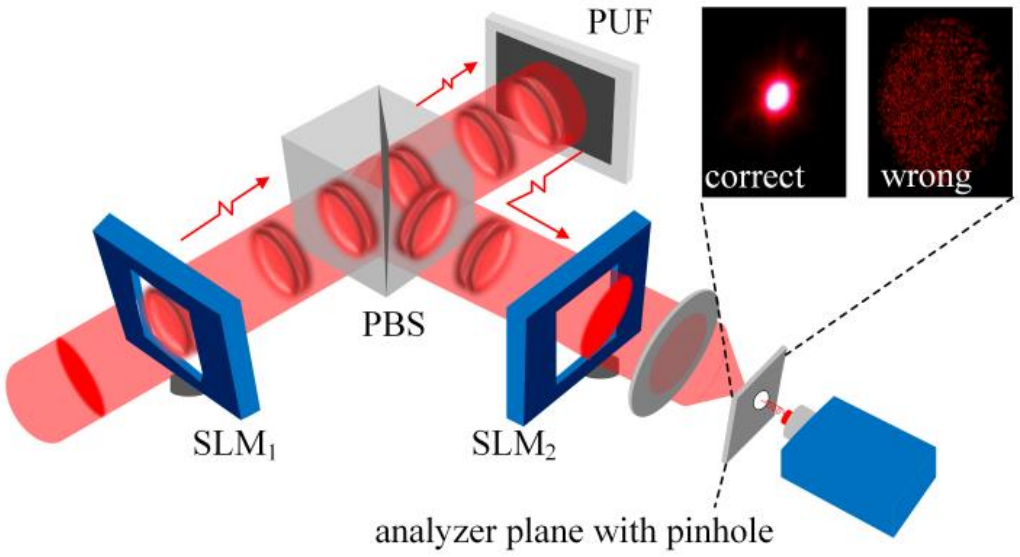
Το τρανζίστορ πεδίου-αποτελέσματος (FinFET), το οποίο εισήχθη το 1999 [47], βασίζεται στην τεχνολογία CMOS με βελτίωση της κλασσικής δομής του CMOS. Η 3D δομή του διευρύνει την περιοχή επαφής μεταξύ των πυλών και του καναλιού για την καταστολή του SCE χωρίς τη χρήση μεγάλης ενίσχυσης διαύλου / σώματος [48]. Τα αντικρουόμενα κριτήρια μεγέθους των τρανζίστορ με τη σταθερότητα ανάγνωσης-εγγραφής του SRAM μετριάζονται από την ασύμμετρη πύλη FinFET, καθιστώντας το έτσι σαν έναν ιδανικό υποψήφιο για την εφαρμογή ισχυρής υψηλής πυκνότητας SRAM [49].

Τεχνικές για τη βελτίωση της αξιοπιστίας του κλασικού CMOS PUF που βασίζεται σε SRAM έχει προταθεί στο [31]. Ελέγχοντας τον λόγο διαστάσεων της διαμόρφωσης των κελιών και της ισχυρότερης πόλωσης της πίσω πόρτας, πιστεύεται ότι το FinFET έχει μεγαλύτερη δυνατότητα από τα συμβατικά CMOS για βελτιστοποίηση της απόδοσης των PUF και της λειτουργίας της μνήμης τους. Δυστυχώς, αυτή η σκέψη αμφισβητείται από επιθέσεις μειωμένης καθυστέρησης που μπορούν να αξιοποιήσουν τις αναντιστοιχίες μεγέθους των συσκευών FinFET.

6.2 Quantum-secure PUF

Τα περισσότερα PUF υποστηρίζουν μόνο ένα πεπερασμένο, αν και ενδεχομένως εκθετικό αριθμό CRP. Τα ισχυρά PUFs δεν αποτελούν εξαίρεση. Δεδομένου ότι χρειάζεται να αφιερωθεί αρκετός χρόνος, όποιος έχει πρόσβαση στο PUF μπορεί να εξαγάγει αρκετά CRPs για να συμπεράνει σωστά με μεγάλη πιθανότητα την ανταπόκριση σε οποιαδήποτε μελλοντική πρόκληση χωρίς να χρειάζεται να κατέχει το PUF. Για να αποφύγει την παραβίαση του PUF, ο απομακρυσμένος έλεγχος ταυτότητας (χειροκίνητος εκ των προτέρων) μπορεί να πραγματοποιηθεί με την χρήση μιας βάσης δεδομένων ερώτησης-απάντησης (challenge-response), αλλά αυτό αυξάνει τον κίνδυνο εξαπάτησης. Αντί να επενδύσουν σε ακριβούς αξιόπιστους αναγνώστες ή επιπλέον αισθητήρες κατά της πλαστογράφησης, το πρόβλημα της πλαστογράφησης στο σενάριο μεταβίβασης μπορεί να εξαλειφθεί με ασφάλεια με τη βοήθεια της quantum-readout [50]. Οι προκλήσεις και οι απαντήσεις ενός quantum-readout PUF (QR-PUF) εξασφαλίζονται από κβαντικές καταστάσεις. Η κβαντική κατάσταση είναι μια κατάσταση που μπορεί να αποτυπωθεί μαθηματικά από μια ακτίνα (ή ένα διάνυσμα) στο χώρο Hilbert. Κωδικοποιεί το εύρος πιθανότητας εύρεσης ενός ηλεκτρονίου σε μια συγκεκριμένη τροχιακή κατάσταση (π.χ. θέση, ορμή, περιστροφή κ.λπ.). Σε ένα οπτικό QR-PUF [50], η φυσική πρόκληση είναι η κβαντική κατάσταση που καθορίζεται από μερικές φάσεις κύματος φωτονίων. Μέσω ενιαίας εξέλιξης, το PUF παράγει μια απάντηση, η οποία είναι επίσης μια κβαντική κατάσταση της ίδιας συνεκτικής μορφής με την πρόκληση, αλλά με ένα μεγαλύτερο εύρος πάνω από τα οποία απλώνονται τα φωτόνια. Αυτό συμβαίνει επειδή λόγω της διάχυσης η περιοχή από την οποία το φως εξέρχεται είναι μεγαλύτερη από το φωτεινό σημείο. Σύμφωνα με το μη κλωνοποιητικό θεώρημα [51], μια αυθαίρετη κβαντική κατάσταση είναι αδύνατο να κλωνοποιηθεί. Οποιαδήποτε παρακολούθηση των CRP θα αλλάξει την κατάσταση και θα εντοπιστεί εύκολα από το σύστημα. Δεδομένου ότι η κατάσταση μιας άγνωστης κβαντικής πρόκλησης δεν μπορεί να προσδιοριστεί πλήρως, ο εισβολέας

δεν μπορεί να τρέξει αξιόπιστα το πρόγραμμα εξομοίωσης για την κατασκευή της αναμενόμενης απόκρισης.



Σχήμα 15. Quantum-secure οπτική ανάγνωση ενός φυσικού κλειδιού [57]

6.3 Sensor PUF

Οι αισθητήρες παίζουν βασικό ρόλο στη συλλογή δεδομένων από το περιβάλλον. Δεδομένου ότι τα συλλεχθέντα δεδομένα χρησιμοποιούνται συχνά για ανάλυση και λήψη αποφάσεων, ένας αισθητήρας είναι ικανός να καταστρέψει μια μεγάλη δικτυακή υποδομή, εάν έχει πειραχτεί ώστε να εισάγει ψευδή δεδομένα. Μια κοινή προσέγγιση για τη διασφάλιση ενός κόμβου αισθητήρα είναι η ενσωμάτωση ενός εξωτερικού PUF στο σύστημα ανίχνευσης, όπως δίδεται παραδειγματικά από την εξακρίβωση της γνησιότητας των έξυπνων μετρητών σε ένα σύστημα έξυπνου δικτύου. Σε αυτές τις εφαρμογές, η έξοδος αισθητήρα μπορεί είτε να χρησιμοποιηθεί για τη δημιουργία προκλήσεων PUF [52] ή να κρυπτογραφηθούν από τις απαντήσεις PUF [53]. Μια γενική αρχιτεκτονική Sensor PUF για την αλληλεπίδραση συμβατικών αποκρίσεων PUF πυριτίου με τα δεδομένα αισθητήρα προτείνεται στο [53], το οποίο αποδεικνύεται από μια σειρά φωτοδιόδων. Ένα πλεονέκτημα αυτής της

προτεινόμενης λύσης είναι ότι το σύνολο CRP του PUF μπορεί να ρυθμιστεί εκ νέου. Αυτό είναι ιδιαίτερα χρήσιμο όταν η αρχική αντιστοίχιση CRP εκτίθεται ή τα CRP μπορούν να ανανεώνονται περιοδικά για αποτροπή επιθέσεων μοντελοποίησης. Η αναγνώριση αισθητήρα από μόνη της μπορεί να μην παρέχει επαρκή αξιοπιστία μιας εφαρμογής ανίχνευσης, εκτός εάν η ακεραιότητα, η αυθεντικοποίηση και η χρονική σήμανση είναι στενά συνδεδεμένες.

ΣΥΜΠΕΡΑΣΜΑ

Τα PUFs σαν τεχνολογία δείχνουν ότι είναι ικανά να παράσχουν επαρκή ασφάλεια ειδικά σε θέματα αυθεντικοποίησης. Παρόλα αυτά δείχνει να μην έχουν ευρεία χρήση και προτιμώνται άλλες υλοποιήσεις. Αυτό δείχνει να οφείλεται στο κόστος υλοποίησης ασφαλών συστημάτων PUF και στον θόρυβο που υπάρχει στην έξοδο των PUF. Επίσης κάτι το οποίο είναι πιθανό να μην τα καθιστά τόσο δημοφιλή είναι ότι τα συστήματα δεν είναι ευέλικτα. Για παράδειγμα, όταν ανακαλυφθεί ένα κενό ασφάλειας, δεν μπορεί το PUF να πάρει κάποιο security update, αλλά θα πρέπει να δημιουργηθεί νέα υλοποίηση.

Το quantum-secure PUF δείχνει ότι μπορεί να λύσει πολλά από τα προβλήματα των PUF και να αποτελέσει ένα νέο πολλά υποσχόμενο πεδίο για έρευνα και ανάπτυξη. Σε αυτό μπορεί να βοηθήσει η ραγδαία ανάπτυξη του IOT και η ανάγκη για αυθεντικοποίηση συσκευών. Το αν θα γίνει αυτό θα φανεί στο κοντινό μέλλον.

ΠΗΓΕΣ

[1]https://el.wikipedia.org/wiki/%CE%86%CE%BB%CE%B1%CE%BD_%CE%A4%CE%BF%CF%8D%CF%81%CE%B9%CE%BD%CE%B3%CE%BA

[2] https://www.geeksforgeeks.org/what-are-hash-functions-and-how-to-choose-a-good-hash-function/

[3] Pappu, R., Recht, B., Taylor, J., Gershenfeld, N.: Physical one-way functions. Science 297, 2026–2030 (2002)

[4] threatpost.com/crypto-legend-ron-rivest-working-replacement-broken-ssl-system-092811/75696/

[5] Gassend B, Lim D, Clarke D, Dijk MV, Devadas S (2004) Identification and authentication of integrated circuits. Concurr Comput Pract Exper 16:1077–1098. DOI 10.1002/cpe.805, URL: http://www.cse.msstate.edu/~ramkumar/fulltext.pdf

[6] Roel Maes IV Pim Tuyls (2008) Statistical analysis of silicon puf responses for device identification. Katholieke Universiteit Leuven: ESAT-COSIC

[7] Hofer M, Boehm C (2010) Identifikation, authentifizierung und schluesselgenerierung mittels physical unclonable functions. In: Informationstagung Mikroelektronik ME2010, pp 267–272

[8] https://www.tutorialspoint.com/what-is-hamming-distance

[9] Simpson W (1996) Ppp challenge handshake authentication protocol (chap)

[10] Christoph Bohm • Maximilian Hofer: Physical Unclonable Functions in Theory and Practice

[11] James B. Wendt, Miodrag Potkonjak (2014) : Hardware obfuscation using PUF-based logic

[12] Florian Kohnhäuser, André Schaller, Stefan Katzenbeisser (2015): PUF-Based Software Protection for Low-End Embedded Devices

[13] Skoric B, Tuyls P, Ophey W (2005) Robust key extraction from physical uncloneable functions 3531:407–422. In: 3rd international conference on applied cryptography and network security, New York, 07–10 June 2005

[14] Bohm and Hofer, Austrochip, pp 86–90, 2011; Cabbibo et al. Proceedings ITC 2004 international test conference, pp 655– 660, 2004; Helinski et al. 47th ACM/IEEE design automation conference (DAC), pp 240–243, 2010)

[15] Abhranil Maiti, Jeff Casarona, Luke McHale, Patrick Schaumont (2010) A large scale characterization of RO-PUF

[16] Su Y, Holleman J, Otis B (2008) A digital 1.6 pj/bit chip identification circuit using process variations. IEEE J Solid-State Circ 43(1):69–77. DOI 10.1109/JSSC.2007.910961

[17] Chang L, Fried D, Hergenrother J, Sleight J, Dennard R, Montoye R, Sekaric L, McNab S, Topol A, Adams C, Guarini K, Haensch W (2005) Stable sram cell design for the 32 nm node and beyond. In: Symposium on VLSI Technology, 2005. Digest of Technical Papers, pp 128–129, 2005. DOI 10.1109/.2005.1469239,

[18] Su Y, Holleman J, Otis B (2008) A digital 1.6 pj/bit chip identification circuit using process variations. IEEE J Solid-State Circ 43(1):69–77. DOI 10.1109/JSSC.2007.910961

[19] Lim D, Lee J, Gassend B, Suh G, van Dijk M, Devadas S (2005) Extracting secret keys from integrated circuits. IEEE Trans Very Large Scale Integr (VLSI) Syst 13(10):1200–1205. DOI 10.1109/TVLSI.2005.859470

[20] Maes R, Verbauwhede I (2010) Physically unclonable functions: A study on the state of the art and future research directions. In: Basin D, Maurer U, Sadeghi AR, Naccache D (eds) Towards hardware-intrinsic security, information security and cryptography. Springer, Berlin, pp 3–37, 2010,

[21] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, “Silicon physical random functions,” in Proc. 9th ACM conf. Computer and Commun. security, Washington, USA, 2002, pp. 148–160.

[22] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, “Physical one-way functions,” Science, vol. 297, no. 5589, pp. 2026–2030, Sept. 2002.

[23] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in Proc. 44th ACM/IEEE Design Automation Conf. (DAC), San Diego, USA, Jun. 2007, pp. 9– 14.

[24] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, “Emerging physical unclonable functions with nanotechnology,” IEEE Access, vol. 4, pp. 61–80, Feb. 2016.

[25] L. Zhang, Z. H. Kong, C. H. Chang, A. Cabrini, and G. Torelli, “Exploiting process variations and programming sensitivity of phase change memory for reconfigurable physical unclonable functions, ”IEEE Trans. Inform. Forensics and Security, vol. 9, no. 6, pp. 921– 932, Apr. 2014.

[26] U. Ruhrmair ¨ et al., “Modeling attacks on physical unclonable functions,” in Proc. 17th ACM conf. Computer and commun. security, Chicago, Illinois, USA, Oct. 2010, pp. 237–249.

[27] A. Maiti and P. Schaumont, “The impact of aging on a physical unclonable function,” IEEE Trans. Very Large Scale Integration (VLSI) Syst., vol. 22, no. 9, pp. 1854–1864, Sept. 2014.

[28] M. T. Rahman, D. Forte, F. Rahman, and M. Tehranipoor, “A pair selection algorithm for robust ro-puf against environmental variations and aging,” in Computer Design (ICCD), 2015 33rd IEEE International Conference on. IEEE, 2015, pp. 415–418.

[29] S. R. Sahoo, K. Sudeendra Kumar, K. Mahapatra, and A. Swain, “A novel aging tolerant RO-PUF for low power application,” Dec. 2016.

[30] M. T. Rahman, F. Rahman, D. Forte, and M. Tehranipoor, “An agingresistant RO-PUF for reliable key generation,” IEEE Trans. Emerging Topics in Computing, vol. 4, no. 3, pp. 335–348, Sept. 2016.

[31] A. Garg and T. T. Kim, “Design of SRAM PUF with improved uniformity and reliability utilizing device aging effect,” in Proc. 2014 IEEE Int. Symp.Circuits and Systems (ISCAS). Melbourne, Australia: IEEE, Jun. 2014, pp. 1941–1944

[32] T. Xu and M. Potkonjak, “Stable and secure delay-based physical unclonable functions using device aging,” in Proc. 2015 IEEE Int. Symp. Circuits and Systems (ISCAS). Lisbon, Portugal: IEEE, May 2015, pp. 33–36.

[33] U. Ruhrmair and D. E. Holcomb, “PUFs at a glance,” in ¨ Proc. Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, Mar. 2014, pp. 1–6.

[34] U. Ruhrmair ¨ et al., “Modeling attacks on physical unclonable functions,” in Proc. 17th ACM conf. Computer and commun. security, Chicago, Illinois, USA, Oct. 2010, pp. 237–249.

[35] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, “Physical one-way functions,” Science, vol. 297, no. 5589, pp. 2026–2030, Sept. 2002.

[36] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, “Physical unclonable functions and applications: A tutorial,” Proc. IEEE, vol. 102, no. 8, pp. 1126–1141, May 2014.

[37]https://www.google.com/url?sa=i&source=images&cd=&ved=2ahUKEwiQuaDk7ejmAhWODuwKHU7BrMQjRx6BAgBEAQ&url=https%3A%2F%2Fquantdare.com%2Fwhat-is-the-difference-between-deep-learning-and-machine learning%2F&psig=AOvVaw3AK091mARHghd_Rtg9KMTE&ust=1578189916134989

[38] U. Ruhrmair ¨ et al., “PUF modeling attacks on simulated and silicon data,” IEEE Trans. Inform. Forensics and Security, vol. 8, no. 11, pp. 1876–1891, Aug. 2013.

[39] A. Van Herrewege and otheres, “Reverse fuzzy extractors: Enabling lightweight mutual authentication for PUF-enabled RFIDs,” in Proc.Int. Conf. Financial Cryptography and Data Security, Kralendijk, Bonaire, Feb. 2012, pp. 374–389.

[40] M. Majzoobi, M. Rostami, F. Koushanfar, D. S. Wallach, and S. Devadas, “Slender PUF protocol: A lightweight, robust, and secure authentication by substring matching,” in Proc. IEEE Symp. Security and Privacy Workshop (SPW), San Francisco, USA, May 2012, pp. 33–44.

[41] G. T. Becker, “On the pitfalls of using arbiter-PUFs as building blocks,” IEEE Trans. Computer-Aided Design of Integrated Circuits and Syst., vol. 34, no. 8, pp. 1295–1307, Apr. 2015.

[42] B. Kopf and D. Basin, “An information-theoretic model for adaptive ¨ side-channel attacks,” in Proc. 14th ACM conf. Computer and commun. security, Alexandria, USA, Oct. 2007, pp. 286–296

[43] https://slideplayer.com/slide/5848699/

[44] J. Delvaux and I. Verbauwhede, “Side channel modeling attacks on 65nm arbiter PUFs exploiting CMOS device noise,” in Proc. IEEE Int. Symp. Hardware-Oriented Security and Trust (HOST), Austin, USA, Jun. 2013, pp. 137–142

[45] X. Xu and W. Burleson, “Hybrid side-channel/machine-learning attacks on PUFs: a new threat?” in Proc. conf. Design, Automation & Test in Europe (DATE), Dresden, Germany, Mar. 2014, p. 349

[46] A. Mahmoud, U. Ruhrmair, M. Majzoobi, and F. Koushanfar, “Combined modeling and side channel attacks on strong PUFs.” IACR Cryptology ePrint Archive, vol. 2013, p. 632, 2013.

[47] X. Huang, W.-C. Lee, C. Kuo, D. Hisamoto, L. Chang, J. Kedzierski, E. Anderson, H. Takeuchi, Y.-K. Choi, K. Asano et al., “Sub 50-nmfinfet: PMOS,” in Proc. Electron Devices Meeting (IEDM), Tech. Dig. Int., Washington, USA, Dec. 1999, pp. 67–70.

[48] T. Matsukawa, S. O’uchi, K. Endo, Y. Ishikawa, H. Yamauchi, Y. Liu, J. Tsukada, K. Sakamoto, and M. Masahara, “Comprehensive analysis of variability sources of FinFET characteristics,” in Proc. Symp. VLSI Technology, Honolulu, USA, Jun. 2009, pp. 118–119.

[49] S. M. Salahuddin and V. Kursun, “Asymmetrical FinFET SRAM cells with wider read noise margin and lower leakage currents,” in Proc. TENCON 2015-2015 IEEE Region 10 Conf., Macao, China, Nov. 2015, pp. 1–3.

[50] B. Skori ˇ c, A. P. Mosk, and P. W. Pinkse, “Security of quantum-readout ´ PUFs against quadrature-based challenge-estimation attacks,” Int. J. Quantum Inform., vol. 11, no. 04, p. 1350041, Jun. 2013.

[51] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,”Nature, vol. 299, no. 5886, pp. 802–803, Oct. 1982

[52] M. Potkonjak, S. Meguerdichian, and J. L. Wong, “Trusted sensors andremote sensing,” in Proc. Sensors, IEEE (ICSENS), Kona, USA, Nov. 2010, pp. 1104–1107.

[53] K. Rosenfeld, E. Gavas, and R. Karri, “Sensor physical unclonable functions,” in Proc. IEEE Int. Symp. Hardware-Oriented Security and Trust (HOST), Anaheim, USA, Jun. 2010, pp. 112–117.

[54]https://www.google.com/url?sa=i&source=images&cd=&ved=2ahUKEwib5Y31nafnAhXO66QKHcwmBWQQjRx6BAgBEAQ&url=https%3A%2F%2Fppt-online.org%2F45849&psig=AOvVaw3ztm2eNbgCJ_1MYG5cbpgy&ust=1580333154512719

[55] https://upload.wikimedia.org/wikipedia/commons/2/2b/Caesar3.svg

[56]https://1.bp.blogspot.com/VZZIHRKqtqo/UfIivjb6SZI/AAAAAAAATc8/uXi5t0aA3Y8/s1600/turing_enigma_2.jpg

[57] Chip-Hong Chang, Yue Zheng, Le Zhang, “A Retrospective and a Look Forward: Fifteen Years of Physical Unclonable Function Advancement” , Article in IEEE Circuits and Systems Magazine · August 2017