ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Νευρομορφική μηχανική και εφαρμογές στην οπτική κρυπτογραφία (Photonic PUFs)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΚΑΝΔΥΛΙΩΤΗ ΝΙΚΟΛΑΟΥ

Επιβλέπων καθηγητής:

ΜΕΣΑΡΙΤΑΚΗΣ ΧΑΡΗΣ

Σάμος , Σεπτέμβριος 2023

Ευχαριστίες

Η παρούσα εργασία πραγματοποιήθηκε στο Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων της Πολυτεχνικής Σχολής του Πανεπιστημίου Αιγαίου.

Στην αρχή ,η υλοποίηση αυτής καθώς και ο όγκος πληροφορίας που είχα μπροστά μου με έκαναν να περιμένω να είναι μια ψυχοφθόρα και επίπονη διαδικασία . Με τη βοήθεια όμως του καθηγητή μου κ.Χάρη Μεσαριτάκη κατέληξε να είναι μια πολύ ενδιαφέρουσα μελέτη που μου άνοιξε τους ορίζοντες στο επίπεδο της γνώσης . Πραγματικά δεν είχα φανταστεί ποτέ πόσο ρόλο μπορεί να παίζουν ακόμη και τα πιο μικρά πράγματα στην επιστήμη.

Θα ήθελα πρωτίστως να ευχαριστήσω την οικογένεια μου που μου παρείχε ότι χρειαζόμουν κατά τη διάρκεια αυτού του ταξιδιού που λέγεται Πανεπιστήμιο .

Ακόμα, θα ήθελα να ευχαριστήσω τους συμφοιτητές μου , που μετά από λίγο καιρό απέκτησαν και την ιδιότητα των καλών φίλων για όλη τη στήριξη τους σε μαθησιακό αλλά κυρίως σε ψυχολογικό επίπεδο .

Τέλος , θα ήθελα να ευχαριστήσω τον καθηγητή μου και Αν. Καθηγητή του Πανεπιστημίου Αιγαίου κ. Χάρη Μεσαριτάκη για την υποστήριξη του αλλά κυρίως , για την υπομονή του .

Σας ευχαριστώ θερμά.

Κατάλογος Περιεχομένων

ΠΕΡΙΛΗΨΗ

Στόχος της παρούσας διπλωματικής εργασίας είναι να γίνει μια εκτενής ανάλυση με στόχο την κατανόηση της έννοιας των Φυσικών μη Κλωνοποιήσιμων Συναρτήσεων - Physical Unclonable Functions (PUFs) καθώς και των εφαρμογών τους. Παρουσιάζονται πολλοί διαφορετικοί τύποι PUFs αλλά η έμφαση δίνεται περισσότερο στα οπτικά PUFs (optical PUFs) . Αρχικά , γίνεται επεξήγηση της έννοιας των PUFs και εξετάζονται κάποιες σημαντικές μετρικές για την σαφή αξιολόγηση τους . Στη συνέχεια , παρουσιάζονται οι λύσεις που μπορούν να δώσουν τα PUFs σε συγκεκριμένα προβλήματα . Ακόμη , αναλύεται η επιρροή που έχει η αλλαγή ορισμένων παραμέτρων στο αποτέλεσμα . Αφού εξεταστούν και άλλοι τύποι PUFs , γίνεται σύγκριση και ανάλυση των πλεονεκτημάτων και μειονεκτημάτων των οπτικών έναντι των υπολοίπων PUFs. Τέλος , παρατίθενται κάποια παραδείγματα για την κατανόηση της εφαρμογής τους στην πράξη.

Abstract

The aim of this thesis is to make an extensive analysis, so as to allow the reader comprehend the concept of Physical Unclonable Functions (PUFs) as well as their applications. Many different types of PUFs are demonstrated but the main focus is on optical PUFs. To begin with, the concept of PUFs is explained and some metrics are examined for their clear evaluation. Then, solutions that PUFs can provide to specific problems are demonstrated . Furthermore, the influence the change of several parameters has on the result (output) is analyzed. After considering other types of PUFs, the advantages and disadvantages of optical versus other PUFs are compared and analyzed. In the end, some examples are listed to understand their application in practice.

Κεφάλαιο 1: ΕΙΣΑΓΩΓΗΣΤΙΣ PHYSICAL UNCLONABLE FUNCTIONS (PUFs)

1.1 Επεξήγηση της έννοιας ενός PUF

Τα PUFs χρησιμοποιούνται ευρέως και σε πολλούς τομείς , πολλές φορές χωρίς καν να γνωρίζουμε ότι χρησιμοποιούμε PUFs .

Αν και δύσκολα μπορούμε να αποδώσουμε επακριβώς τον ορισμό ενός PUF , μια από τις καλύτερες αποδόσεις θα ήταν **"το δακτυλικό αποτύπωμα ενός αντικειμένου"** που βρίσκουμε στο βιβλίο του (Maes, 2013). Το παρομοιάζουμε με δακτυλικό αποτύπωμα καθώς όπως και στον άνθρωπο , ένα δακτυλικό αποτύπωμα εκφράζει συγκεκριμένα χαρακτηριστικά . Αυτά τα βασικά χαρακτηριστικά είναι :

Μοναδικότητα

Όπως ένα δακτυλικό αποτύπωμα απαντά στην ερώτηση "Ποιος άνθρωπος είναι αυτός;" έτσι αντίστοιχα ένα PUF διακρίνει ένα αντικείμενο από ένα άλλο , είναι δηλαδή εν ολίγοις , το καθοριστικό χαρακτηριστικό του αντικειμένου αυτού.

Είναι έμφυτο

Τα μοναδικά δακτυλικά αποτυπώματα μας είναι ήδη υπάρχοντα από την γέννηση μας .Αντίστοιχα τα PUFs υπάρχουν σε ένα αντικείμενο από την στιγμή της δημιουργίας του , ως αποτέλεσμα μοναδικών παραλλαγών που πραγματοποιούνται κατά της διαδικασία παραγωγής του.

Είναι μη κλωνοποιήσιμο

Τα δακτυλικά αποτυπώματα τέλος , έχουν το χαρακτηριστικό της μη κλωνοποίησης , ακόμη και να πετυχαίναμε να φτιάξουμε 2 οπτικά ίδιους ανθρώπους , δεν θα είχαν το ίδιο δακτυλικό αποτύπωμα (καθώς όπως ανεφέρθη είναι έμφυτο) .Αυτό συνδυαστικά με τα άνω χαρακτηριστικά , είναι αυτό που κάνει ένα PUF τόσο ισχυρό για εφαρμογές ασφαλείας . Είναι ανέφικτη η κλωνοποίηση του και συνεπώς η παραγωγή ενός εντελώς ίδιου αντικειμένου. Ακόμη δηλαδή και με τον πλήρη έλεγχο της διαδικασίας παραγωγής των αντικειμένων δεν είναι εφικτό να φτιαχτούν 2 πανομοιότυπα αντικείμενα.

Αν θέλουμε να αποδώσουμε την έννοια του PUF σε μία φράση θα μπορούσαμε να το πούμε ως εξής:

Ένα PUF είναι μια έκφραση ενός έμφυτου και μη κλωνοποιήσιμου χαρακτηριστικού για ένα συγκεκριμένο στιγμιότυπο ενός φυσικού αντικειμένου.

Τα PUFs είναι διακριτά από δακτυλικά αποτυπώματα και άλλες βιομετρικές παραμέτρους που σχετίζονται με τον άνθρωπο . Παρόλαυτά μπορούν να θεωρηθούν από πολλές απόψεις ισοδύναμα.

1.2Ορολογία και σημειογραφικές συμβάσεις

1.2.1 Ορολογία και συμβάσεις

Σε αυτή την ενότητα θα περιγραφεί η απαραίτητη ορολογία , ονοματολογία και σημειογραφικές συμβάσεις ώστε να καθίστανται σαφείς οι όροι που θα χρησιμοποιηθούν στη συνέχεια και να μην υπάρχει σύγχυση , καθώς και πιθανότητα παρερμηνείας ορισμένων όρων .

Κλάση ενός PUF

Μια κλάση συμβολίζεται με το γράμμα Pκαι είναι η πλήρης περιγραφή της συγκεκριμένου κατασκευαστικού τύπου ενός PUF. Η κλάση παρέχει συγκεκριμένες διαδικασίες .

Χρησιμοποιώντας τη διαδικασία$P.$Create μπορούμε να δημιουργήσουμε στιγμιότυπα της κλάσης $P.$Η διαδικασία $P.$Create είναι μια πιθανολογική διαδικασία την οποία αν θέλουμε να διευκρινίσουμε παρέχουμε μια τυχαία είσοδο:

$$P.Create(r^C) \quad \text{με } r^C \xleftarrow{\$} \{0,1\}* \qquad \text{(Maes, 2013)[6]}$$

Η rC αντιπροσωπεύει έναν απροσδιόριστο αριθμό δίκαιων ρίψεων νομισμάτων . Το Pστην πράξη αντιπροσωπεύει τη λεπτομερή δομική σχεδίαση κατασκευής όπως PUF και η $P.$Create τη φυσική παραγωγική διαδικασία κατασκευής του σχεδίου.

Στιγμιότυπο (instance) PUF

Το αντικείμενο ή στιγμιότυπο μιας κλάσης PUF P συμβολίζεται puf και είναι μια διακριτή περίπτόπωςςυτής τηόπωςάσης όπως δημιουργείται από την $P.$Create .Μια κλάση είναι το σύνολο όλων των στιγμιοτύπων που δημιουργήθηκαν από αυτήν :

$$P \equiv \{puf_i \leftarrow P.Create(r_i{}^C) : \forall i\ , r_i{}^C \xleftarrow{\$} \{0,1\}*\} \quad [6]$$

Ένα στιγμιότυπο puf θεωρείται μια συγκεκριμένη κατάσταση της κατασκευής που περιγράφεται από την κλάση $P.$ Αν κατασκευάσουμε πολλές κλάσεις PUF μπορούμε να διαμορφώσουμε ένα μέρος της κατάστασης του στιγμιοτύπου του PUF που δεν έχει καθοριστεί από τη διαδικασία παραγωγής . Πρακτικά , το ρυθμίζουμε μέσω μιας εξωτερικής εισόδου.

Πρόκληση

Η διαμορφώσιμη κατάσταση x ενός στιγμιοτύπου puf του PUF συμβολίζεται ως puf(x). Αυτή η διαμορφώσιμη κατάσταση ενός στιγμιοτύπου puf του PUF λέγεται challenge (πρόκληση) που εφαρμόζεται στο στιγμιότυπο puf .

Σύνολο προκλήσεων

Το σύνολο των δυνατών προκλήσεων που μπορούν να εφαρμοσθούν σε ένα στιγμιότυπο μιας κλάσης P ενός PUF λέγεται challenge set και συμβολίζεται μεX_P.

Αξιολόγηση PUF

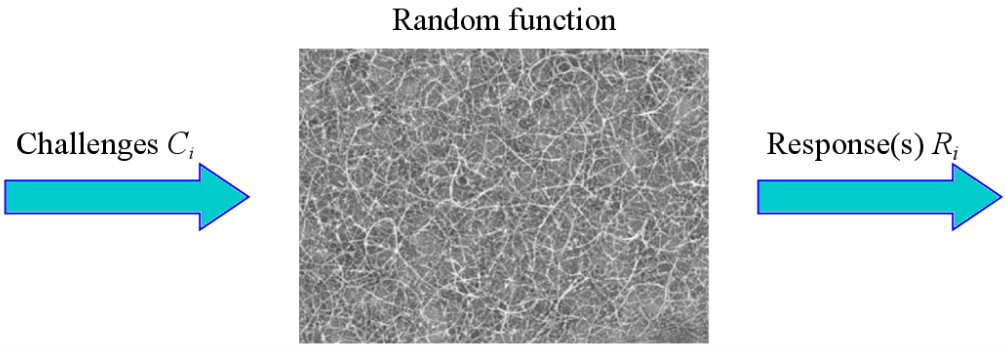
Κάθε στιγμιότυπο puf παρέχει μια διαδικασία αξιολόγησης $puf.Eval$ η οποία παράγει ένα ποσοτικό αποτέλεσμα που αντιπροσωπεύει μια μέτρηση του στιγμιοτύπου αυτού . Όταν το στιγμιότυπο αυτό είναι διαμορφώσιμο γράφουμε : $puf(x).Eval$. Αυτή η διαδικασία είναι επίσης μια πιθανολογική διαδικασία. Αν θέλουμε να διευκρινίσουμε :

$puf(x).Eval(r^E \xleftarrow{\$} \{0,1\}^*)$

Απόκριση

Η διαδικασία αξιολόγησης πρακτικά είναι το αποτέλεσμα του φυσικού πειράματος . Μας δίνει μια συγκεκριμένη μέτρηση για την κατάσταση του στιγμιοτύπου τη δεδομένη στιγμή . Αυτή η μέτρηση θα ονομάζεται απόκριση(response) του στιγμιοτύπου του PUF .

Το σύνολο των δυνατών αποκρίσεων που μπορούν να παραχθούν από ένα στιγμιότυπο puf μιας κλάσης P ενός PUF θα συμβολίζεταισυμβολίζεται με Y_P



Εικόνα 1 : Απεικόνιση της εφαρμογής μιας πρόκλησης για την παραγωγή απόκρισης (P.Eder, 2023)[10]

Συνθήκες αξιολόγησης

Το αποτέλεσμα μιας αξιολόγησης ενός στιγμιοτύπου μια κλάσης ενός PUF επηρεάζεται από φυσικές παραμέτρους. Τέτοιες είναι η θερμοκρασία του περιβάλλοντος , το επίπεδο τάσης τροφοδοσίας κ.λπ. Αυτό ονομάζεται συνθήκη της αξιολόγησης . Όταν χρειάζεται αναφέρουμε μια τέτοια παράμετρο για παράδειγμα τη θερμοκρασία του περιβάλλοντος γράφουμε :

$$puf(x).Eval^{a}, \text{όπου } \alpha = (T_{env} = 60°\text{C})$$

Όταν αυτό παραλείπεται σημαίνει ότι η αξιολόγηση έλαβε μέρος σε κανονικές συνθήκες.

Συντομεύσεις συμβολισμών

Για να αποφεύγουμε την φλύαρη χρήση των μεταβλητών τυχαιοποίησης θα χρησιμοποιούμε πιο συμπαγείς συμβολισμούς χρησιμοποιώντας τυχαίες μεταβλητές. Όταν θέλουμε δηλαδή να δημιουργήσουμε ένα τυχαίο στιγμιότυπο ενός PUF:

$puf_i \leftarrow P.Create(r_i{}^C \xleftarrow{\$} [0,1]*)$ θα γράφεται

PUF$\leftarrow P.Create$ ή ακόμη πιο σύντομα PUF$\leftarrow P$

Η τυχαία αξιολόγηση ενός στιγμιοτύπου puf_iτου PUF με πρόκληση x :

$y_i{}^{(j)}(x) \leftarrow puf_i(x).Eval(r_j{}^E \xleftarrow{\$} [0,1]*)$ θα γράφεται

$Y_i(x) \leftarrow puf_i(x).Eval$ ή ακόμη πιο σύντομα $Y_i(x) \leftarrow puf_i(x)$

Η τυχαία αξιολόγηση ενός τυχαίου στιγμιοτύπου του PUF με πρόκληση x :

$Y(x) \leftarrow PUF(x).Eval$ ή πιο σύντομα $Y(x) \leftarrow PUF(x)$

1.2.2 Παράμετροι των PUF σε πειραματικό επίπεδο

Όπως αναφέρθηκε και παραπάνω , η απόκριση θεωρείται μια τυχαία μεταβλητή . Πειραματικά μπορούμε να κάνουμε εκτίμηση των στατιστικών κατανομής από τις τιμές αποκρίσεων που έχουμε μετρήσει . Έτσι , μια κλάση ενός PUF μπορεί να αξιολογηθεί ως προς την χρηστικότητα της.

Κάνοντας πείραμα παρατηρούμε τις τιμές των αποκρίσεων . Από αυτές τις αποκρίσεις υπάρχουν τρεις σημαντικές κατηγορίες που είναι ευδιάκριτες.

α) Οι αποκρίσεις από διαφορετικά στιγμιότυπα του PUF

β)Οι αποκρίσεις από το ίδιο στιγμιότυπου του PUF αλλά χρησιμοποιώντας διαφορετική πρόκληση

γ)Οι αποκρίσεις από το ίδιο στιγμιότυπο του PUF χρησιμοποιώντας την ίδια πρόκληση αλλά από διαφορετικές αξιολογήσεις.

Ορισμός :

Ένα πείραμα $(N_{puf}, N_{chal}, N_{meas})$σε μια κλάση Pενός PUF είναι ένας πίνακας από τιμές των αποκρίσεων του PUF που αποκτήθηκαν μέσω παρατήρησης. Ένα πείραμα περιέχει $N_{puf} * N_{chal} * N_{meas}$ τιμές που αποτελούνται από αξιολογήσεις αποκρίσεων από N_{puf} τυχαία στιγμιότυπα του PUF από την κλάση P του PUF στις οποίες έχουν εφαρμοστεί οι ίδιες N_{chal}τυχαίες προκλήσεις, με N_{meas} διακριτές αξιολογήσεις αποκρίσεων για κάθε πρόκληση που χρησιμοποιήθηκε σε κάθε στιγμιότυπο του PUF. [6]

$$Experiment_P(N_{puf}, N_{chal}, N_{meas}) \rightarrow Y_{Exp(P)} = [y_i{}^{(j)}(x_k) \leftarrow puf_i(x_k).Eval(r_j{}^E)]$$

Όπου:

$$\forall 1 \le i \le N_{puf} : puf_i \xleftarrow{\$} P$$

$$\forall 1 \le k \le N_{chal}: x_k \xleftarrow{\$} X_p$$

$$\forall 1 \le j \le N_{meas}: r_j^E \xleftarrow{\$} \{0,1\}*$$

Σε περίπτωση που θέλουμε να δηλώσουμε ότι οι αποκρίσεις του πειράματος μετρήθηκαν κάτω από συγκεκριμένες ή ιδιαίτερες συνθήκες , όπως και παραπάνω το δηλώνουμε με το γράμμα α , γράφουμε δηλαδή :

$Experiment_P^a(N_{puf}, N_{chal}, N_{meas})$

1.2.3 Εσωτερική απόσταση απόκρισης PUF (Intra distance)

Η Intra-Distance είναι μια τυχαία μεταβλητή που περιγράφει την απόσταση μεταξύ δύο responses από το ίδιο στιγμιότυπο ενός PUF χρησιμοποιώντας το ίδιο challenge και γράφεται:

$$D_{puf_i}^{intra}(x) \triangleq dist[Y_i(x);\ Y_i'(x)] \text{ [6]}$$

Τα $Y_i(x)$και $Y_i{}'(x)$ συμβολίζουν τις διακριτές τυχαίες αξιολογήσεις του στιγμιοτύπου puf_iτου PUF χρησιμοποιώντας το ίδιο challenge x . Επιπλέον , η απόκριση Intra-Distance του PUF για μια τυχαία πρόκληση σε ένα τυχαία στιγμιότυπο ενός PUF ορίζεται ως η τυχαία μεταβλητή:

$$D_P^{intra} \triangleq D_{PUF \leftarrow P}^{intra}\ (X \leftarrow X_P) \text{ [6]}$$

Η απόσταση **dist**[·;·μπορεί να είναι οποιαδήποτε μέτρηση απόστασης του set αποκρίσεων Y .Μια απόκριση είναι ένα δυαδικό διάνυσμα (bit vector) και η μέτρηση απόστασης που χρησιμοποιούμε είναι η απόσταση Hamming.

Η κατανομή της απόστασης Intra-Distance είναι καθοριστικής σημασίας όταν μιλάμε για εφαρμογές που βασίζονται σε PUFs καθώς μας δείχνει την **αναπαραγωγιμότητα (reproducibility**) μιας κλάσης ενός PUF , έννοια που θα εξηγήσουμε στο επόμενο κεφάλαιο. Επειδή αποτελεί μια από τις σημαντικότερες βασικές μετρήσεις μιας τάξης ενός PUF , τα στατιστικά στοιχεία αυτής της κατανομής μας δίνουν πολλά ποιοτικά χαρακτηριστικά. Αφού παρατηρήσουμε τις αποκρίσεις σε ένα πείραμα $Experiment_P(N_{puf}, N_{chal}, N_{meas})$ υπολογίζουμε ένα νέο πίνακα $D_{Exp(P)}^{intra}$ ως εξής :

$$D_{Exp(P)}^{intra} = [dist[y_i{}^{(j1)}(x_k); y_i{}^{(j2)}(x_k)]]$$

Όπου $\forall 1 \le i \le N_{puf}; \forall 1 \le k \le N_{chal}; \forall 1 \le j_1 \ne j_2 \le N_{meas}$

Από τον πίνακα των Intra-Distances των αποκρίσεων υπολογίζουμε τα παρακάτω στατιστικά για να κάνουμε εκτιμήσεις της κατανομής της απόστασης D_P^{intra}:

Μέσος όρος κατανομής της D_P^{intra}

Ο μέσος όρος της κατανομής υπολογίζεται από το δείγμα του μέσου όρου του πειράματος $D_{Exp(P)}^{intra}$:

$$\mu_P^{intra} = \overline{D_{Exp(P)}^{intra}} = \frac{2}{N_{puf}N_{chal}\,N_{meas}\,(N_{meas}-1)} * \sum D_{Exp(P)}^{intra}$$

Τυπική απόκλιση της κατανομής της D_P^{intra}

$$\sigma_P^{intra} = \sqrt{\frac{2 * \sum(D_{Exp(P)}^{intra} - \mu_P^{intra})^2}{N_{puf}N_{chal}\,N_{meas}\,(N_{meas}-1)-2}}$$

Εκτίμηση του σχήματος της κατανομής της D_P^{intra}:

Η εκτίμηση αυτή γίνεται βλέποντας το ιστόγραμμα του πειράματος της $D_{Exp(P)}^{intra}$:

Στατιστικά μετά το πείραμα

Αν παρατηρήσουμε την κατανομή της $D_{Exp(P)}^{intra}$μπορούμε να βγάλουμε σημαντικά συμπεράσματα . Συνήθως κοιτάμε την ελάχιστη , την μέγιστη και την μέση τιμή. Για περισσότερη λεπτομέρεια μπορούμε να δούμε τα ποσοστά στο 1% και στο 99% . Αυτό το κάνουμε διότι μας επιτρέπουν να κάνουμε μια πολύ αξιόπιστη εκτίμηση π.χ. για τη μέγιστη απόστασηD_P^{intra}των αποκρίσεων του PUF . Έτσι , μπορούμε να έχουμε εικόνα για τη λιγότερο αξιόπιστη απόκριση που μπορούμε να περιμένουμε.

D_P^{intra} και συνθήκες αξιολόγησης

Γενικά , οι συνθήκες αξιολόγησης επηρεάζουν την D_P^{intra}μεταξύ των αποκρίσεων . Η D_P^{intra} μεταξύ δύο αποκρίσεων που αξιολογούνται για το ίδιο στιγμιότυπο του PUF έχοντας εφαρμόσει πάνω του την ίδια πρόκληση αλλά υπό διαφορετικές συνθήκες a_1, a_2 είναι γενικά μεγαλύτερη από την D_P^{intra}μεταξύ των ίδιων αποκρίσεων που όμως αξιολογούνται κάτω από τις ίδιες συνθήκες. Επειδή σε εφαρμογές που χρησιμοποιούμε PUFs μας νοιάζει να γνωρίζουμε πάντα το worst case scenario , θέλουμε να ξέρουμε πάντα τη μεγαλύτερη τιμή της D_P^{intra}κάτω από τις εκάστοτε διαφορετικές συνθήκες αξιολόγησης σε σχέση με την τιμή της D_P^{intra}κάτω από μια συγκεριμένη συνθήκη αναφοράς a_{ref}.

Η D_P^{intra}της απόκρισης ενός PUF υπό συνθήκη a σε σχέση με μια συνθήκη a_{ref}ορίζεται ως η τυχαία μεταβλητή:

$$D_{P;a}^{intra} \triangleq dist[Y_i^{a_{ref}}(x); Y_i^{a}(x)] \quad [6]$$

Όπου $y_i^{a_{ref}}$ και y_i^{a}είναι δύο διακριτές αξιολογήσεις του στιγμιοτύπου puf_iτου PUF έχοντας εφαρμόσει την ίδια πρόκληση xαλλά υπό τις διαφορετικές συνθήκες aκαι a_{ref}.Η D_P^{intra}της απόκρισης ενός PUF για ένα τυχαίο στιγμιότυπο του PUF εφαρμόζοντας μια τυχαία πρόκληση ορίζεται ως η τυχαία μεταβλητή:

$D_{P;a}^{intra} \triangleq D_{PUF \leftarrow P;a}^{intra}(X \leftarrow X_p)$ [6]

Στην πράξη ,ως συνθήκη αναφοράς επιλέγεται μια λειτουργική συνθήκη . Για να βρούμε το χειρότερο intra-distance σε ένα εύρος συνθηκών , αξιολογούμε την intra-distance στα άκρα αυτού του εύρους. Τα άκρα αυτά ονομάζονται corner cases.

1.2.4 Εξωτερική απόσταση απόκρισης PUF (Inter distance)

Η Inter-Distance είναι μια τυχαία μεταβλητή που περιγράφει την απόσταση μεταξύ δύο responses από διαφορετικά στιγμιότυπα ενός PUF χρησιμοποιώντας το ίδιο challenge και γράφεται:

$D_P^{inter}(x) \triangleq \text{dist}[Y(x); Y'(x)]$ [6]

Η κατανομή της τυχαίας μεταβλητής D_P^{inter} είναι πολύ σημαντικό μετρικό για μια κλάση ενός PUF καθώς είναι ενδεικτική της **μοναδικότητας** των στιγμιοτύπων που αυτή η κλάση παράγει. Παρατηρώντας τις αποκρίσεις $Y_{\text{Exp }(P)}$ ενός πειράματος $Experiment_P(N_{puf}, N_{chal}, N_{meas})$, μπορεί να υπολογιστεί ένας νέος πίνακας $D_{Exp(P)}^{inter}$των αποστάσεων inter-distance των αποκρίσεων :

$$D_{Exp(P)}^{inter} = [dist[{y_{i_1}}^{(j)}(x_k); {y_{i_2}}^{(j)}(x_k)]]$$

$$\forall 1 \le i_1 \ne i_2 \le N_{puf}; \forall 1 \le k \le N_{chal}; \forall 1 \le j \le N_{meas}$$

Από το δειγματοληπτικό αυτό πίνακα που υπολογίσαμε , μπορούμε πάλι να κάνουμε μια εκτίμηση των παραμέτρων της κατανομής της D_P^{inter} :

Ο μέσος όρος του δείγματος της $D_{Exp(P)}^{inter}$:

$$\mu_P^{inter} = \overline{D_{Exp(P)}^{inter}} = \frac{2}{N_{puf}\left(N_{puf}-1\right)N_{chal}\ N_{meas}} * \sum D_{Exp(P)}^{inter}$$

Αντίστοιχα , η τυπική απόκλιση υπολογίζεται :

$$\sigma_P^{inter} = \sqrt{\frac{2 * \sum (D_{Exp(P)}^{inter} - \mu_P^{inter})^2}{N_{puf}\left(N_{puf}-1\right)N_{chal}\,N_{meas}\ - 2}}$$

Εκτίμηση του σχήματος της κατανομής της D_P^{inter} μπορούμε να έχουμε κοιτώντας το ιστόγραμμα του πειράματος της $D_{Exp(P)}^{inter}$.

Τα στατιστικά κατά αύξουσα σειρά της $D_{Exp(P)}^{inter}$δίνουν δυνατή πληροφορία για την κατανομή της D_P^{inter} όταν απότομα γίνεται λοξό. Για τις inter-distance των αποκρίσεων ενός

PUF , μας ενδιαφέρουν κυρίως οι ελάχιστες τιμές και συγκεκριμένα το 1% των τιμών της $D_{Exp(P)}^{inter}$ μιας και μας δίνουν την ευκαιρία να κάνουμε καλές εκτιμήσεις για τη μικρότερη inter-distance . Αφού όπως είπαμε η απόσταση Inter-distance χαρακτηρίζει τη μοναδικότητα των στιγμιοτύπων μιας κλάσης ενός PUF , βρίσκοντας τις χαμηλές αυτές τιμές της μπορούμε να προσδιορίσουμε το λιγότερο μοναδικό ζευγάρι στιγμιοτύπου – PUF που μπορούμε να περιμένουμε .

Η inter-distance μεταξύ των αποκρίσεων ενός PUF είναι ευάλωτη σε μεταβολές σε συνθήκες αξιολόγησης . Επειδή όμως για συνηθισμένες εφαρμογές που βασίζονται σε PUFs η αρχική παραγωγή γίνεται σε ελεγχόμενο και ασφαλές , μας νοιάζει μόνο η inter-distance της αξιολόγησης που έχει συμβεί υπό συνθήκη a_{ref} .

1.3 Κατηγορίες των PUFs

1.3.1.1 Μη ηλεκτρονικά PUFs (Non-electronic PUFs)

Αυτή είναι μια κατηγορία μη ηλεκτρονικών αντικειμένων . Η συμπεριφορά τους που θυμίζει PUFs βασίζεται σε υλικά ή μη ηλεκτρονικές τεχνολογίες . Για παράδειγμα τέτοια αντικείμενα μπορεί να είναι :

Η τυχαία δομή ινών ενός φύλλου χαρτιού

Η τυχαία ανάκλαση των χαρακτηριστικών σκέδασης ενός οπτικού

Ο όρος μη ηλεκτρονικά έχει να κάνει με την προέλευση της συμπεριφοράς ενός PUF και όχι με τον τρόπο αποθήκευσης ή επεξεργασίας των αποκρίσεων (responses) του PUF για τον οποίο συχνά χρησιμοποιούνται ηλεκτρονικά και ψηφιακά κυκλώματα.

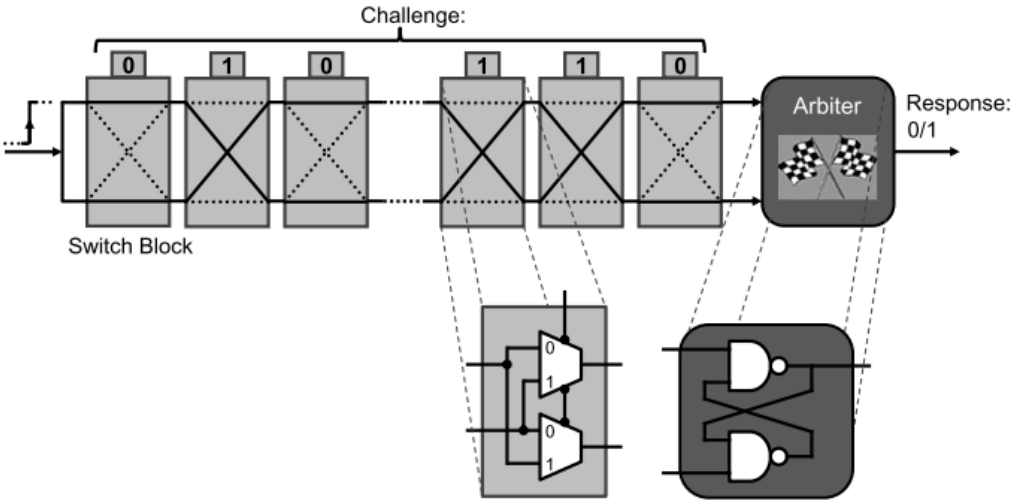
1.3.1.2 Ηλεκτρονικά PUFs (Electronic PUFs)

Σε αυτή την κατηγορία ουσιαστικά μιλάμε για PUFs τα οποία περιέχουν τυχαίες παραλλαγές στα ηλεκτρονικά τους χαρακτηριστικά όπως είναι η αντίσταση , η χωρητικότητα κ.λπ. Και αυτές οι μεταβολές μετριούνται με ηλεκτρονικό τρόπο .

Εδώ αξίζει να αναφέρουμε ότι η διάκριση μεταξύ ηλεκτρονικών και μη ηλεκτρονικών PUFs δεν έχει πάντα σαφή όρια .Πρακτικά όμως ο τρόπος παραγωγής των αποκρίσεων είναι ο ίδιος . Αυτό συμβαίνει διότι η διαφοροποίηση στην ηλεκτρονική συμπεριφορά είναι πάντα συνέπεια των παραλλαγών που λαμβάνουν χώρα σε μη ηλεκτρονικές παραμέτρους π.χ. η αντίσταση ενός μεταλλικού σύρματος καθορίζεται από το μήκος και την τομή του.

Παράδειγμα ενός ηλεκτρονικού PUF που θα αναλυθεί στο κεφάλαιο 5:

Arbiter PUF (PUF διαιτητής) (Εικόνα 39)



1.3.2.1 Εγγενή (intrinsic) PUFs

Για να κατανοήσουμε την έννοια ενός intrinsic PUF θα πρέπει να κοιτάξουμε τις κατασκευαστικές του ιδιότητες . Υπάρχουν δύο ιδιότητες τις οποίες θα πρέπει ένα PUF να πληροί για να θεωρείται intrinsic .

α) Οι μετρήσεις που γίνονται σε αυτό το PUF θα πρέπει να πραγματοποιούνται μέσα σε αυτό με ενσωματωμένο εξοπλισμό μέτρησης.

β) Τα χαρακτηριστικά ενός τυχαίου στιγμιοτύπου του να έχουν δημιουργηθεί κατά τη διαδικασία παραγωγής του.

Όλες οι γνωστές κατασκευές εγγενών PUF είναι PUFs βασισμένα σε πλατφόρμες πυριτίου που βασίζονται σε τυχαίες παραλλαγές που συμβαίνουν κατά τη διαδικασία παραγωγής τους.

1.3.2.2 Μη εγγενή(non-intrinsic) PUFs

Όπως γίνεται κατανοητό σε αντίθεση με τα intrinsic , τα non-intrinsic PUFs θα πρέπει να έχουν τις ανάποδες ιδιότητες .

α) Οι μετρήσεις που γίνονται σε αυτά το PUF θα πρέπει να πραγματοποιούνται εκτός αυτών με εξωτερικό εξοπλισμό μέτρησης.

β) Τα χαρακτηριστικά ενός τυχαίου στιγμιοτύπου του να έχουν εισαχθεί σαφώς από εμάς και να μην εισάγονται τυχαία κατά της διαδικασία κατασκευής τους.

Παράδειγμα ενός non-intrinsic PUF

Η έννοια ενός οπτικού PUF

Μια από τις πιο διαδεδομένες και αναπτυσσόμενες εφαρμογές που βασίζονται σε PUFs είναι τα οπτικά PUFs.

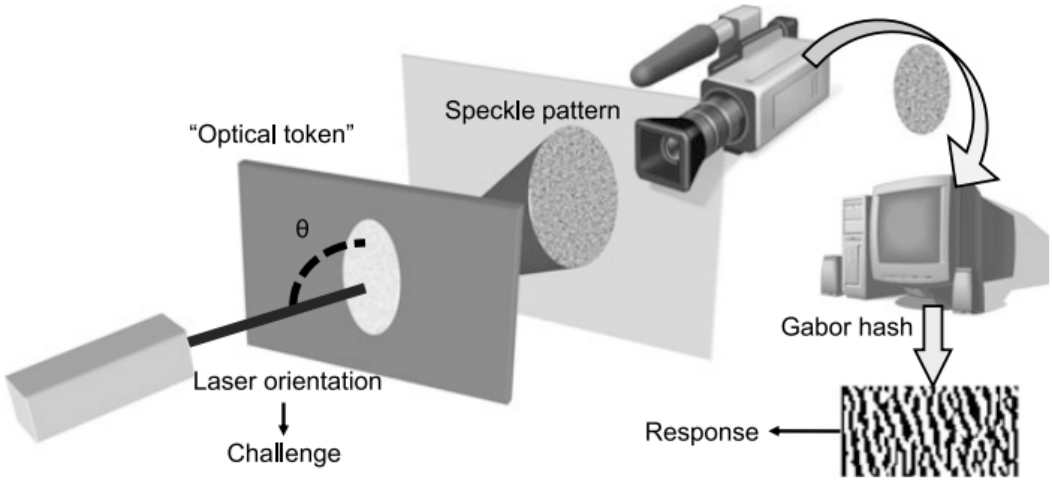
Η ιδέα των οπτικών PUF έγκειται στην αλληλεπίδραση του ορατού φωτός με μια τυχαία μικροδομή . Αυτή την αλληλεπίδραση επηρεάζουν πολλά φυσικά φαινόμενα όπως η

απορρόφηση , η μετάδοση , η ανάκλαση και η σκέδαση .Αν η μικροδομή περιέχει τυχαία στοιχεία , καταλαβαίνουμε ότι το αποτέλεσμα της αλληλεπίδρασης θα είναι σε μεγάλο βαθμό τυχαίο και απρόβλεπτο . Αυτό το αποτέλεσμα μιας τέτοιας σύνθετης αλληλεπίδρασης τα οπτικά PUF το χρησιμοποιούν σαν απόκριση του PUF.

Ο Pappu (Pappu, 2001)[11] ήταν αυτός που εισήγαγε την ιδέα ενός οπτικού PUF , βασισμένο σε ένα διαφανές μέσο ως μια φυσική μονόδρομη συνάρτηση (POWF) , όπως ισχυρίζεται ο Pappu[11] . Εδώ αξίζει να αναφέρουμε ότι με την κρυπτογραφική έννοια του όρου αυτό δεν είναι ακριβές .Η ιδέα είναι η εξής:

Αρχικά κατασκευάζονται μάρκες (tokens) που περιέχουν μια οπτική μικροδομή , αποτελούμενη από μικροσκοπικά διαθλαστικά σωματίδια τα οποία τυχαία αναμιγνύονται μέσα σε ένα μικρό διαφανές εποξειδικό πιάτο. Όταν ρίξουμε φως με ένα laser πάνω στο token , αυτό παράγει ένα ακανόνιστο τυχαίο μοτίβο κηλίδων εξαιτίας της πολλαπλής διασποράς της δέσμης φωτός με τα διαθλαστικά σωματίδια .Στη συνέχεια , το μοτίβο αυτό το παίρνουμε και το επεξεργαζόμαστε ψηφιακά . Έτσι προκύπτει ένα δυαδικό διάνυσμα χρησιμοποιώντας μια τεχνική επεξεργασίας εικόνας γνωστή ως Gabor hashing . Αυτό το διάνυσμα , προκύπτει ότι είναι μοναδικό για το κάθε token και εξαιρετικά ευαίσθητο σε αλλαγές αν πειράξουμε τη θέση του token ή της δέσμης φωτός που ρίχνουμε με το laser.

Στο συγκεκριμένο παράδειγμα , η θέση τοποθέτησης του laser θεωρείται το challenge (η πρόκληση) και το διάνυσμα που προκύπτει θεωρείται το response (η απόκριση) . Για να το οπτικοποιήσουμε , αν κοιτάξουμε την εικόνα μπορεί να γίνει αρκετά πιο κατανοητό .



Εικόνα 2: Σχήμα ενός οπτικού PUF (Pappu R. S., 2002)[11]

Ωστόσο , το πρωτότυπο αυτό PUF που προτάθηκε από τον Pappu έχει κάποια μειονεκτήματα . Αρχικά , η χρήση ενός τέτοιου PUF είναι κουραστική και ακριβή λόγω του εξωτερικού εξοπλισμού που χρειαζόμαστε για να κάνουμε το πείραμα . Το laser και ο μηχανικός εντοπισμός θέσης το καθιστούν μια επίπονη διαδικασία .

Ένα άλλο μειονέκτημα , είναι ότι οι αποκρίσεις είναι λίγες , συγκριτικά με άλλες προτάσεις.

Η φυσική λειτουργικότητα του συγκεκριμένου PUF είναι προφανής . Έχουμε μια φυσική πρόκληση και μια φυσική απόκριση και όλες οι ιδιότητες που θέλουμε να έχει ένα PUF ικανοποιούνται . Τα tokens δηλαδή που παράγονται από την ίδια διαδικασία μας δίνουν αποκρίσεις με ένα υψηλό επίπεδο μοναδικότητας . Αυτές οι απαντήσεις μπορούν να μετρηθούν σχετικά εύκολα και αξιόπιστα .

Αυτά τα οπτικά PUFs , μας παρέχουν ένα μεγάλο αριθμό από προκλήσεις και αποδεικνύεται υπολογιστικά δύσκολο να προβλεφθούν αποκρίσεις για ένα συγκεκριμένο token , ακόμη και στην περίπτωση που κάποιος έχει πολλές πληροφορίες για το token. Ένα άλλο μεγάλο πλεονέκτημα , είναι ότι είναι εύκολο να παρατηρηθούν πιθανές παραβιάσεις , καθώς οποιαδήποτε φυσική τροποποίηση του token αλλοιώνει τις αναμενόμενες αποκρίσεις μέχρι και κατά 50% .

Καμία άλλη κατασκευή PUF δεν επιτυγχάνει όλες αυτές τις ιδιότητες του οπτικού PUF . Έτσι , τα οπτικά PUF θεωρούνται σημείο αναφοράς για τις ιδιότητες ενός PUF.

Άλλες κατασκευές non-intrinsic PUFs που βασίζονται στα οπτικά είναι τα PUF που βασίζονται στο χαρτί , καθώς και τα PUF Φωσφόρου.

1.3.3 Δυνατά και αδύναμα PUFs

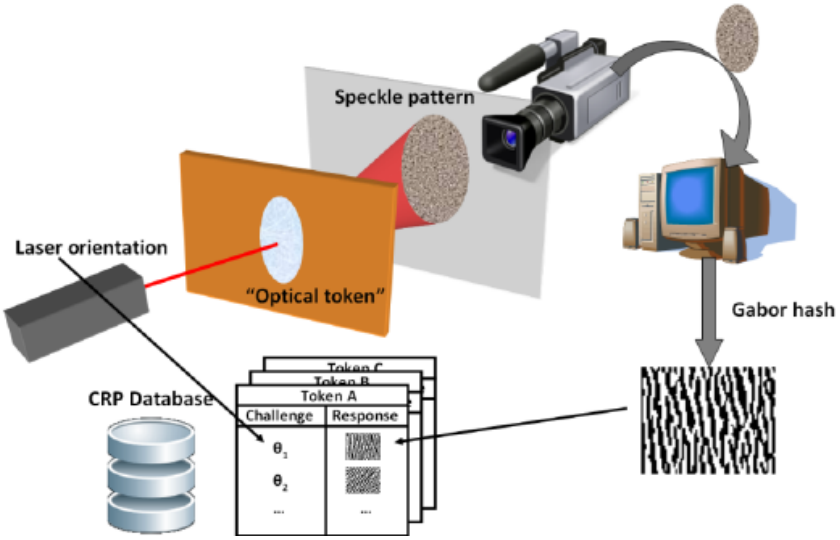
Η ιδιότητα που καθιστά ένα PUF δυνατό ή αδύναμο έγκειται στην συμπεριφορά του ως προς την πρόκληση και την απόκριση αυτής.

Ισχυρό ονομάζεται ένα PUF όταν αν δώσουμε σε έναν αντίπαλο πρόσβαση σε ένα στιγμιότυπο του PUF για ένα μεγάλο χρονικό διάστημα , τότε υπάρχει ακόμη μεγάλη πιθανότητα ο αντίπαλος να μη γνωρίζει την απόκριση για την πρόκληση . Αυτό προϋποθέτει ότι :

α) Πρέπει το σύνολο των δυνατών προκλήσεων να είναι μεγάλο , έτσι ώστε να μη μπορεί ο αντίπαλος εξαντλητικά να δοκιμάσει όλα τα σενάρια προκλήσεων.

β) Είναι απρόβλεπτο . Είναι δηλαδή ανέφικτο να δημιουργήσουμε ένα ακριβές μοντέλο που να βασίζεται σε ζευγάρια προκλήσεων-αποκρίσεων που έχουν παρατηρηθεί.

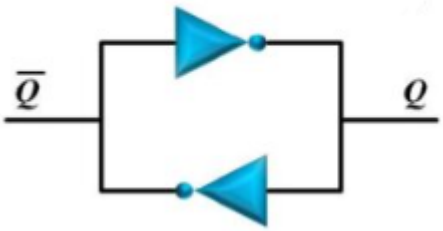
Παράδειγμα ενός δυνατού PUF είναι το οπτικό PUF (Εικόνα 2) :



(Maes, Towards Hardware-Intrinsic Security)[8]

Συνεπώς τα PUF που δεν ικανοποιούν τις προαναφερθείσες προϋποθέσεις και συγκεκριμένα , PUFs που έχουν μικρό σετ προκλήσεων ονομάζονται αδύναμα PUFs. Το χειρότερο δυνατό σενάριο δηλαδή είναι ένα PUF που έχει μόνο μια πρόκληση .Γίνεται λοιπόν σαφές ότι τα δυνατά PUFs προσφέρουν μεγαλύτερη ασφάλεια από τα αδύναμα PUFs , καθιστώντας τα ιδανικά για περισσότερες εφαρμογές . Ωστόσο , η κατασκευή ενός δυνατού εγγενούς PUF αποδεικνύεται πολύ δύσκολη στην πράξη.

Παράδειγμα ενός αδύναμου PUF είναι το SRAM PUF που θα δούμε αναλυτικότερα στο Κεφάλαιο 5 (Εικόνα 42) :



(Professor Helena Silva, 2019)[13]

1.3.4.1 Δυναμικά PUFs

Τα δυναμικά PUFs μας παρέχουν χρονικά ανεξάρτητες αποκρίσεις . Χρησιμοποιούνται κυρίως για την ασφάλεια στο software . Σε αυτά τα PUFs , η απόκριση δεν εξαρτάται μόνο από την πρόκληση αλλά και από τη χρονική στιγμή που πραγματοποιείται η ερώτηση . Ένα δυναμικό PUF δίνει διαφορετικές αποκρίσεις ακόμη και αν ερωτηθεί υπό την ίδια πρόκληση αλλά σε διαφορετική χρονική στιγμή . Θα πρέπει λοιπόν να καλύπτουν 2 ιδιότητες , να παράγουν ανεξάρτητες χρονικά αποκρίσεις και οι αποκρίσεις αυτές να είναι σταθερές. Δεδομένου ότι

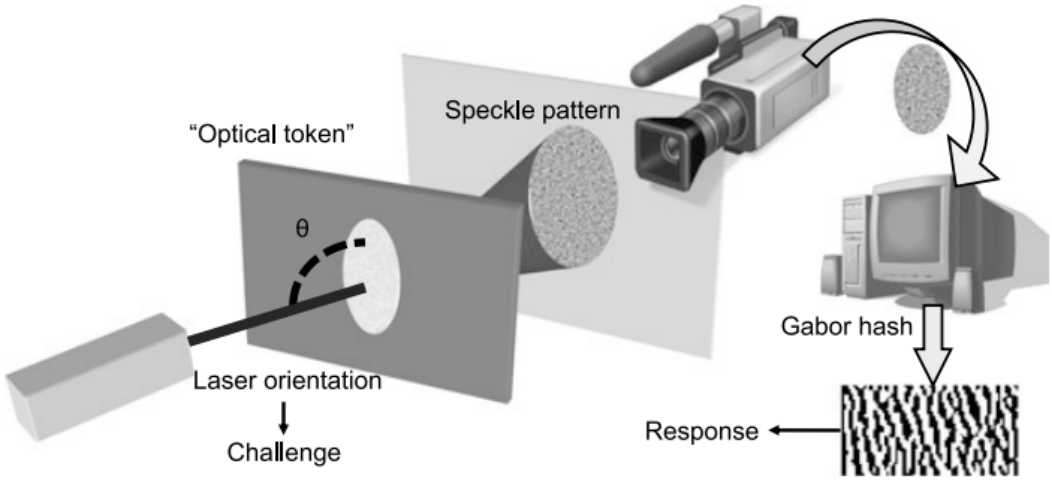
υπάρχει θόρυβος θα πρέπει οι αποκρίσεις να υποστούν επιδιόρθωση λαθών. Για να επιτύχουμε και τις 2 ιδιότητες , χρησιμοποιούμε ένα σύστημα βοηθητικών δεδομένων (HDS) . Έτσι κάθε απόκριση που εξάγουμε είναι συγκεκριμένη ως προς τον χρόνο ερώτησης .

1.3.4.2 Στατικά PUFs

Εδώ ανήκουν τα περισσότερα PUFs όπως τα PUFs που βασίζονται στην καθυστέρηση και τα PUFs που βασίζονται στη μνήμη . Ουσιαστικά η διαφορά τους με τα δυναμικά PUFs είναι ότι η απόκριση τους είναι ανεξάρτητη από τη χρονική στιγμή που θα εφαρμόσουμε την πρόκληση.

Παράδειγμα ενός στατικού PUF (Εικόνα 2) :

Το οπτικό PUF



1.4 Παράμετροι αξιολόγησης ενός PUF

1.4.1 Εξωτερική και εσωτερική αξιολόγηση ενός PUF

Η αξιολόγηση ενός PUF είναι μια φυσική μέτρηση . Αυτή η αξιολόγηση μπορεί να επιτευχθεί είτε εσωτερικά είτε εξωτερικά .

Εξωτερική αξιολόγηση : Η αξιολόγηση αυτή επιτυγχάνεται μετρώντας χαρακτηριστικά που είναι παρατηρούνται εξωτερικά με εξοπλισμό που είναι εξωτερικός του PUF που έχει αυτά τα χαρακτηριστικά.

Εσωτερική αξιολόγηση : Από την άλλη , μια εσωτερική αξιολόγηση επιτυγχάνεται μετρώντας χαρακτηριστικά που είναι παρατηρούνται εσωτερικά με εξοπλισμό που είναι επίσης εσωτερικά ενσωματωμένος στο PUF.

1.4.2 Πλεονεκτήματα και μειονεκτήματα εσωτερικής αξιολόγησης

Οι **εσωτερικές αξιολογήσεις** παρουσιάζουν **αρκετά σημαντικά πλεονεκτήματα** , κάποια από τα οποία είναι τα ακόλουθα :

α) Πρακτικότητα

Έχοντας τον εξοπλισμό ενσωματωμένο στο PUF , σημαίνει ότι κάθε PUF μπορεί να αξιολογεί τον εαυτό του χωρίς την ανάγκη κανενός εξωτερικού περιορισμού .

β) Ακρίβεια

Μια εσωτερική αξιολόγηση είναι πιο ακριβής , καθώς δεν υπάρχει κίνδυνος για εξωτερικές επιρροές και σφάλματα μέτρησης.

γ) Ασφάλεια

Καθώς η απόκριση ενός PUF προέρχεται από το αντικείμενο ενσωμάτωσης , μια εσωτερική αξιολόγηση μπορεί να διασφαλίσει ότι η απόκριση αυτή δεν θα αποκαλυφθεί στον έξω κόσμο και αυτό μπορεί να θεωρηθεί ένα εσωτερικό μυστικό . Χαρακτηριστικό παράδειγμα είναι όταν το αντικείμενο ενσωμάτωσης είναι ένα ψηφιακό ενσωματωμένο κύκλωμα. Σε αυτή την περίπτωση , μπορεί να χρησιμοποιηθεί αμέσως σαν μυστική είσοδος για μια ενσωματωμένη υλοποίηση ενός κρυπτογραφικού αλγορίθμου.

Ένα πιθανό μειονέκτημα μιας εσωτερικής αξιολόγησης είναι η εμπιστοσύνη . Η μέτρηση που θα κάνει ο ενσωματωμένος μηχανισμός μέτρησης δεν μπορεί να επαληθευθεί εξωτερικά αν είναι η αναμενόμενη . Σε μια εξωτερική αξιολόγηση αντιθέτως η μέτρηση μπορεί να παρατηρηθεί εν εξελίξει.

1.4.3 Σαφείς και ασαφείς τυχαίες παραλλαγές

Σαφείς (explicit) και ασαφείς (implicit) τυχαίες παραλλαγές

Μια άλλη κατηγορία διάκρισης των PUFs είναι η πηγή τυχαιότητας των αξιολογούμενων χαρακτηριστικών ενός PUF κατά την κατασκευή του. Ένα instance ενός PUF κατά τη διαδικασία κατασκευής του μπορεί να περιέχει μια σαφή διαδικασία τυχαιοποίησης , έτσι ώστε να εισάγει τυχαία χαρακτηριστικά τα οποία θα μετρηθούν κατά την αξιολόγηση του PUF .

Από την άλλη , μπορεί αυτά τα τυχαία χαρακτηριστικά να εισαχθούν λόγω ανεξέλεγκτων επιδράσεων κατά τη διαδικασία κατασκευής. Αυτό όμως δεν είναι απαραίτητα αρνητικό και παρουσιάζει βασικά πλεονεκτήματα .

1.4.4 Πλεονεκτήματα και μειονεκτήματα των ασαφών (implicit) τυχαίων παραλλαγών

α) Κόστος

Όταν μια παραλλαγή είναι ασαφής σημαίνει ότι είναι πραγματοποιείται τυχαία κατά τη διαδικασία κατασκευής ενός PUF . Πρακτικά αυτό σημαίνει ότι δεν έχει επιπλέον κόστος . Αντίθετα μια σαφής διαδικασία τυχαιοποίησης την οποία εισάγουμε εμείς μπορεί να

αποδειχθεί ακριβή , λόγω χρονικών περιορισμών στην κατασκευαστική ροή μεγάλου όγκου προϊόντων . Η διαδικασία γίνεται πιο αργή λόγω αυτού.

β) Ασφάλεια

Το πιο ενδιαφέρον πλεονέκτημα είναι ότι ακριβώς λόγω αυτής της αδυναμίας ελέγχου τέτοιων τυχαίων παραλλαγών κατά τη διαδικασία παραγωγής , ούτε ο κατασκευαστής που ελέγχει πλήρως τη διαδικασία παραγωγής και έχει όλες τις λεπτομέρειες δεν μπορεί να ελέγξει ή ακόμα περισσότερο να αφαιρέσει τα τυχαία αυτά χαρακτηριστικά .

Μειονέκτημα των ασαφών (implicit) τυχαίων παραλλαγών

Το κύριο μειονέκτημα τέτοιων τυχαίων παραλλαγών είναι ότι ρίχνουν την απόδοση . Αυτό αναγκάζει τους κατασκευαστές να λαμβάνουν μέτρα ώστε να ελέγξουν και να μειώσουν όσο περισσότερο γίνεται τις διακυμάνσεις στη διαδικασία παραγωγής .

ΚΕΦΑΛΑΙΟ 2 : Ιδιότητες των PUFs και σχετικά μετρικά

2.1 Σαφήνεια των ορισμών και των ιδιοτήτων

Στο προηγούμενο κεφάλαιο αναλύσαμε την έννοια ενός PUF και είδαμε παραδείγματα από διαφορετικά είδη εφαρμογών που χρησιμοποιούν PUFs . Όλα αυτά τα παραδείγματα μοιράζονται κάποιες ιδιότητες . Αυτές οι ιδιότητες είναι που μας επιτρέπουν να ορίσουμε κάτι σαν PUF . Σε πολλές κατασκευές όμως , ενώ για τις συγκεκριμένες κατασκευές ταιριάζει ο ορισμός του PUF , στην προσπάθεια γενίκευσης δημιουργείται μια σύγχυση καθώς σε ένα ευρύτερο κομμάτι κατασκευών δεν είναι σαφείς .

Κάποιοι ορισμοί είναι αρκετά αυστηροί (ορισμός μιας POWF)όμως πολλές φορές οι κατασκευές που προτείνονται στη συνέχεια δεν πληρούν τις προϋποθέσεις αυτές.

Από την άλλη , άλλοι ορισμοί είναι πολύ αφηρημένοι (ορισμός μια RNG) και σαν αποτέλεσμα ισχύουν για κατασκευές που δεν θεωρούνται PUFs.

Τέλος , πολλοί από τους προτεινόμενους ορισμούς επινοούνται επί σκοπώ, με στόχο τις ιδιότητες της νέας κατασκευής και δεν τίθενται σε σαφή όρια. Πολλές φορές δηλαδή καταλήγει ο ορισμός να εξυπηρετεί την εκάστοτε κατασκευή και επομένως να έχουμε όσους ορισμούς όσες και κατασκευές PUF. Έτσι , δημιουργείται σύγχυση και ασάφεια . Σύνηθες είναι ορισμοί που εμφανίζονται σε κάποιες κατασκευές να γενικεύονται και να θεωρείται ότι ισχύουν για κάθε κατασκευή PUF , κάτι που όμως δε συμβαίνει στην πραγματικότητα.

Στην πράξη , αυτό αποδεικνύεται καταστροφικό , καθώς τίθενται θέματα ασφαλείας όταν μια κατασκευή βασίζεται σε αυτούς τους ορισμούς , άρα και στις ιδιότητες που αυτοί προασπίζουν .

2.2 Ιδιότητες

2.2.1 Κατασκευασιμότητα

Η κατασκευασιμότητα είναι η συνθήκη που μας διασφαλίζει ότι είναι πραγματικά εφικτό να κατασκευαστούν στιγμιότυπα ενός PUF.

Ορισμός :

Μια κλάση Pενός PUF είναι κατασκευάσιμη αν είναι εύκολο να επικαλεστούμε τη διαδικασία Create και να παράξουμε ένα τυχαία στιγμιότυπο puf του PUF τέτοιο ώστε :

$$puf \leftarrow P.\text{Create}\{0, 1\}^*)$$

Δεν έχει νόημα να κοιτάξουμε τίποτα άλλο για ένα PUF αν αυτό δεν μπορεί να παράγει εφικτά στιγμιότυπα . Έτσι , η ιδιότητα της κατασκευασιμότητας είναι προαπαιτούμενη για όλες τις ιδιότητες που ακολουθούν .

Εδώ να σημειωθεί ότι η κατασκευασιμότητα έχει να κάνει μόνο με το αν είναι εύκολο να παράγουμε τυχαία στιγμιότυπα ενός PUF και δεν έχει να κάνει με άλλες παραμέτρους όπως η συμπεριφορά πρόκλησης-απόκρισης . Η κατασκευή ενός συγκεκριμένου στιγμιοτύπου από την άλλη μπορεί να είναι πολύ δύσκολη .

2.2.2 Αξιολογησιμότητα

Ορισμός:

Μια κλάση Pενός PUF είναι αξιολογήσιμη , εάν είναι κατασκευάσιμη και αν για κάθε τυχαία στιγμιότυπο $puf \in P$του PUF και κάθε τυχαία πρόκληση $x \in X_P$είναι εύκολο να αξιολογήσουμε μια απόκριση :

$$y \leftarrow puf(x).\text{Eval}\{0, 1\}^*)$$

Δεδομένου ότι οι ιδιότητες που θα δούμε ασχολούνται με τη συμπεριφορά πρόκλησης-απόκρισης , δεν έχει νόημα να συζητάμε για κατασκευές που είναι μη αξιολογήσιμες .

Η ευκολία που περιγράφεται στον ορισμό είναι σχετική . Στην πράξη , εύκολη αξιολόγηση θεωρείται αυτή που είναι εφικτή μέσα σε όρια χρόνου , κόστους , ενέργειας κ.λπ.

2.2.3 Αναπαραγωγιμότητα

Η αναπαραγωγιμότητα ορίζεται σε σχέση με την κατανομή της intra-distance των αποκρίσεων όλης της κλάσης του PUF , δηλαδή λαμβάνοντας υπόψιν αξιολογήσεις τυχαίων προκλήσεων πάνω σε τυχαία στιγμιότυπα του PUF.

Ορισμός:

Μια κλάση Pενός PUF είναι αναπαραγώγιμη εάν είναι αξιολογήσιμη και αν η πιθανότητα να είναι μικρή η Pr) είναι μεγάλη.

Αυτό σημαίνει ότι με μεγάλη πιθανότητα , οι αποκρίσεις που προκύπτουν από την αξιολόγηση της ίδιας πρόκλησης στο ίδιο στιγμιότυπο του PUF θα πρέπει να είναι παρόμοιες , δηλαδή κοντινές τιμές στο μετρικό απόστασης .

Οι έννοιες ‘μικρή’ και ‘μεγάλη’ όταν μιλάμε για την απόσταση και την πιθανότητα αυτή να είναι μικρή ή μεγάλη στον ορισμό εξαρτάται από το πλαίσιο και τις απαιτήσεις της εφαρμογής . Δεν υπάρχει μια de facto απόσταση που θεωρείται μικρή .

2.2.4 Μοναδικότητα

Η πιο βασική ιδιότητα ενός PUF σε ότι έχει να κάνει με την ασφάλεια είναι η μοναδικότητα . Η παρατήρηση δηλαδή ότι μια απόκριση του PUF είναι μια μέτρηση ενός τυχαίου χαρακτηριστικού για ένα συγκεκριμένο στιγμιότυπο .

Ορισμός:

Μια κλάση Pενός PUF είναι μοναδική εάν είναι αξιολογήσιμη , και αν η πιθανότητα να είναι μεγάλη η $Pr)$ είναι μεγάλη .

Η μοναδικότητα ορίζεται σε σχέση με την κατανομή της intra-distance των αποκρίσεων για όλη την κλάση του PUF , αξιολογώντας δηλαδή τυχαίες προκλήσεις πάνω σε τυχαία ζεύγη στιγμιοτύπων του PUF.

Στην πράξη αυτό σημαίνει ότι οι αποκρίσεις που προκύπτουν από την αξιολόγηση των ίδιων προκλήσεων πάνω σε διαφορετικά στιγμιότυπα του PUF θα πρέπει να είναι ανόμοιες (να απέχουν πολύ στη μέτρηση της απόστασης) με μεγάλη πιθανότητα . Ο όρος μεγάλη όταν χρησιμοποιείται για την απόσταση και την πιθανότητα είναι και πάλι σχετικός με το πλαίσιο .

2.2.5 Αναγνωρισιμότητα

Όταν μια κλάση είναι ταυτόχρονα αναπαραγώγιμη και μοναδική , αυτό σημαίνει ότι τα στιγμιότυπα αυτής μπορούν να ταυτοποιούνται βάσει των αποκρίσεων τους . Αυτό εκφράζεται ως μια νέα ιδιότητα :

Ορισμός :

Μια κλάση Pενός PUF είναι αναγνωρίσιμη (ή ταυτοποιήσιμη) εάν είναι αναπαραγώγιμη και μοναδική , και συγκεκριμένα αν η πιθανότητα $Pr)$είναι υψηλή .

Η αναγνωρισιμότητα εκφράζει το γεγονός ότι η ίδια πρόκληση στο ίδιο στιγμιότυπο ενός PUF θα έχει πιο παρόμοιες αποκρίσεις συγκριτικά με τις αποκρίσεις από διαφορετικά στιγμιότυπα του PUF. Αυτό σημαίνει ότι βασει της αξιολόγησης των αποκρίσεων , τα στιγμιότυπα μπορούν να εκφράσουν μια στατική ταυτότητα που κατά μεγάλη πιθανότητα είναι μοναδική .

Οι κατανομές των αποστάσεων inter-distance και intra-distance όπως γίνεται αντιληπτό παίζουν καθοριστικό ρόλο στη χρησιμότητα μιας κλάσης και άρα είναι ζωτικής σημασίας να έχουμε ακριβή πληροφορία για αυτές τις κατανομές από τα στατιστικά του πειράματος.

2.2.6 Φυσική μη Κλωνοποιησιμότητα

Ας υποθέσουμε ότι δίνουμε σε έναν αντίπαλο τον έλεγχο της διαδικασίας δημιουργίας μιας κλάσης του PUF και έτσι μπορεί να επηρεάσει τις παραμέτρους της P.Create σε ένα μεγάλο βαθμό όσο αυτό είναι εφικτό . Όταν εξετάζεται η αναγνωρισιμότητα λοιπόν παρουσία του αντιπάλου αυτού με βάση τις αποκρίσεις του PUF προκύπτει η ανάγκη για περαιτέρω

διασφάλιση ότι οι ιδιότητες του PUF είναι μοναδικές και με μεγάλη πιθανότητα . Αυτό χρειάζεται καθώς ένας τέτοιος αντίπαλος θα μπορεί να δημιουργήσει τέτοια στιγμιότυπα , που θα είναι περισσότερο όμοια από ότι θα περιμέναμε . Κρίνεται λοιπόν απαραίτητη η μοναδικότητα , τέτοια όμως ώστε να υπάρχει ασφάλεια ακόμη και με την παρουσία ενός τέτοιου αντιπάλου . Αυτό ονομάζεται φυσική μη κλωνοποιησιμότητα .

Ορισμός :

Μια κλάση Pενός PUF είναι φυσικά μη κλωνοποιήσιμη εάν είναι αξιολογήσιμη και αν είναι δύσκολο να επηρεαστεί η P.Create ώστε να παραχθούν δύο διακριτά στιγμιότυπα $puf και puf'$ του της κλάσης Pτου PUF με τέτοιο τρόπο ώστε να είναι μεγάλη η πιθανότητα :

$$Pr\textbf{dist}\,[Y \leftarrow puf(X); Y' \leftarrow puf'(X) < D_P^{inter}(X)$$

για $X \leftarrow X_P$. Στο ακράιο αλλά ιδανικό σενάριο θα θέλαμε να είναι δύσκολη η παραγωγή δύο στιγμιοτύπων του PUF με τέτοιο τρόπο ώστε να είναι μικρή η πιθανότητα :

$$Pr\textbf{dist}\,[Y \leftarrow puf(X); Y' \leftarrow puf'(X) < D_P^{intra}(X)$$

Η δυσκολία παραγωγής ενός μη μοναδικού ζευγαριού στιγμιοτύπων του PUF όπως περιγράφεται στον ορισμό υπονοεί τη δυσκολία παραγωγής ενός στιγμιοτύπου του PUF το οποίο να είναι πιο όμοιο με ένα δεδομένο στιγμιότυπο του PUF από αυτό που εκφράζεται από την ιδιότητα της μοναδικότητας . Αν ικανοποιείται η κατασκευασιμότητα , τότε πρακτικά ξέρουμε ότι είναι εύκολο να δημιουργηθεί ένα τυχαίο στιγμιότυπο του PUF αλλά είναι δύσκολο να δημιουργηθεί ένα συγκεκριμένο στιγμιότυπο του PUF.

Άρα , μια κλάση που παρουσιάζει φυσική μη κλωνοποιησιμότητα είναι ιδανική για εφαρμογές ασφαλείας καθώς ούτε ο κατασκευαστής των στιγμιοτύπων του PUF δεν μπορεί να σπάσει την ιδιότητα της μοναδικότητας . Άρα κάθε στιγμιότυπο του PUF είναι μοναδικό με υψηλή πιθανότητα ασχέτως του κατασκευαστή . Αυτό το πλεονέκτημα ονομάζεται manufacturer resistance.

2.2.7 Απροβλεπτότητα

Πολλές εφαρμογές των PUF βασίζονται στη λειτουργικότητα των ζευγαριών πρόκληση-απόκριση δηλαδή στην ικανότητα όταν εφαρμόζουμε μια πρόκληση να λαμβάνουμε σαν απάντηση μια τυχαία απόκριση . Έτσι όμως , φυσική μη κλωνοποιησιμότητα και πόσο μάλλον η μοναδικότητα από μόνη της δεν αρκούν για την διασφάλιση της ασφάλειας. Χρειαζόμαστε απροβλεπτότητα μεταξύ των αποκρίσεων σε ένα συγκεκριμένο στιγμιότυπο ενός PUF έτσι ώστε οι αποκρίσεις που δεν έχουμε παρατηρήσει να παραμένουν αρκετά τυχαίες , ακόμη και μετά την παρατήρηση αποκρίσεων εφαρμόζοντας άλλες προκλήσεις στο ίδιο στιγμιότυπο του PUF.

Ορισμός:

Μια κλάση Pενός PUF είναι απρόβλεπτη εάν είναι αξιολογήσιμη , και αν είναι δύσκολο για ένα τυχαίο στιγμιότυπο του PUF να κερδηθεί το ακόλουθο παιχνίδι :

Στη φάση μάθησης , επιτρέπεται να αξιολογήσουμε το puf πάνω σε συγκεκριμένο αριθμό προκλήσεων και να παρατηρήσουμε τις αποκρίσεις . Το σύνολο των αξιολογούμενων

προκλήσεων συμβολίζεται X'_pκαι οι προκλήσεις επιλέγονται είτε τυχαία (οπότε έχουμε αδύναμη απροβλεπτότητα) είτε επιλέγονται προσαρμοστικά (οπότε έχουμε υψηλή απροβλεπτότητα) .

Σε φάση που εφαρμόζουμε πρόκληση , παρουσιάζεται κάποιος με μια τυχαία πρόκληση $X \leftarrow X_P{}'_p$. Απαιτείται να κάνει μια πρόβλεψη Y_{pred} για την απόκριση στην πρόκληση που εφάρμοσε όταν αξιολογείται το puf. Δεν έχει πρόσβαση στο puf , αλλά η πρόβλεψη γίνεται με έναν αλγόριθμο πρόβλεψης που χρησιμοποιεί τα δεδομένα που μάζεψε από τη φάση μάθησης : $Y_{pred} \leftarrow predict(X)$.

Το παιχνίδι κερδίζεται αν η πιθανότητα:

Pr (**dist**[$Y_{pred} \leftarrow predict(X); Y \leftarrow puf(X) < D_P^{inter}(X)$είναι υψηλή.

Υπάρχει μια ομοιότητα της ιδιότητας αυτής με τη φυσική μη-κλωνοποιησιμότητα αφού περιλαμβάνουν την κατανομή της D_P^{inter} .Ωστόσο , εδώ εξετάζουμε την απόσταση από έναν αλγόριθμο πρόβλεψης που έχει λάβει τη γνώση του από ένα σύνολο προκλήσεων και αποκρίσεων που έχει παρατηρήσει πάνω στο ίδιο στιγμιότυπο του PUF, σε αντίθεση με τη φυσική μη-κλωνοποιησιμότητα όπου εξετάζουμε αυτή την απόσταση σε ένα δεύτερο puf' του PUF που δημιουργήσαμε .

Η απροβλεπτότητα ορίζεται σε σχέση με το καλύτερο δυνατό αλγόριθμο πρόβλεψης που δύναται να κατασκευαστεί , να εκπαιδευτεί και να αξιολογηθεί εντός των δυνατοτήτων του αντιπάλου . Η ιδανική περίπτωση για να έχουμε τη μέγιστη απροβλεπτότητα , είναι όταν οι αποκρίσεις σε διαφορετικές προκλήσεις είναι εντελώς ανεξάρτητες , πράγμα που σημαίνει ότι δεν μπορούν να προβλεφθούν από κανένα αλγόριθμο πρόβλεψης . Αυτό βέβαια αποδεικνύεται πολύ δύσκολα και είναι σπανίως εφικτό .

Για άλλες κατασκευές PUF ,οι αποκρίσεις δεν είναι ανεξάρτητες και η απροβλεπτότητα που επιδιώκουμε να έχουμε έγκειται στην υπολογιστική δυσκολία κατασκευής , εκπαίδευσης και αξιολόγησης ενός καταλλήλου αλγορίθμου πρόβλεψης .Σε αυτή την περίπτωση , η απροβλεπτότητα μπορεί μόνο να εκτιμηθεί σε σύγκριση με την καλύτερη πιο γνωστήεπίθεση μοντελοποίησης καθώς κανείς δεν διαβεβαιώνει ότι δεν υπάρχει ή θα υπάρξει κάποια καλύτερη.

2.2.8 Μαθηματική μη κλωνοποιησιμότητα

Σε αντίθεση με την απροβλεπτότητα όπου ο αντίπαλος μαθαίνει μόλις έναν περιορισμένο και πιθανότατα τυχαίων αριθμό ζευγαριών πρόκλησης-απόκρισης , θα πρέπει να ληφθεί υπόψιν ένα ίσως ισχυρότερο μοντέλο αντιπάλου όταν αυτός έχει απεριόριστη φυσική πρόσβαση σε ένα στιγμιότυπο του PUF. Αυτό σημαίνει ότι μπορεί να μάθει όσα ζευγάρια πρόκλησης-απόκρισης όσα είναι δυνατό να αποθηκεύσει και πέραν αυτού να κάνει και περαιτέρω παρατηρήσεις για το στιγμιότυπο πέραν της συμπεριφοράς πρόκλησης-απόκρισης .

Ορισμός:

Μια κλάση Pενός PUF θεωρείται μαθηματικά μη κλωνοποιήσιμη αν είναι απρόβλεπτη , ακόμη και αν δεν υπάρχει όριο στην πρόσβαση που μπορεί να έχει κανείς στο στιγμιότυπο του PUF κατά της διάρκεια της φάσης μάθησης ασχέτως των δυνατοτήτων του.

Η μαθηματική μη κλωνοποιησιμότητα είναι δηλαδή μια επέκταση της απροβλεπτότητας για το σενάριο όπου ένας αντίπαλος έχει απεριόριστη φυσική πρόσβαση στο στιγμιότυπο του PUF. Βασική προϋπόθεση για να θεωρείται μια κλάση μαθηματικά μη κλωνοποιήσιμη , είναι τι σύνολο προκλήσεων X_P να είναι πολύ μεγάλο και κατά προτίμηση εκθετικό ως προς μια παράμετρο της κλάσης P.Αυτό το χρειαζόμαστε διότι αν το σύνολο των προκλήσεων είναι μικρό , μπορεί κάποιος που έχει φυσική πρόσβαση σε ένα στιγμιότυπο να αξιολογήσει εξαντλητικά το σύνολο των προκλήσεων και να αποθηκεύσει τις αποκρίσεις αυτών σε έναν πίνακα . Αυτός ο πίνακας με τη σειρά του αποτελεί το τέλειο μοντέλο πρόβλεψης αυτού του στιγμιοτύπου και άρα δεν έχουμε απροβλεπτότητα.

Το ίδιο ισχύει και στο σενάριο που ενώ έχουμε ένα μεγάλο σύνολο προκλήσεων παρουσιάζεται ένας σχεδόν τέλειος αλγόριθμος πρόβλεψης των αποκρίσεων που μπορεί να εκπαιδευτεί πάνω σε ένα υποσύνολο του συνόλου προκλήσεων.

2.2.9 Πραγματική μη κλωνοποιησιμότητα

Παραπάνω είδαμε τις έννοιες της φυσικής καθώς και της μαθηματικής κλωνοποιησιμότητας . Και οι δύο έννοιες περιγράφουν το ίδιο πράγμα αλλά υπό διαφορετικές οπτικές. Η φυσική κλωνοποιησιμότητα έχει να κάνει με πραγματικούς κλώνους ενός PUF ενώ η μαθηματική κλωνοποιησιμότητα επικεντρώνεται στην κλωνοποίηση της συμπεριφορά πρόκλησης-απόκρισης ενός στιγμιοτύπου . Για να είναι μια κλάση ενός PUF πραγματικά μη κλωνοποιήσιμη θα πρέπει να είναι και φυσικά και μαθηματικά μη κλωνοποιήσιμη.

Ορισμός:

> Μια κλάση Pενός PUF είναι πραγματικά μη κλωνοποιήσιμη αν είναι ταυτόχρονα φυσικά και μαθηματικά μη κλωνοποιήσιμη .

2.2.10 Μονόδρομη

> Ορισμός:
>
> Μια κλάση Pενός PUF είναι μονόδρομη εάν είναι αξιολογήσιμη για αν για κάθε στιγμιότυπο του PUF puf $\in P$δεν υπάρχει κάποιος γνωστός αποτελεσματικός αλγόριθμος $invert_{puf} : Y_P \rightarrow X_P$ που να του επιτρέπεται να αξιολογήσει το puf έναν ικανοποιητικό αριθμό φορών και για τον οποίο ισχύει ότι είναι χαμηλή πιθανότητα :
>
> $$\Pr(\textbf{dist}\,[Y \leftarrow puf(X); Y' \leftarrow puf\left(invert_{puf}(Y)\right) > D_P^{intra}(X)$$

Θέλουμε δηλαδή να μην υπάρχει κανένας αποτελεσματικός αλγόριθμος αντιστροφής που να μπορεί να βρει την πρόκληση που θα παρήγαγε μια συγκεκριμένη απόκριση κοντά στη δεδομένη απόκριση . Ωστόσο αυτό έχει να κάνει και με το μέγεθος του συνόλου των προκλήσεων και αποκρίσεων των κατασκευών PUF. Για κατασκευές με λίγες προκλήσεις δεν μπορούμε να επιτύχουμε το να είναι η κλάση μονόδρομη καθώς μπορεί εύκολα να αξιολογηθεί κάθε δυνατή πρόκληση και να αναζητηθεί ο αντίστροφος πίνακας για την αντιστροφή της δεδομένης απάντησης .Από την άλλη , αν ο αριθμός των αποκρίσεων είναι

μικρός , τότε ο αλγόριθμος αντιστροφής μπορεί να αξιολογήσει τυχαίες προκλήσεις στο στιγμιότυπο του PUF και να βρει γρήγορα μία που αντιστρέφει την δεδομένη απόκριση.

2.2.11 Η παραβίαση να έχει αντίκτυπο

Ορισμός:

Μια κλάση P ενός PUF παρουσιάζει αντίκτυπο αν παραβιαστεί εαν είναι αξιολογήσιμη και αν για κάθε στιγμιότυπο του PUF , κάθε φυσικός μετασχηματισμός $puf \Rightarrow puf'$ έχει τέτοιο αποτέλεσμα ώστε η πιθανότητα:

Pr(**dist** $[Y \leftarrow puf(X); Y' \leftarrow puf'(X) > D_P^{intra}(X)$ να είναι υψηλή

και ιδανικά

Pr(**dist** $[Y \leftarrow puf(X); Y' \leftarrow puf'(X) < D_P^{inter}(X)$ να είναι χαμηλή

Πρακτικά αυτό σημαίνει ότι είναι πολύ δύσκολο να αλλοιωθεί φυσικά ένα στιγμιότυπο του PUF χωρίς αυτό να επηρεάσει τη συμπεριφορά πρόκλησης – απόκρισης . Για παράδειγμα , μια επίδραση που με μεγάλη πιθανότητα είναι μεγαλύτερη από την αναξιοπιστία του PUF όπως αυτή εκφράζεται από την κατανομή της D_P^{intra} .Τα PUF με προφανή παραβίαση είναι αυτοπροστατευτικά που σημαίνει ότι μια επίθεση παραποίησης αλλάζει αναπόφευκτα τις αποκρίσεις τους , επομένως η λειτουργικότητα χαλάει και έχουμε απώλεια μυστικών πληροφοριών. Μπορούν να χρησιμοποιηθούν για την κατασκευή ενός μεγαλύτερου συστήματος ασφαλείας ανθεκτικού στην παραβίαση ενσωματώνοντας το σύστημα σε ένα στιγμιότυπο του PUF με εμφανή παραβίαση.

Αφού έγινε ανάλυση όλων των ιδιοτήτων , ας δούμε ποιες κατασκευές PUF ικανοποιούν τις ιδιότητες που είναι επιθυμητές .

Property	Optical PUF	Coating PUF	Simple Arbiter PUF	FF Arbiter PUF	XOR Arbiter PUF	Basic Ring Oscillator PUF	Enhanced Ring Oscillator PUF	SRAM PUF	Flip-flop / Butterfly / Latch / Buskeeper PUF	Glitch PUF	Bistable Ring PUF
Constructibility	V	V	V	V	V	V	V	V	V	V	V
Evaluability	V	V	V	V	V	V	V	V	V	V	V
Reproducibility	V	V	V	V	V	V	V	V	V	V	V
Uniqueness	V	V	V	V	V	V	V	V	V	V	V
Identifiability	V	V	V	V	V	V	V	V	V	V	V
Physical Unclonability	V	V	V	V	V	V	V	V	V	V	V
Unpredictability	V	V	!	!	?	V	?	V	V	?	?
Mathematical Unclonability	V	X	X	X	?	X	?	X	X	?	?
True Unclonability	V	X	X	X	?	X	?	X	X	?	?
One-wayness	V	X	X	X	X	X	X	X	X	X	X
Tamper Evidence	V	V	?	?	?	?	?	?	?	?	?

Εικόνα 3 : Πίνακας ικανοποίησης ιδιοτήτων του κάθε PUF

✓ : ικανοποιεί την ιδιότητα
X : δεν ικανοποιεί την ιδιότητα
? : δεν είναι ακόμα σίγουρο / χρειάζεται περισσότερη έρευνα
! : ικανοποιεί την ιδιότητα υπό συνθήκες

Κεφάλαιο 3: Φυσικές μονόδρομες συναρτήσεις με χρήση οπτικών σκεδαστών πολλαπλής σκέδασης

3.1 Εισαγωγή

Η κρυπτογραφία στις μέρες μας , βασίζεται στη χρήση μονόδρομων συναρτήσεων που αξιολογούνται εύκολα αλλά αντιστρέφονται δύσκολα . Δυστυχώς , οι ευρέως διαδεδομένες τέτοιες συναρτήσεις είναι είτε βασισμένες σε μη αποδεδειγμένες θεωρίες είτε έχουν γνωστές ευπάθειες. Αντί λοιπόν να βασιζόμαστε στη θεωρία των αριθμών , η μεσοσκοπική φυσική της συνεκτικής μεταφοράς μέσα από ένα διαταραγμένο μέσο θα μας βοηθήσει να προσπαθήσουμε να υλοποιήσουμε ένα άλλο σενάριο με στόχο την κατανομή και τον έλεγχο ταυτότητας μοναδικών αναγνωριστικών . Αυτό θα επιτευχθεί αν φυσικά μετατρέψουμε τη μικροδομή του μέσου σε μια σταθερού μήκους συμβολοσειρά δυαδικών ψηφίων. Τέτοιες φυσικές μονόδρομες συναρτήσεις είναι φθηνές στην κατασκευή , απαγορευτικά δύσκολο να αντιγραφούν , δεν δύνανται να αναπαρασταθούν με μαθηματικά και είναι εγγενώς ανθεκτικές σε παραβιάσεις . Θα δούμε ένα πρωτόκολλο ταυτοποίησης που βασίζεται στο μεγάλο μέγεθος των διευθύνσεων που αποτελεί κύριο χαρακτηριστικό για τις φυσικές μονόδρομες συναρτήσεις .

3.2 Θεωρητική προετοιμασία

Οι κρυπτογραφικές εφαρμογές με εισόδους μεταβλητού μήκους όπως η αποθήκευση κωδικών του υπολογιστή ή η ψηφιακή υπογραφή ηλεκτρονικών εγγράφων χρησιμοποιούν ως κρυπτογραφική αρχή τις μονόδρομες συναρτήσεις κατακερματισμού . Μια τέτοια συνάρτηση συμπιέζει ένα αυθαίρετο μήκος εισόδου σε ένα σταθερό μήκος εξόδου και έχει την ιδιότητα ότι αν αλλάξουμε ένα bit στην είσοδο αλλάζουν περίπου τα μισά στην έξοδο . Για μια μονόδρομη συνάρτηση κατακερματισμού θεωρείται αδύνατο να βρεθεί η είσοδος που δίνει μια συγκεκριμένη έξοδο και είναι επίσης δύσκολο να βρεθούν δύο είσοδοι που να δίνουν την ίδια έξοδο .

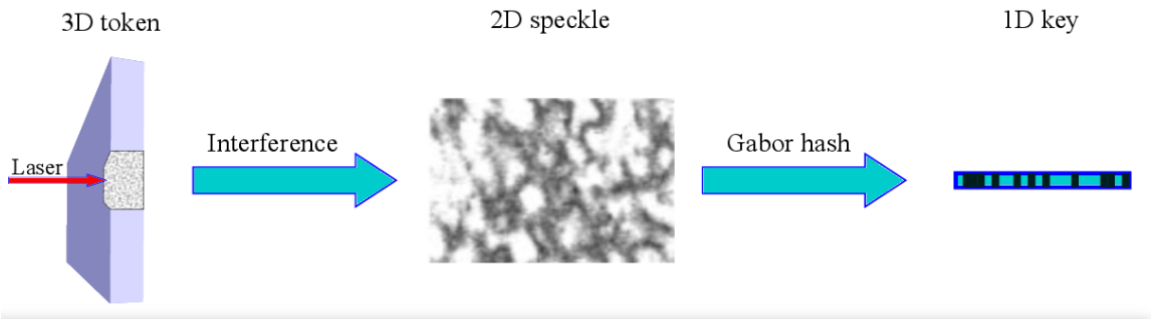
Αν και οι αλγοριθμικές μονόδρομες συναρτήσεις χρησιμοποιούνται ευρέως , αντιμετωπίζουν κάποιες προκλήσεις . Για παράδειγμα μια τέτοια πρόκληση είναι η τεχνολογική καθώς τεράστια παράλληλα δίκτυα υπολογιστών σπάνε κωδικούς που θεωρούνταν ασφαλείς και ασφαλείς επεξεργαστές που περιέχουν κλειδιά υπόκεινται σε αντίστροφη μηχανική . Μια άλλη πρόκληση είναι ότι δεν υπάρχει απόδειξη ότι δεν υπάρχουν αποτελεσματικές επιθέσεις που μπορούν να σπάσουν τις κρυπτογραφικές αρχές στις οποίες βασιζόμαστε και χρησιμοποιούμε για ασφάλεια. Τέτοιες επιθέσεις μπορούν να γίνουν με κβαντικούς υπολογιστές.

Η πιο σοβαρή όμως πρόκληση είναι πρακτική . Οι απαιτήσεις των φυσικών ενσωματώσεων των μονόδρομων συναρτήσεων από ενσωματωμένες εφαρμογές όπως οι έξυπνες κάρτες ξεπερνούν τους περιορισμούς κόστους και συσκευασίας της συμβατικής τεχνολογίας ημιαγωγών.

Όλα αυτά τα προβλήματα , μπορούν να αντιμετωπιστούν χρησιμοποιώντας **συνεκτική πολλαπλή σκέδαση** από ανομοιογενείς δομές παρά χρησιμοποιώντας τη θεωρία αριθμών για την υλοποίηση μονόδρομων συναρτήσεων .

3.3 Πείραμα

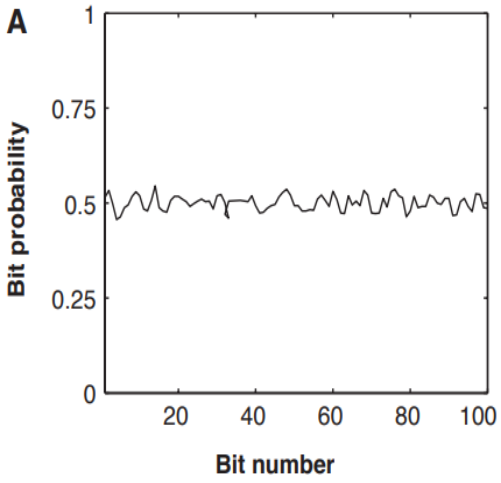
Στο ακόλουθο πείραμα (Pappu R. S., 2002) χρησιμοποιήθηκε ακτίνα laser HeNeμήκους κύματος λ = 632.8 nm για να φωτίσουμε οπτικά εποξειδικά tokens διαστάσεων 10 x 10 x 2.5 mm^3 που περιέχουν σφαίρες γυαλιού διαμέτρου 500-800 μm. Η πυκνότητα των σφαιρών επιλέχθηκε ώστε να δώσουν μια μέση απόσταση της τάξης των 100μm που ισούται με τη μέση ελεύθερη διαδρομή του φωτονίου στα όρια της υψηλής σκέδασης που θα εφαρμοστεί. Το μοτίβο κηλίδων που προέκυψε καταγράφηκε με φωτογραφική μηχανή συζευγμένου φορτίου 320 x 240 pixels . Τα tokens καταχωρήθηκαν μηχανικά με μια φθηνή κινηματική βάση , η οποία επιτρέπει ακρίβεια θέσης σε έξι βαθμούς ελευθερίας παρέχοντας επαναληψιμότητα του συστήματος εγγραφής . Τα μοτίβα κηλίδων στη συνέχεια φιλτράρονται από έναν μετασχηματισμό του Gabor για να παραχθούν κλειδιά μήκους 2400 bits.Ας δούμε αναλυτικά το σύστημα εγγραφής στην παρακάτω εικόνα:



Εικόνα 4: Η διαδικασία παραγωγής δυαδικής συμβολοσειράς ως απόκριση (P.Eder, 2023)[10]

Εδώ βλέπουμε τη βασική ιδέα . Μια τρισδιάστατη ανομοιογενής δομή κατακερματίζεται οπτικά για να μας δώσει μια δισδιάστατη εικόνα (μοτίβο κηλίδων) η οποία στη συνέχεια φιλτράρεται από έναν μετασχηματισμό Gabor πολλαπλών κλιμάκων για να μας δώσει ένα μονοδιάστατο κλειδί 2400 bits. (Αυτό το κλειδί θα λειτουργεί ως το μοναδικό χαρακτηριστικό όπως θα δούμε στη συνέχεια). Για να γίνει πιο κατανοητό σε επίπεδο αριθμών , ένας κύβος 1 cm^2 έχει περίπου 10^{12} κυβικά μπλοκ μήκους κύματος μεγέθους 1 μm^3 , που αντιστοιχεί σε 1terabit δομικής πληροφορίας . Η εικόνα διαστάσεων 320x240 pixels που βλέπουμε περιέχει πληροφορία έντασης της τάξεως του 1 megabit . Ο μετασχηματισμός Gabor το μειώνει σε ένα κλειδί 2400 bits.

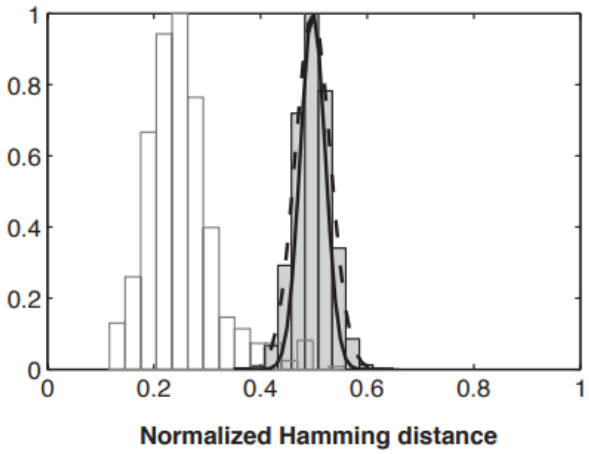
Για να εξετάσουμε πειραματικά τη συμπεριφορά της φυσικής μονόδρομης συνάρτησης (POWF) φτιάχτηκαν 4 tokens και καταγράφηκαν τα μοτίβα κηλίδων τους υπό 144 διαφορετικές γωνίες για κάθε token . Επομένως εύκολα καταλαβαίνουμε ότι 4 x 144 = 576 κλειδιά. Κατασκευάζοντας το διάγραμμα πιθανότητας κάθε ενός από τα bit στο κλειδί που φτιάχνεται βλέπουμε ότι η μέση πιθανότητα είναι περίπου 0.50 , πράγμα που μας δείχνει ότι επιτυγχάνουμε να έχουμε τη μέγιστη δυνατή εντροπία για τα bit μας.



Εικόνα 5: Διάγραμμα πιθανότητας για κάθε bit (Pappu R. S., 2002)[12]

Αυτό είναι πολύ καλό καθώς μας δείχνει την ανεξαρτησία κάθε bit από τα υπόλοιπα bits. Στην εικόνα βλέπουμε ενδεικτικά τα 100 πρώτα bits .

Ωστόσο υπάρχουν συσχετίσεις μεταξύ των bits. Στην παρακάτω εικόνα βλέπουμε τις αποστάσεις Hamming (ο αριθμός των bits που διαφέρουν , στο διάγραμμα το 1.0 αναπαριστά διαφορά και στα 2400 bits) μεταξύ αυτών των κλειδιών και μεταξύ των κλειδιών όταν ξαναμετρήθηκαν αφού είχαμε υποβάλει τα tokens σε routine handling.



Εικόνα 6 :Διαφορά αποστάσεων Hamming σε 2 μετρήσεις των κλειδιών (Pappu R. S., 2002)[12]

Η κατανομή 'ανόμοιων' κλειδιών (κλειδιών από διαφορετικά tokens)απεικονίζεται με γκρι χρώμα και δείχνει 165,600 αποστάσεις μεταξύ ανόμοιων κλειδιών .Ο μέσος όρος της διακεκομμένης είναι 0.50 (διαφέρουν τα μισά bit) και η απόκλιση είναι 1.07x 10^{-3}(περίπου 0.107 %) . Αν διπλασιάσουμε το μέγεθος του κλειδιού δηλαδή το κάνουμε 4800 bits κάνοντας ζευγάρια τα αποτελέσματα που πήραμε από 2 διαφορετικές γωνίες παράγεται η κατανομή που βλέπουμε από την συνεχόμενη καμπύλη , μειώνοντας έτσι την απόκλιση σε 5.42x 10^{-4} (0,0542 % περίπου δηλαδή υποδιπλάσια από πριν) . Η κατανομή 'όμοιων' κλειδιών που απεικονίζεται με άσπρο χρώμα δείχνει τα λάθη από το διάβασμα ξανά 576 όμοιων κλειδιών

μετά από routine handling των tokens. Ο μέσος όρος που είναι 0,25 σημαίνει ότι τα 1800 bits θα είναι τα ίδια και τα 600 θα διαφέρουν .

Η απόσταση Hamming στην οποία οι 2 κατανομές τέμνονται είναι στο 0.41 . Αν η κατανομή των ανόμοιων κλειδιών ήταν διωνυμική , αυτό θα σήμαινε 233 ανεξάρτητες πανομοιότυπα κατανεμημένες μεταβλητές. Αυτό δεν αλλάζει ακόμη και αν αφαιρέσουμε τα μισά κλειδιά , όπως και θα έπρεπε να συμβαίνει για ένα μέγεθος δεδομένων ικανό να κάνει εκτίμηση της κατανομής. Ως εκ τούτου , η μονόδρομη συνάρτηση μας δίνει θεωρητικά ένα χώρο κλειδιών της τάξεως του 2^{233} διακριτά κλειδιά.

Η επικάλυψη των κατανομών όμοιων και ανόμοιων κλειδιών μπορεί να γίνει όσο μικρή θέλουμε . Αυτό γίνεται αν διαβάσουμε κάθε token από περισσότερες από μία γωνίες καθώς κάθε γωνία μας δίνει ουσιαστικά ανεξάρτητη πληροφορία . Για να το δείξουμε αυτό , συνδυάσαμε πληροφορία από ζευγάρια γωνιών για να φτιάξουμε κλειδιά 4800 bits σε ένα σύνολο δεδομένων 82,800 εισόδων (οι μισές από ότι στην πρώτη περίπτωση) . Η κατανομή των αποστάσεων είχε τον ίδιο μέσο όρο (0.5) και μια απόκλιση 5.42 x 10^{-4} που σημαίνει 461 ανεξάρτητες μεταβλητές . Άρα διπλασιάζοντας το μέγεθος των κλειδιών που χρησιμοποιούμε σχεδόν διπλασιάζονται και οι ανεξάρτητες μεταβλητές που προκύπτουν .

Κανόνας επιλογής ή απόρριψης υποψηφίου token

Ο κανόνας που εφαρμόζεται για να αποφασίσουμε αν ένα token που τοποθετείται σε ένα τερματικό είναι το ίδιο με ένα που υπάρχει ήδη στη βάση δεδομένων είναι ο κανόνας ελάχιστης πιθανότητας . Σύμφωνα με αυτόν το token απορρίπτεται αν η πιθανότητα να είναι ίδιο με ένα της βάσης δεδομένων είναι μικρότερη ή ίση με την πιθανότητα να μην είναι ίδιο. Προσαρμόζοντας μια Gaussian συνάρτηση πυκνότητας πιθανότητας στις κατανομές αυτές , προκύπτει ότι ένα token θα απορρίπτεται αν τα κλειδιά διαφέρουν περισσότερο από 984 bits (0.41 x 2400) . Η πιθανότητα σύμφωνα με αυτά τα δεδομένα να υπάρξει ψευδής άρνηση του token είναι $9.8*10^{-3}$. Το ποσοστό αυτό μπορεί να μειωθεί εκθετικά αν πάρουμε μετρήσεις από διαφορετικές γωνίες .

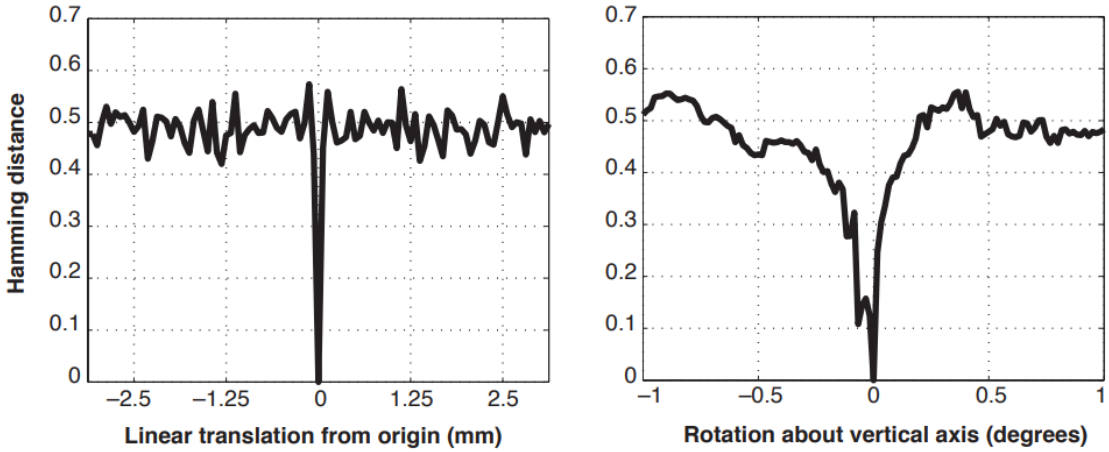
Αντίσταση σε παραβιάσεις

Όσον αφορά την αντίσταση σε παραβιάσεις έγινε ένα πείραμα . Με ένα τρυπάνι no.75 ανοίχτηκαν μικρές τρύπες μήκους 533μm και βάθους 1mm πάνω στο token . Τα κλειδιά που παρήχθησαν πριν και μετά από αυτή την παραβίαση παρουσίασαν μια απόσταση Hamming 0.46 που σημαίνει ότι σχεδόν τα μισά bit τους διέφεραν από τα αρχικά . Για να προστατέψουμε τα token από ακούσια ζημιά μπορούμε να τα περιβάλλουμε από ένα υλικό που τα προστατεύει από γρατσουνιές . Το ενδιαφέρον είναι ότι μπορούμε επίσης με τον μετασχηματισμό Gabor πολλαπλών κλιμάκων να απορρίπτουμε την πληροφορία που προήλθε από γρατσουνιές στην επιφάνεια ενώ παράλληλα κρατάμε την πληροφορία που προέρχεται από το εσωτερικό της μικροδομής.

Αντιγραφή του token

Μια άλλη ανησυχία είναι η δυνατότητα αντιγραφής του token μέσω κάποιων τεχνικών που καθορίζουν την τρισδιάστατη δομή των σκεδαστών . Όπως καταλαβαίνουμε , αλλαγή στη θέση του σκεδαστή μπορούν να προκαλέσουν σημαντικές αλλαγές στην έξοδο . Ακόμα και οι τεχνικές αυτές είναι πολύ μακριά από να μπορούν να αποδώσουν αυθαίρετα την παραμικρή λεπτομέρεια αλλά ακόμη και να μπορούσαν το κόστος είναι απαγορευτικό καθώς υπερβαίνει την αξία που προστατεύουν αυτά τα tokens ελέγχου ταυτότητας εξαρχής.

Μια εναλλακτική είναι να προσπαθήσουμε να αντιγράψουμε τη φυσική δομή του token και να προσπαθήσουμε να παράγουμε τη συμπεριφορά του ρίχνοντας αυθαίρετα φωτισμό πάνω του . Σύμφωνα με τη θεωρία , μια αλλαγή στη γωνία της τάξεως των $\delta\theta = 4x10^{-5}$ rad θα παράγει ένα ανεξάρτητο μοτίβο κηλίδων. Αν το εύρος των προσβάσιμων γωνιώνοριοθετείται από $\Delta\theta = \pi/2$ κατά μήκος της γωνίας εισόδου υπάρχει ένα σύνολο $\left(\frac{\Delta\theta}{\delta\theta}\right)^2 = 10^9$ διακριτών μοτίβων .Εφαρμόζοντας την δέσμη φωτός $1mm^2$ πάνω στην επιφάνεια $100mm^2$ του token πολλαπλασιάζει των αριθμό των μοτίβων κατά 100 καταλήγοντας σε 10^{11} διακριτά μοτίβα. Ο αριθμός αυτός των μοτίβων μπορεί να αυξηθεί κι άλλο αν αλλάξουμε το πλάτος , τη φάση και την κατανομή μήκους κύματος του φωτισμού . Αυτός ο αριθμός θα μειωθεί σε μικρό βαθμό από χωρικές συσχετίσεις που προκύπτουν στο μοτίβο κηλίδων και αφαιρούνται από τον κατακερματισμό . Στην εικόνα που ακολουθεί απεικονίζεται η μετρημένη ευαισθησία ενός κλειδιού υπό την εφαρμογή φωτός καθώς και περιστροφή του token .



Εικόνα 7: Ευαισθησία του κλειδιού σε μεταβολές του καθετήρα σε σχέση με το token (Pappu R. S., 2002)[12]

Στην αριστερή εικόνα απεικονίζεται η απόσταση Hamming μεταξύ ενός κλειδιού αναφοράς που αποκτήθηκε από κεντρική θέση και κλειδιών που αποκτήθηκαν κατά την γραμμική μετατόπιση του laser σε σχέση με την επιφάνεια του token .Παρατηρούμε ότι αρκεί μια μετατόπιση μόλις 60μm ώστε το κλειδί να αποσυσχετιστεί εντελώς . Όσον αφορά την γωνιακή ευαισθησία με περίπου 1.7mrad έχουμε πλήρη αποσυσχέτιση το κλειδιού επίσης.

Έτσι καταλήγουμε στο συμπέρασμα ότι από την επιφάνεια $100mm^2$του token μπορούμε να έχουμε 2.37 x 10^{10}κλειδιά με 2400 bit έκαστο . Αυτό το νούμερο προκύπτει αφαιρώντας τα κλειδιά που έχουν συσχετίσεις μεταξύ τους από το προηγούμενο νούμερο 10^{11}που είδαμε πιο πάνω που είναι θεωρητικά ο συνολικός αριθμός κλειδιών που μπορούμε να έχουμε .

Επίθεση επανάληψης

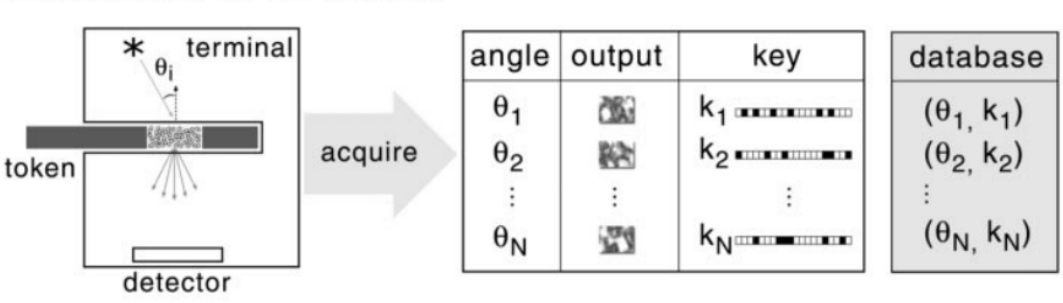
Λόγω του ότι η οπτική έξοδος ανιχνεύεται σαν μια ασυνάρτητη εικόνα που μετά χρησιμοποιείται για να παράγει το κλειδί , κάποιος που θα είχε πρόσβαση στο τερματικό θα μπορούσε να διαβάσει το εισερχόμενο ερώτημα και στη συνέχεια να απαντήσει από έναν πίνακα αποκτηθέντων κλειδιών . Αυτό λέγεται επίθεση επανάληψης . Το πρόβλημα με αυτό είναι κυρίως θέμα χωρητικότητας . Με 10^{11} δυνατές ερωτήσεις και υποθέτοντας ότι το κλειδί

έχει μόνο 1000bit και όχι 2400 bit σημαίνει ότι για να αποθηκεύσουμε όλες τις πιθανές μετρήσεις χρειαζόμαστε 10^{14} bit μνήμης .

Παρόλο που η φυσική δομή από μόνη της δεν περιέχει τόσο μεγάλη πληροφορία , αν ο όγκος του token είναι της τάξεως ενός κυβικού εκατοστού $1cm^3$ και ρίξουμε πάνω του φως με μήκος κύματος της τάξεως του 1μm τότε φτάνουμε μέχρι και τα 10^{12}(10^{-2}/10^{-6}) bits καθώς στους μικροσκοπικούς ανομοιογενείς σκεδαστές η σύσταση κάθε κυβικού μπλοκ του μεγέθους του μήκους κύματος είναι τυχαία. Αυτά τα bit θα μπορούσαν να χρησιμεύσουν για να προσομοιώσουμε υπολογιστικά την έξοδο αντί να προ αποθηκεύουμε όλες τις πιθανές εξόδους. Αν δούμε μεσοσκοπικά ένα φωτόνιο που περνά μέσα από μια δομή εκτελεί έναν τυχαίο περίπατο . Για να καταφέρει το φωτόνιο να βγει από το token θα πρέπει να κάνει κάποια συγκεκριμένα βήματα που υπολογίζονται βάσει του μέσου όρου ελεύθερου μονοπατιού *l* , καλύπτοντας μια απόσταση $l\sqrt{N}$ όπου *N* το νούμερο των γεγονότων σκέδασης και το πάχος *L* του token .Για να βγει το φωτόνιο από το πάχος *L* θα πρέπει $L= l\sqrt{N}$ και άρα N = $(L / l)^2$. Στην περίπτωση μας ο αριθμός αυτός είναι 625 βήματα . Σε κάθε βήμα στην προσομοίωση θα πρέπει να διαδώσουμε ευθεία μονοπάτια που συνδέουν όλα τα ζεύγη σκεδαστών , πράγμα που μας δίνει ένα σύνολο 10^{26} λειτουργιών . Δηλαδή η προσομοίωση της σκέδασης ακόμη και από ένα μόνο αυθαίρετο σχήμα σωματιδίου σε σημείο που η διάσταση του είναι πολλές φορές το μήκος κύματος του είναι ανέφικτη χωρίς έναν υπερυπολογιστή.

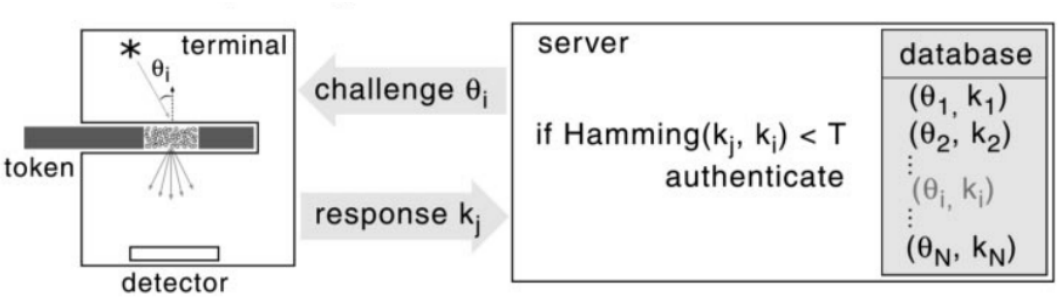
Οι προηγούμενες προσεγγίσεις αποδεικνύονται ανέφικτες καθώς ο χώρος τον πιθανών ζευγαριών εισόδου με τα κλειδιά εξόδου είναι τεράστιος . Αυτό μπορεί να θεωρηθεί ως μια λειτουργική αντιστοίχιση που παράγει μια απόκριση σε μια πρόκληση που καθορίζει τις παραμέτρους του φωτισμού .

Σε αντίθεση όμως με άλλα πρωτόκολλα του είδους εδώ ο όγκος πληροφορίας είναι τεράστιος και δεσμεύεται στο token εκ των προτέρων . Αυτή η πληροφορία μπορεί να χρησιμοποιηθεί για να διαβαστεί το token σε ένα μη ασφαλές τερματικό που είναι υπό τον έλεγχο ενός μη εξουσιοδοτημένου χρήστη. Αρχικά ,όταν διαβάσουμε το token στο ασφαλές τερματικό αποκτώνται πολλά ζευγάρια φωτισμού-κλειδιού και αποθηκεύονται σε ασφαλές μέρος .



Εικόνα 8: Στάδιο εγγραφής (Pappu R. S., 2002)[12]

Αν μετά γίνει αίτημα ταυτοποίησης από μη ασφαλές τερματικό μπορούμε να το προκαλέσουμε με ένα ζευγάρι από τα προ αποθηκευμένα και να ζητηθεί να παράγει ένα κλειδί .



Εικόνα 9: Στάδιο επαλήθευσης (Pappu R. S., 2002)[12]

Επειδή όμως το ζευγάρι αυτό είναι αποθηκευμένο μόνο στο ασφαλές τερματικό , ο μόνος τρόπος να μπορέσει να παράγει το κλειδί είναι να έχει φυσική πρόσβαση στο token. Αφού το ζευγάρι χρησιμοποιείται μία φορά δεν υπάρχει πρόβλημα η πρόκληση και η απόκριση να σταλθούν μέσω ενός δημοσίου καναλιού .Η παραγωγή του κλειδιού καθιερώνει ένα κοινό μυστικό μεταξύ του ασφαλούς μέρους που αναφέρθηκε πάνω και του κατόχου του token . Η ασφάλεια του συγκεκριμένου συστήματος βασίζεται στην αδυναμία αποθήκευσης όλων των ζευγαριών φωτισμού-κλειδιού. Επειδή μπορούμε να πειράξουμε τις παραμέτρους του φωτισμού όπως το μήκος κύματος ,η θέση και ο προσανατολισμός του laser οδηγούμαστε σε ένα μαθηματικά τεράστιο χώρο , που εξακολουθεί να είναι γραμμικός στους βαθμούς ελευθερίας της εισόδου επειδή τα ανεξάρτητα μοτίβα φωτισμού προστίθενται γραμμικά και άρα μπορούν να επεκταθούν . Αν χρησιμοποιηθεί όμως ένα μη γραμμικό μέσο σκέδασης που διεγείρεται με μια διαδικασία 2 φωτονίων αυτός ο χώρος μπορεί να γίνει εκθετικά μεγάλος . Ο αριθμός αυτών των μοτίβων είναι εκθετικός κατά$\left(\frac{L}{l}\right)^3$ και όπως γίνεται αντιληπτό ξεφεύγει από τα τεχνολογικά όρια.

Στην πάνω περίπτωση , προϋπόθεση είναι το token και το τερματικό να είναι διακριτά . Το μέσο σκέδασης όμως μπορεί να είναι ενσωματωμένο σε ένα μεγαλύτερο σύστημα για επαλήθευση της ταυτότητας του συστήματος. Επιπλέον θα μπορούσε να χρησιμοποιηθεί για την ενθυλάκωση βασικών στοιχείων που προστατεύουν από παραβιάσεις . Η μόνη μυστική πληροφορία που απαιτείται δηλαδή το ζευγάρια φωτισμού-κλειδιού αποθηκεύονται σε απομακρυσμένο ασφαλές μέρος . Άρα σε αντίθεση με τα υπάρχοντα chips που προστατεύουν από παραβιάσεις , οι λειτουργίες μιας POWF μπορούν να είναι φανερές.

Με τη χρήση πολύπλοκων φυσικών δομών για έλεγχο ταυτότητας δείξαμε ότι η συνεκτική πολλαπλή σκέδαση ικανοποιεί όλα τα χαρακτηριστικά μιας μονόδρομης συνάρτησης με θόρυβο . Η τεράστια διαφορά του όγκου πληροφορίας που είναι διαθέσιμη σε τέτοιες δομές και της πληροφορίας που πραγματικά χρησιμοποιείται μας δίνει τη δυνατότητα να χρησιμοποιούμε αυτό το μεγάλο χώρο σαν σημειωματάριο μιας χρήσης που παράγεται όταν χρειάζεται. Μεγάλη χρησιμότητα έχει ένα τέτοιο σύστημα όταν είναι ενσωματωμένο ως πρωτόγονο σε ένα μεγαλύτερο κατανεμημένο σύστημα κρυπτογραφίας που βλέπει τη φυσική αλληλεπίδραση σαν ένα μέρος του συνολικού υπολογισμού που διακρίνεται από την ταχύτητα που μπορεί να μετατρέψει τεράστιο όγκο πληροφορίας με πολύ χαμηλό κόστος.

Συμπέρασμα:

Σε μια προσπάθεια να αντιμετωπιστούν οι προκλήσεις που αντιμετωπίζουν οι σύγχρονες αλγοριθμικές μονόδρομες συναρτήσεις κατακερματισμού , προτείνεται η χρήση συνεκτικής πολλαπλής σκέδασης από ανομοιογενείς δομές για την υλοποίηση μονόδρομων συναρτήσεων. Πειραματικά βλέπουμε ότι μπορούμε να έχουμε πολύ χαμηλή πιθανότητα

ψευδώς αρνητικών/θετικών αν διαβάσουμε από πολλές γωνίες τα token με πολύ μικρές αποκλίσεις. Επίσης η αντιγραφή κρίνεται απαγορευτικά δύσκολη .Η ευαισθησία είναι αρκετά υψηλή .Ακόμα , οι επιθέσεις επανάληψης δεν κρίνονται αποδοτικές και αυτό οφείλεται σε θέματα κυρίως χωρητικότητας. Η ασφάλεια αυτού του σχήματος βασίζεται στο ότι είναι ανέφικτο να δημιουργήσουμε την μικροδομή ενός μακροσκοπικού αντικειμένου σε επίπεδο μήκους ατόμου . Έτσι αντί να βασίζεται σε εικασίες γύρω από τη θεωρία των αριθμών , αυτή η προσέγγιση βασίζεται στους τεχνολογικούς περιορισμούς που ενώ δεν έχουν θεωρητική βάση , παρουσιάζουν τρομακτικές προκλήσεις σε έναν αντίπαλο .

Κεφάλαιο 4: Physical Unclonable Functions με χρήση πολύτροπου οπτικού κυματοδηγού

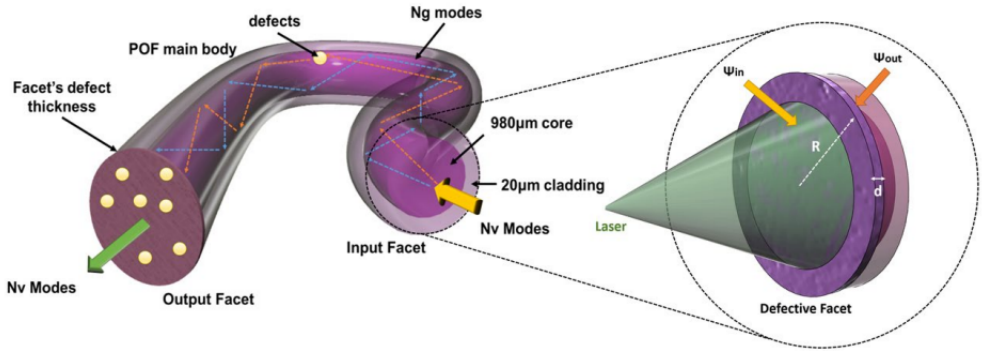
Ο φυσικός μηχανισμός των οπτικών PUFs βασίζεται στο μοτίβο τυχαίας παρεμβολής που δημιουργείται όταν η δέσμη φωτός του laser περνά από ένα ανομοιογενές υλικό. Οι περισσότερες υλοποιήσεις χρησιμοποιούν διαφανή tokens που περιέχουν τυχαίες μικροδομές , δείγματα χαραγμένα με laser ή ακόμα και κανονικά φύλλα χαρτιού. Ότι και αν χρησιμοποιούν όμως το κοινό είναι ότι η ασφάλεια βασίζεται στην πολυπλοκότητα του φυσικού μηχανισμού . Αυτό τα καθιστά αρκετά ασφαλέστερα σε επιθέσεις μοντελοποίησης σε αντίθεση με τα αντίστοιχα ηλεκτρονικά PUFs. Τα περισσότερα οπτικά PUFs έχουν ως κύριο πρόβλημα το αυξημένο αποτύπωμα που αφήνουν και θεωρούνται συνεπώς ευάλωτα σε επιθέσεις μηχανικής μάθησης . Με τέτοιες επιθέσεις μπορεί ένας αντίπαλος να αποκτήσει έλεγχο στις αποκρίσεις και στις αντίστοιχες προκλήσεις . Εκμεταλλευόμενος αυτό , μπορεί να αποκτήσει πρόσβαση στη συνάρτηση μεταφοράς (TF) . Στην πλειονότητα των οπτικών PUFs αυτό συμβαίνει λόγω της γραμμικότητας της διαδικασίας σκέδασης.

Επεξήγηση της προτεινόμενης υλοποίησης

Λύση μπορεί να δώσει μια καινοτόμα εναλλακτική οπτική διαμόρφωση PUF που βασίζεται σε ένα οπτικό κυματοδηγό σαν μοναδικό φυσικό token του PUF . Οι δομικές παράμετροι αυτού του προτεινόμενου PUF επιλέγονται ώστε να επιτρέπουν τη διέγερση και την αποτελεσματική καθοδήγηση μεγάλου αριθμού εγκάρσιων τρόπων κυματοδήγησης. Ο φυσικός μηχανισμός εκτός από τη σκέδαση περιλαμβάνει ευαίσθητους πολύτροπους μηχανισμούς παρεμβολής και βλάβες κατά τη διάδοση στην ίνα . Επειδή αυτά τα χαρακτηριστικά το κάνουν δομικά ευαίσθητο , είναι και λιγότερο πιθανό να κλωνοποιηθεί . Παράλληλα είναι εφικτή η φυσική επαναδιαμόρφωση. Αυτή η προτεινόμενη αρχή λειτουργίας περιλαμβάνει πολλές διεπαφές που καθιστούν τη φυσική τους αντιγραφή και αναπαραγωγή πιο δύσκολη σε σχέση με τις συμβατικές προσεγγίσεις . Αυτά τα πλεονεκτήματα σε συνδυασμό με τις ίδιες περίπου απαιτήσεις κόστους συγκριτικά με συμβατικά οπτικά PUFs το καθιστούν μια πολύ καλή λύση . Μπορεί να αντικαταστήσει τα οπτικά PUF που χρησιμοποιούνται για έλεγχο ταυτότητας όπως και θα δούμε παρακάτω.

Όλη η ουσία αυτής της προτεινόμενης υλοποίησης βρίσκεται στον οπτικό κυματοδηγό δηλαδή στην περίπτωση μας σε μια πολυμερή ή πλαστική οπτική ίνα που μας επιτρέπει να έχουμε μεγαλύτερο αριθμό οπτικών εγκάρσιων τρόπων κυματοδήγησης. Η ίνα δρα ταυτόχρονα ως οπτικός κυματοδηγός και ως οπτικό token σκέδασης . Το token χωρίζεται σε τρία εικονικά τμήματα .

Το πρώτο είναι η όψη εισόδου της ίνας (facet) που αποτελείται από έναν αριθμό τυχαίων δομικών ατελειών όπως γρατσουνιές , ακαθαρσίες , διαθλαστικές ανωμαλίες . Αυτές οι ατέλειες προκύπτουν σκόπιμα , όπως η μηχανική τριβή που προκαλείται από θόρυβο και συνδυάζονται με τυχαίες κατασκευαστικές ατέλειες. Με δεδομένο ότι η επιφάνεια εισόδου της οπτικής ίνας παρουσιάζει δομικές ατέλειες με πάχος (d) μεγαλύτερο του μήκους κύματος φωτισμού (λ) και μικρότερο της μέσης ελεύθερης διαδρομής των φωτονίων (l) , την αντιμετωπίζουμε ως οπτικό διαχυτή και θεωρούμε ότι οι στατιστικές της ιδιότητες μπορούν να διαμορφωθούν μαθηματικά σαν μια μίξη τυχαίων διαδρομών των φωτονίων. Σύμφωνα με τη θεωρία , μπορούν να προκύψουν $N_v = \frac{2\pi A}{\lambda^2}$ ανεξάρτητοι τρόποι διάδοσης και αυτό εξαρτάται από το μέγεθος της όψης της ίνας (A) . Οπότε υπολογίζεται περίπου στουςN_v= 2.05 x 10^6 τρόπους θεωρώντας ότι η διάμετρος είναι 1 mm και το μήκος κύματος λ=1550nm . Λόγω του περιορισμένου πάχους , οι περισσότεροι από αυτούς τους τρόπους δεν θα εξασθενήσουν (δεν θα έχουν απώλειες διάδοσης καθώς η διαδρομή είναι πολύ μικρή) και θα μεταφέρουν ενέργεια στην άλλη πλευρά της όψης (Ψ_{out}) , δηλαδή στην διεπαφή πυρήνα – επένδυσης.



Εικόνα 10: Το σχήμα της προτεινόμενης υλοποίησης (Charis Mesaritakis, 2018)[3]

Η βασική αρχή είναι ότι κάθε εξερχόμενος τρόπος αποσυντίθεται σε ένα γραμμικό συνδυασμό όλων των εισερχόμενων τρόπων .

$$\Psi^j{}_{out} = \sum_{i=1}^{N} T_{i,j}\,\Psi^i$$

Όπου $T_{i,j}$ο πίνακας σκέδασης της ελαττωματικής εισόδου της ίνας. Στην ιδανική περίπτωση , η συνάρτηση μεταφοράς TF του διαχυτή περιέχει $N_v x N_v$ στοιχεία που αντιστοιχούν στη φυσική πολυπλοκότητα . Σε αυτό το PUF η κατανομή των τρόπων δεν μπορεί να παρακολουθηθεί ικανοποιητικά όπως σε ένα τυπικό οπτικό PUF ακόμη και με εξελιγμένες τεχνικές .

Επιπλέον , αυτοί οι αρχικοί τρόποι θα έρθουν σε επαφή με τις οριακές συνθήκες από τη διεπαφή της επένδυσης της ίνας και του πυρήνα . Επομένως κάποιοι από αυτούς δεν θα υποστηρίζονται λόγω του αριθμητικού διαφράγματος NA (numerical aperture). Αυτή η διαδικασία φιλτραρίσματος οδηγεί σε ένα άνω όριο το οποίο υπολογίζεται από :

$$N_g =$$

Όπου R η ακτίνα της ίνας . Χρησιμοποιώντας R=0.5 , NA = 0.5 , λ=1540nm) υπολογίζουμε το $N_g < 2.510^5$. Αν συγκρίνουμε αυτό το νούμερο με το N_v = 2.05 x 10^6 συμπεραίνουμε ότι η διεπαφή όψης ίνας οδηγεί σε ένα φιλτράρισμα του 87% των τρόπων , σε σύγκριση με ένα λεπτό οπτικό διαχυτή στην περίπτωση του οποίου σχεδόν όλοι οι τρόποι εξέρχονται από το υλικό . Τα παραπάνω μας δίνουν εικόνα για το άνω όριο σχετικά με τον αριθμό των υποστηριζόμενων τρόπων εντός της ίνας . Ωστόσο υπεύθυνες για τον αριθμό τον τρόπων που θα διεγερθούν αλλά και για την κατανομή της ισχύος ανάμεσα τους είναι οι συνθήκες φωτισμού. Οπότε αν οι παράμετροι του laser μείνουν σταθερές , η αρχική κατανομή στους τρόπους εξαρτάται από τις ατέλειες της όψης και τις συνθήκες ορίων στην ίνα.

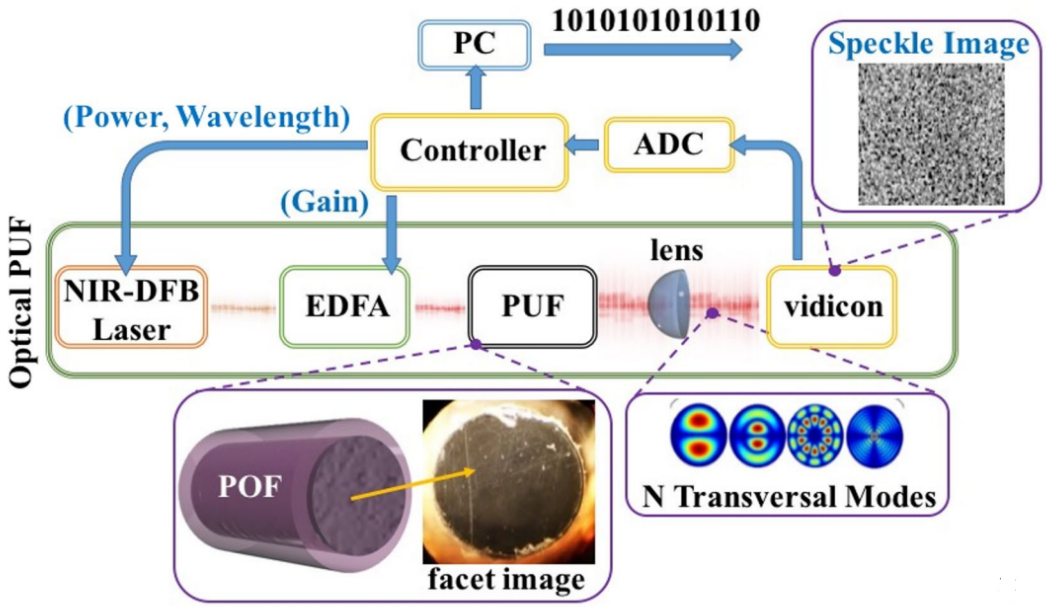
Το δεύτερο τμήμα αποτελείται από το κύριο σώμα της οπτικής ίνας μέσα στο οποίο οι υποστηριζόμενοι τρόποι κυματοδήγησης θα διαδοθούν με το ίδιο μήκος κύματος αλλά με διαφορετικές ταχύτητες. Η διάδοση μέσω της οπτικής ίνας επηρεάζει την αρχική κατανομή ανακατεύοντας ξανά την ισχύ των τρόπων διάδοσης ή διεγείροντας νέους τρόπους. Αυτός ο φυσικός μηχανισμός αποδίδεται σε μηχανικές παραμορφώσεις ή κοινές ατέλειες μέσα στην ίνα που προκύπτουν κατά τη διαδικασία παραγωγής της. Τέτοιες είναι η διακύμανση του δείκτη διάθλασης ή μικρορωγμές. Έτσι θα επηρεαστεί το χωρικό προφίλ του κάθε τρόπου και θα προκληθούν συζεύξεις πολλών τρόπων κυματοδήγησης. Αυτά τα φαινόμενα μέσα στην ίνα δεν μπορούν να ελεγχθούν διεξοδικά χωρίς να αλλοιώσουμε τη φυσική δομή . Το PUF θα πρέπει να είναι μικρό σε μήκος ώστε αυτές οι ατέλειες να μην επηρεάσουν την αρχική κατανομή της ισχύος στους τρόπους και αρχίσουν και συγκλίνουν πάλι σε μία ισορροπία ισχύος .

Το τρίτο τμήμα είναι η έξοδος της ίνας που ομοίως με την είσοδο έχει έναν τυχαίο αριθμό δομικών ατελειών μεγέθους μήκους κύματος ή μεγαλύτερες , ικανές να διασκορπίσουν τους τρόπους οπτικής κυματοδήγησης . Η έξοδος της ίνας φωτίζεται από το καθοδηγούμενο οπτικό πεδίο ώστε οι N_v τρόποι που έρχονται να διεγείρονται και να στείλουνN_vτρόπους στην έξοδο. Λειτουργεί δηλαδή ως οπτικός διαχυτής . Ο αριθμός των τρόπων εξαρτάται μόνο από την επιφάνεια της ίνας. Έτσι το τελευταίο αυτό κομμάτι του PUF επεκτείνει τον αριθμό των εγκάρσιων τρόπων N_vσε έναν παρόμοιο με ένα λεπτό τυπικό οπτικό διαχυτή. Επομένως , ο συνολικός πίνακας μεταφοράς του PUF θα έχει μέγεθος $N_v x N_v$που με τη σειρά του εξαρτάται από τη διατομή του κυματοδηγού και το μήκος κύματος εισόδου.

Οι τρόποι που διαδίδονται δηλαδή μέσα στην ίνα έχουν μια αρχική κατανομή ισχύος και όσο διαδίδονται μέσα στην ίνα ανταλλάσσουν ισχύ εξαιτίας εσωτερικών ατελειών και φωτίζουν την όψη εξόδου που με τη σειρά της λειτουργεί ως δεύτερος διαχυτής . Είναι προφανές ότι η απόκριση του συστήματος είναι το μοτίβο κηλίδων που παρατηρείται μετά την έξοδο από την ίνα.

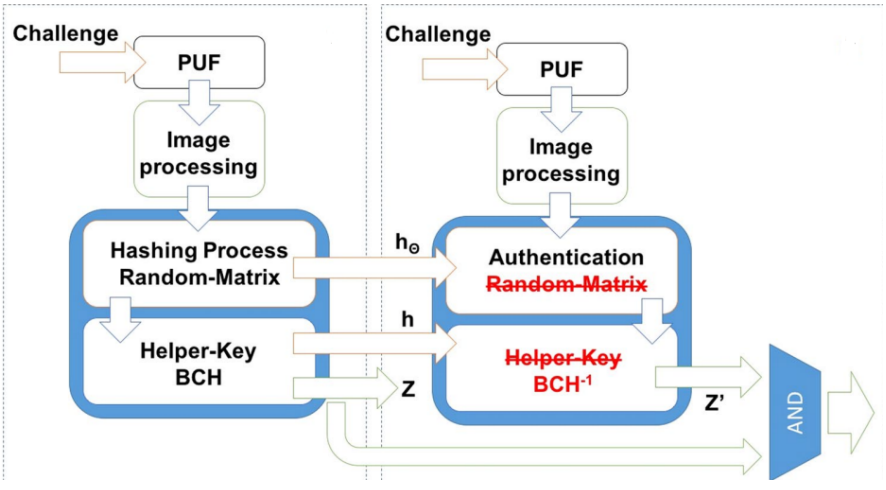
Πειραματικές ρυθμίσεις

Στον πυρήνα αποτελείται από ένα μικρό κομμάτι μιας κλασσικής εμπορικής οπτικής ίνας που χρησιμοποιείται ως δείγμα PUF. Οι προκλήσεις παράγονται από ένα laser και οι όψεις της ίνας παρουσιάζουν ατέλειες .



Εικόνα 11: Διάγραμμα του πειράματος (Charis Mesaritakis M. A., 2018)[3]

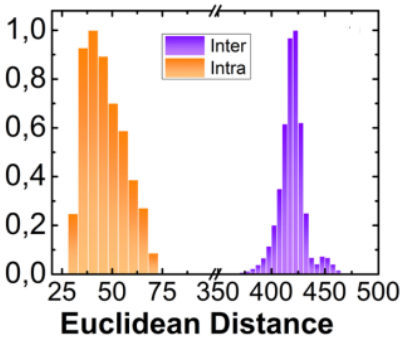
Θέλοντας να τροποποιήσουμε την επιζήμια επίδραση του θορύβου ώστε να παράγουμε χρονικά αμετάβλητες δυαδικές συμβολοσειρές , η ακατέργαστη έξοδος του PUF επεξεργάζεται από τεχνικές ασαφούς εξαγωγής ταυτόχρονα με προσεγγίσεις κατακερματισμού όπως η μέθοδος random binary hashing και η μέθοδος Gabor hashing. Η διαδικασία έχει ως εξής . Κάνουμε δειγματοληψία σε τυχαία pixels της εικόνας και στην περίπτωση της μεθόδου random binary hashing , πολλαπλασιάζονται με ένα πίνακα που παρουσιάζει τυχαία κανονική κατανομή και στη συνέχεια κβαντίζονται χρησιμοποιώντας το μέσο όρο έντασης της εικόνας. Ομοίως , στην περίπτωση της μεθόδου Gabor hashing , εφαρμόζεται επεξεργασία που περιέχει φίλτρα Gabor και επιλέγονται οι συντελεστές Gabor αντί για ακατέργαστα pixel της εικόνας . Αυτά τα δεδομένα μπορούν να χρησιμοποιούνται για ταυτοποίηση σαν κλειδιά ταυτοποίησης όταν χρησιμοποιείται το PUF .



Εικόνα 12: Διαδικασία παραγωγής κλειδιού και ταυτοποίηση

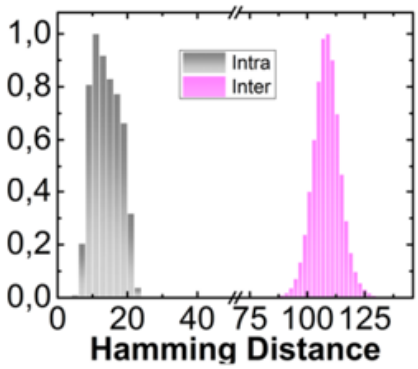
Πειραματικά αποτελέσματα

Η πρώτη μέτρηση για την αποτελεσματικότητα του συστήματος απέναντι σε καλοπροαίρετους κατασκευαστές είναι οι ευκλείδιες αποστάσεις μεταξύ των εικόνων από κάθε dataset. Στην περίπτωση του πρώτου dataset(intra-distance με πορτοκαλί χρώμα)εκτιμάται η επίδραση του θορύβου ενώ στην περίπτωση του δευτέρου dataset από 1000 διαφορετικά αντικείμενα του PUF εκτιμάται η μεταβλητότητα των αποκρίσεων του PUF (inter-distance με μπλε). Η μέση τιμή της intra-distance υπολογίστηκε 40.5 ενώ η μέση τιμή inter-distance υπολογίστηκε 422.5 . Αυτή είναι μια αρκετά μεγάλη διαφορά που μας επιτρέπει μαζί με την μηδενική επικάλυψη (οι κατανομές δεν έχουν κοινά σημεία) μεταξύ των 2 κατανομών να είμαστε σίγουροι ότι 2 διαφορετικά στιγμιότυπα δεν θα θεωρηθούν ψευδώς το ίδιο λόγω του θορύβου .



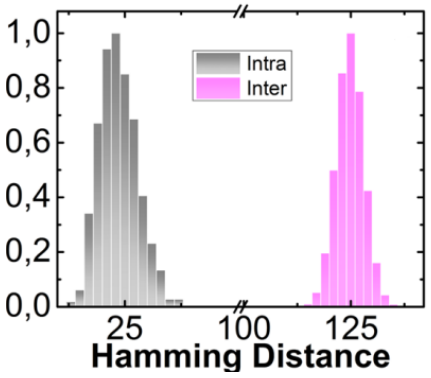
Εικόνα 13: Ευκλείδιες αποστάσεις για κανονικοποιημένες ακατέργαστες αποκρίσεις (εικόνες 8bit) (Charis Mesaritakis M. A., 2018)[3]

Η δεύτερη μέτρηση είναι η απόσταση Hamming μεταξύ των δυαδικών συμβολοσειρών που παρήχθησαν από κάθε απόκριση χρησιμοποιώντας είτε Random binary hashing είτε Gabor binary hashing. Οι δυαδικές συμβολοσειρές έχουν μήκος 255 bits. Η τεχνική Gabor hashing απαιτεί χωρικό φιλτράρισμα της εικόνας σε αντίθεση με την Binary hashing που δεν είναι υπολογιστικά απαιτητική . Το γκρι dataset (intra)μας δείχνει πόσα bits αλλοιώθηκαν λόγω θορύβου ενώ το μωβ dataset (inter) μας δείχνει πόσα bits αλλοιώθηκαν λόγω κατασκευαστικών παραλλαγών. Εφαρμόζοντας binary hashing, στην περίπτωση intra ο μέσος όρος των αλλοιωμένων bits είναι 13.7 $\pm$3.9 (5.3% $\pm$ 1%) ενώ στην inter107.8 $\pm$4.9 (42.2% $\pm$ 2%) .



Εικόνα 14: Αποστάσεις Hamming για ζευγάρια κωδικών λέξεων χρησιμοποιώντας Random Binary Hashing (Charis Mesaritakis M. A., 2018)[3]

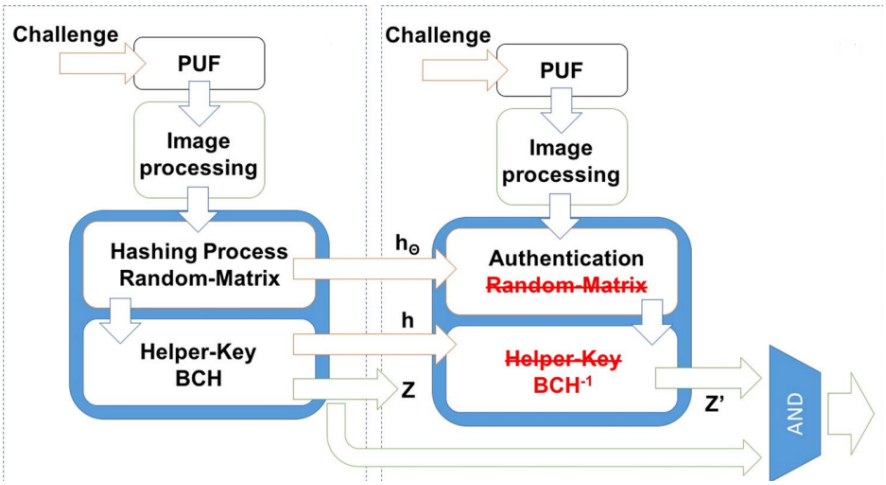
Εφαρμόζοντας Gabor hashing οι τιμές intra και inter είναι 25(9.8%) και 125(49%) αντίστοιχα. Αυτή η αύξηση των αλλοιωμένων bits σε σχέση με το Binary Hashing οφείλεται στην συντελεστή Gabor που επιλέχθηκε κατά το hashing .



Εικόνα 15: Αποστάσεις Hamming για ζευγάρια κωδικών λέξεων χρησιμοποιώντας χωρικό χωρικό φιλτράρισμα Gabor (Charis Mesaritakis M. A., 2018)[3]

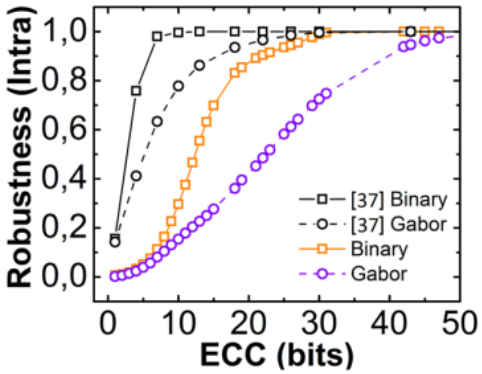
Η σημαντική παρατήρηση που κάνουμε εδώ , είναι ότι σε καμία από τις 2 μεθόδους hashing δεν υπάρχει επικάλυψη των κατανομών . Αυτό ελαχιστοποιεί την πιθανότητα ψευδώς θετικών.

Κάθε συνδυασμός PUF-challenge από το πρώτο σύνολο δεδομένων (ίδια πρόκληση σε ίδιο PUF) χρησιμοποιείται για την παραγωγή της δυαδικής συμβολοσειράς και των αντίστοιχων βοηθητικών δεδομένων (helper data).



Όπως είδαμε στην εικόνα 12, αυτές οι έξοδοι τώρα τροφοδοτούνται στο σύστημα που είναι σε λειτουργία ελέγχου ταυτότητας επιτρέποντας τη δημιουργία μιας νέας κωδικής λέξης z' . Η δυνατότητα διόρθωσης σφαλμάτων καθορίζει και την πιθανότητα το z να διαφέρει απτο z' .

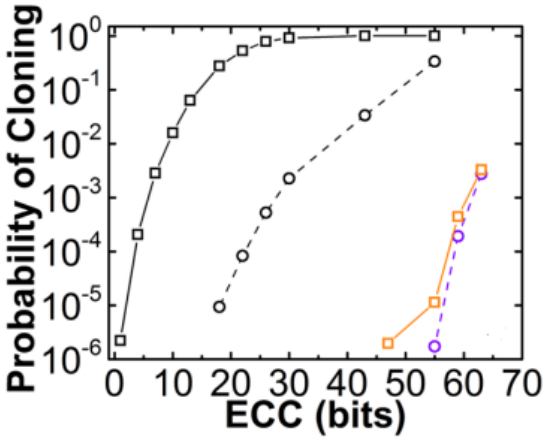
Έτσι μπορούμε να χαρακτηρίσουμε την απόδοση ενός συστήματος . Για να καταλάβουμε την χρησιμότητα του συστήματος θα το συγκρίνουμε με ένα τυπικό οπτικό PUF ως προς τη απόδοση .



Εικόνα 16: Διάγραμμα ευρωστίας της προτεινόμενης υλοποίησης με Random Binary και Gabor Hashing συναρτήσει του αριθμού των ECC bits (Charis Mesaritakis M. A., 2018)[3]

Το τυπικό οπτικό PUF όπως φαίνεται έχει καλύτερη απόδοση από το προτεινόμενο σχέδιο είτε χρησιμοποιηθεί η μέθοδος random binary hashing είτε η μέθοδος Gabor binary hashing .Όπως βλέπουμε , σε ένα τυπικό οπτικό PUF χρησιμοποιώντας Random Binary hashing χρειαζόμαστε 10 ECC bits ενώ για την υλοποίηση με τους πολύτροπους οδηγούς χρειαζόμαστε 30 ECC bits για να πετύχουμε την ίδια απόδοση . Εκ πρώτης αυτό φαίνεται ότι δίνει προβάδισμα στο τυπικό οπτικό PUF . Όμως αυτές οι μέθοδοι επηρεάζουν και την ποικιλομορφία των αποκρίσεων του PUF επομένως δεν μπορούμε να κρίνουμε μόνο με τη μία μέτρηση αλλά πρέπει να λάβουμε υπόψιν και τις αποκρίσεις .

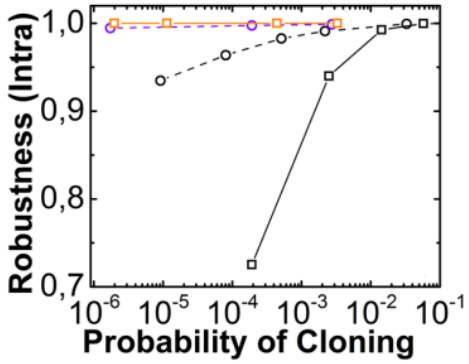
Το δεύτερο σύνολο δεδομένων χρησιμοποιείται για την εκτίμηση της πιθανότητας κλωνοποίησης . Σε αυτή την περίπτωση από κάθε PUF παράγεται ένα δυαδικό κλειδί αλλά και τα βοηθητικά δεδομένα . Αυτά τα δεδομένα τροφοδοτούνται σε κάθε ένα από τα άλλα PUFs που είναι σε διαδικασία ελέγχου ταυτότητας .Έτσι υπολογίζεται η πιθανότητα ενός false negative σε σχέση με τις δυνατότητες διόρθωσης σφαλμάτων .



Εικόνα 17: Διάγραμμα πιθανότητας κλωνοποίησης των κωδικών λέξεων μήκους 255 bits συναρτήσει του αριθμού ECC bits (Charis Mesaritakis M. A., 2018)[3]

Στην εικόνα βλέπουμε την πιθανότητα κλωνοποίησης και για τις 2 υλοποιήσεις συναρτήσει των απαιτούμενων ECC bits και για τις 2 μεθόδους hashing . Η υλοποίηση μας έχει προφανώς μεγαλύτερη βελτίωση . Όπως βλέπουμε μέχρι τα 44 ECC bits η πιθανότητα κλωνοποίησης είναι αμελητέα (10^{-6})για τη μέθοδο Random binary hashing και αντίστοιχα μέχρι τα 55 ECC bits για τη μέθοδο Gabor hashing . Για λιγότερα ECC bits η πιθανότητα υπολογίζεται στο 0 .

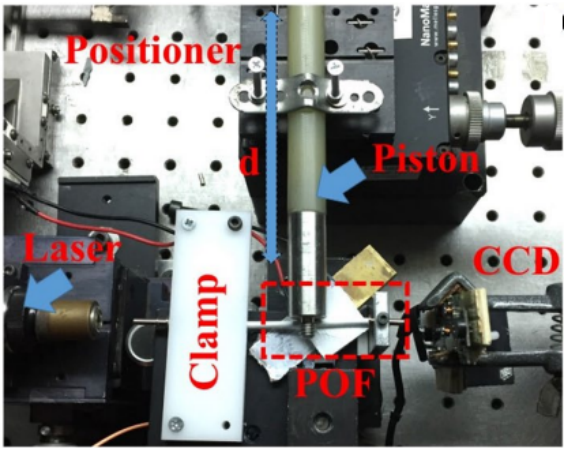
Για να γίνει συνολικά πιο κατανοητό παρουσιάζεται η κάτω εικόνα στην οποία απεικονίζεται η δύναμη του συστήματος συγκριτικά με την πιθανότητα κλωνοποίησης και για τις 2 υλοποιήσεις και τις 2 μεθόδους για κάθε υλοποίηση .



Εικόνα 18: Διάγραμμα ευρωστίας συναρτήσει της πιθανότητας κλωνοποίησης (Charis Mesaritakis M. A., 2018)[3]

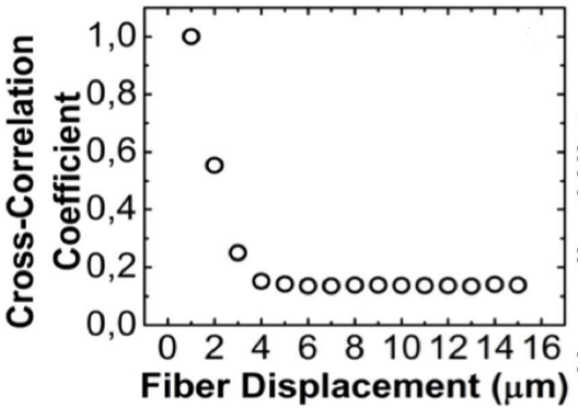
Τα αποτελέσματα αυτά καθιστούν σαφή τον αντίκτυπο των ατελειών στις όψεις τις ίνας .

Με στόχο την παρατήρηση του πόσο επηρεάζει η διάδοση την απόκριση του PUF , έγινε τροποποίηση της αρχικού σχεδίου υλοποίησης . Τοποθετήθηκε ένα έμβολο που μπορεί να ασκήσει τάση στην ίνα με ακρίβεια μικρομέτρου και τα 2 άκρα της ίνας κρατήθηκαν σταθεροποιημένα . Η μετατόπιση που εφαρμόσθηκε είχε ελάχιστο βήμα 1 μm και ο φωτισμός ήταν σταθερός .



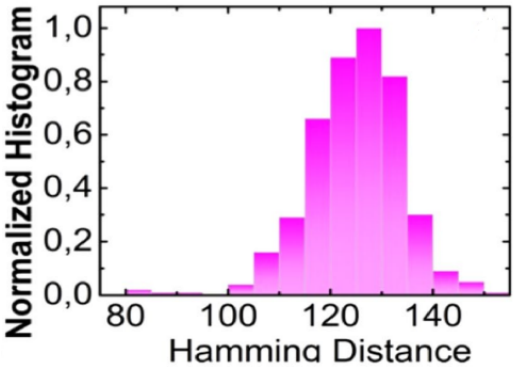
Εικόνα 19 : Εικόνα πειράματος (Charis Mesaritakis M. A., 2018)[3]

Ο συντελεστής διασταυρούμενης συσχέτισης κάθε διαδοχικής εικόνας σε σύγκριση με την αρχική φαίνεται στην παρακάτω εικόνα :



Εικόνα 20: Διάγραμμα συντελεστή συσχέτισης συναρτήσει της παραμόρφωσης της ίνας (Charis Mesaritakis M. A., 2018)[3]

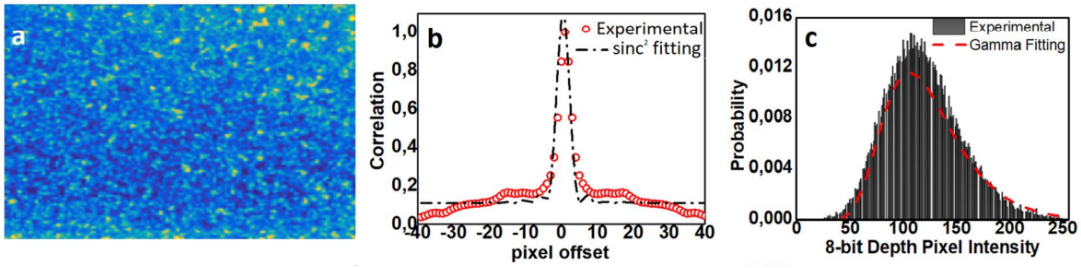
Όπως βλέπουμε μια μετατόπιση 3μm αρκεί για να αποσυσχετιστούν όλες τις αποκρίσεις μικρότερες του 0.15 (τιμή του συντελεστή αποσυσχέτισης) . Αυτές οι αποκρίσεις παρήγαγαν προφανώς κάποιες κωδικές λέξεις των οποίων τις αποστάσεις hamming βλέπουμε στην παρακάτω εικόνα .



Εικόνα 21: Διάγραμμα αποστάσεων Hamming για την ίδια πρόκληση στο ίδιο PUF υπό μηχανική παραμόρφωση (Charis Mesaritakis M. A., 2018)[3]

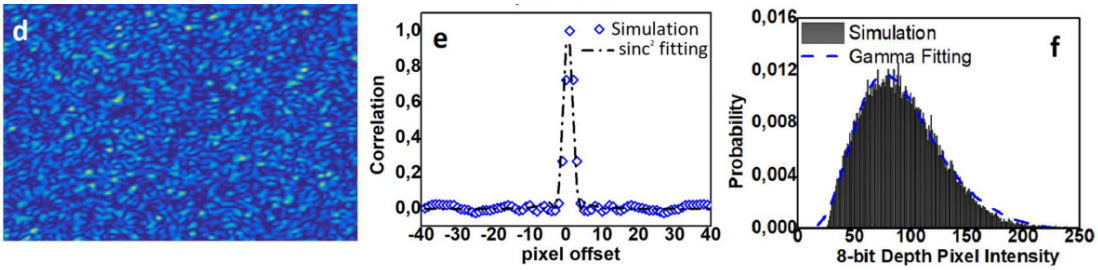
Η πλειονότητα των δειγμάτων όπως φαίνεται είναι ασυσχέτιστα και μας δίνουν μια απόσταση hamming 127.3 bits που αντιστοιχεί στο περίπου 50% αφού όλη η λέξη είναι 255 bits υπό μετατόπιση μεγαλύτερη των 3μm. Αντίθετα ένα αρκετά μικρό δείγμα φαίνεται να συσχετίζεται σε ένα βαθμό καθώς η πιθανότητα αλλοίωσης των bit του είναι 31.3% .

Για να επικυρωθεί η αρχή λειτουργίας, χρησιμοποιήθηκε μια πειραματική εικόνα διαστάσεων 200 x 200 ,υπολογίστηκε το μέσο μέγεθος κηλίδων στα 6 pixels , μια συνάρτηση αποσυσχέτισης με την παράλληλη εφαρμογή $sinc^2$ δίνοντας μέσο μέγεθος κηλίδων 6 pixels και το ιστόγραμμα κατανομής της έντασης τους. Η κατανομή προσαρμόστηκε σύμφωνα με μια συνάρτηση gamma.



Εικόνα 22: Πειραματικά αποτελέσματα (Charis Mesaritakis M. A., 2018)[3]

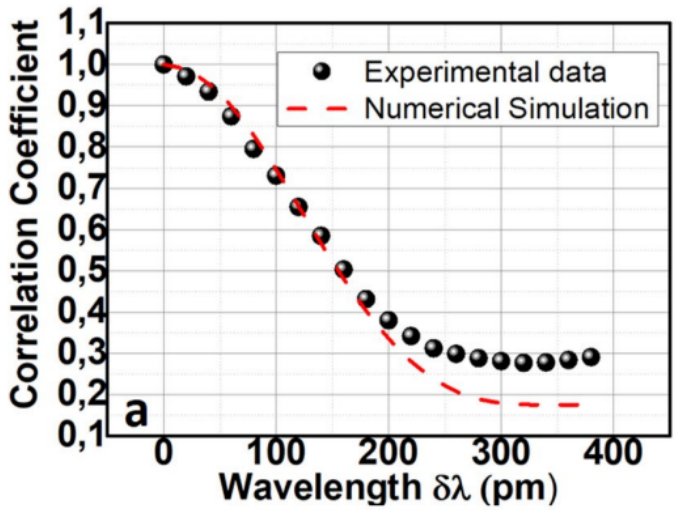
Στη συνέχεια στο κομμάτι της προσομοίωσης η απόσταση μεταξύ κάμερας και PUF τέθηκε στα 15cm (όσο περίπου και στο πειραματικό κομμάτι). Ως υπόθεση παίρνουμε ότι λόγω των ατελειών στην όψη της ίνας , διεγείρονται 100 τυχαίοι τρόποι που εμφανίζουν τυχαία ισχύ μετά από κανονική κατανομή . Με βάση αυτά τα δεδομένα προκύπτουν τα ακόλουθα αποτελέσματα:



Εικόνα 23: Αποτελέσματα προσομοίωσης (Charis Mesaritakis M. A., 2018)[3]

Το μέγεθος του κάθε κόκκου όπως φαίνεται είναι το ίδιο και η ένταση ακολουθεί μια κατανομή gamma. Ενώ τα πειραματικά αποτελέσματα και τα αποτελέσματα της προσομοίωσης ομοιάζουν αρκετά δεν είναι πανομοιότυπα . Αυτό συμβαίνει διότι κατά τη διενέργεια του πειράματος υπάρχει φως στο περιβάλλον το οποίο επηρεάζει τις μετρήσεις.

Στη συνέχεια εξετάζεται ένα άλλο λειτουργικό σενάριο , κατά το οποίο ο πυρήνας του PUF παραμένει σταθερός αλλά το μήκος κύματος της πηγής είναι μεταβλητό από 1540.0 μέχρι 1540.4 nmμε βήμα 10 pm. Στην εικόνα βλέπουμε το συντελεστή συσχέτισης της πρώτης εικόνας (λ=1540nm) συγκριτικά με τις επόμενες εικόνες τόσο για πειραματικά PUFs όσο και για προσομοιωμένα PUFs.

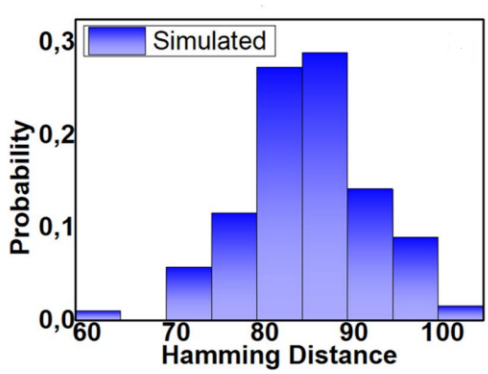


Εικόνα 24: Διάγραμμα μεταβολής του συντελεστή συσχέτισης συναρτήσει του μήκους κύματος της πηγής φωτισμού (Charis Mesaritakis M. A., 2018)[3]

Μέχρι τα 200pm παρατηρούμε ότι τα πειραματικά δεδομένα συμπίπτουν με τα δεδομένα τις προσομοίωσης . Για υψηλότερο όμως αποσυντονισμό , πέραν των 200pm , παρατηρείται μια μικρή αλλά σημαντική απόκλιση . Η μέγιστη τιμή που παίρνει ο συντελεστής για τα πειραματικά δεδομένα είναι 0,28 και οφείλεται επίσης και στην ύπαρξη φωτός του περιβάλλοντος. Για τα αριθμητικά δεδομένα , οι μεταβολές του μήκους κύματος οφείλονται μόνο στην φάση που επηρεάστηκε λόγω της διάδοσης για κάθε τρόπο μετάδοσης. Πιο περίπλοκες διαδικασίες δεν λαμβάνονται υπόψιν .

Προσομοιώσεις με αυξημένο αριθμό τρόπων διάδοσης αλλά σταθερή διαφορά μέγιστης ταχύτητας φάσης βγάζουν ίδια αποτελέσματα με την άνω εικόνα . Άρα βγάζουμε το συμπέρασμα ότι όπως και στις αριθμητικές προσομοιώσεις , η πειραματικά μετρημένη ευαισθησία μήκους κύματος οφείλεται στην διαφορά μέγιστης ταχύτητας φάσης των διεγερμένων τρόπων διάδοσης.

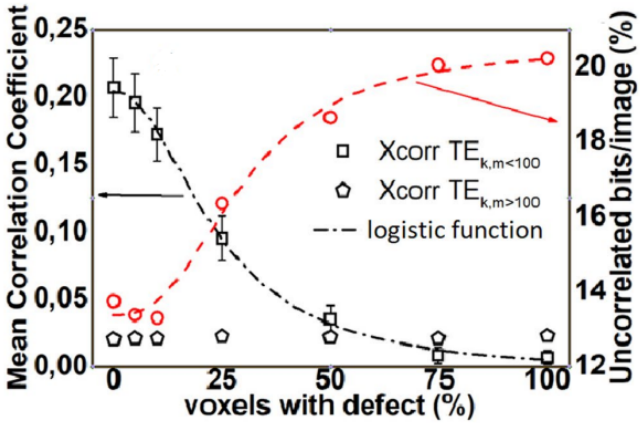
Σε μια άλλη περίπτωση , για την εξέταση της πιθανότητας κλωνοποίησης , κρατήσαμε όλες τις παραμέτρους σταθερές εκτός από τις ατέλειες στην όψη της ίνας. Η κατανομή γίνεται εντός των τρόπων διάδοσης , υπάρχουν 100 τυχαίοι εγκάρσιοι τρόποι υψηλής τάξης και 100 διαφορετικές έξοδοι βάσει των ελαττωμάτων (υποθετικά διαφορετικά PUFs) . Οι κηλίδες που προκύπτουν ψηφιοποιούνται με την τεχνική random binary hashing. Στην εικόνα βλέπουμε την συνάρτηση πυκνότητας πιθανότητας της απόστασης Hamming μεταξύ των ζευγαριών των παραγόμενων λέξεων για 100 διαφορετικά στιγμιότυπα.



Εικόνα 25: Διάγραμμα συνάρτησης πυκνότητας πιθανότητας των αποστάσεων Hamming για 100 διαφορετικά στιγμιότυπα του PUF (Charis Mesaritakis M. A., 2018)[3]

Η μέση τιμή είναι 86.2 που αντιστοιχεί σε ποσοστό περίπου 33.2% , αρκετά χαμηλότερο από το αντίστοιχο 42% που πετύχαμε στην Εικόνα 14. Αυτή η σημαντική απόκλιση οφείλεται στην απουσία φαινομένων θορύβου στην αριθμητική προσέγγιση . Αν προσθέσουμε το επίπεδο θορύβου της εικόνας 4b (13.7) , τότε η μέση απόσταση hamming γίνεται 100 το οποίο είναι κοντά στην πειραματική τιμή 107.

Στην προσπάθεια να υπολογιστούν οι βέλτιστες συνθήκες λειτουργίας , έγινε μια υπόθεση για 2 διαφορετικά set των αρχικών εγκάρσιων τρόπων . Το πρώτο αποτελείται από διαδοχικούς τρόπους χαμηλής τάξης και το δεύτερο αποτελείται από 100 τυχαίους τρόπους υψηλής τάξης. Και για τα 2 σετ υποθέτουμε ότι πραγματοποιήθηκαν 100 τυχαίες εσωτερικές κατανομές ισχύος . Υπολογίστηκε ο συντελεστής συσχέτισης όλων των αντίστοιχων μοτίβων κηλίδων έναντι στο ποσοστό των voxels στην όψη εξόδου.



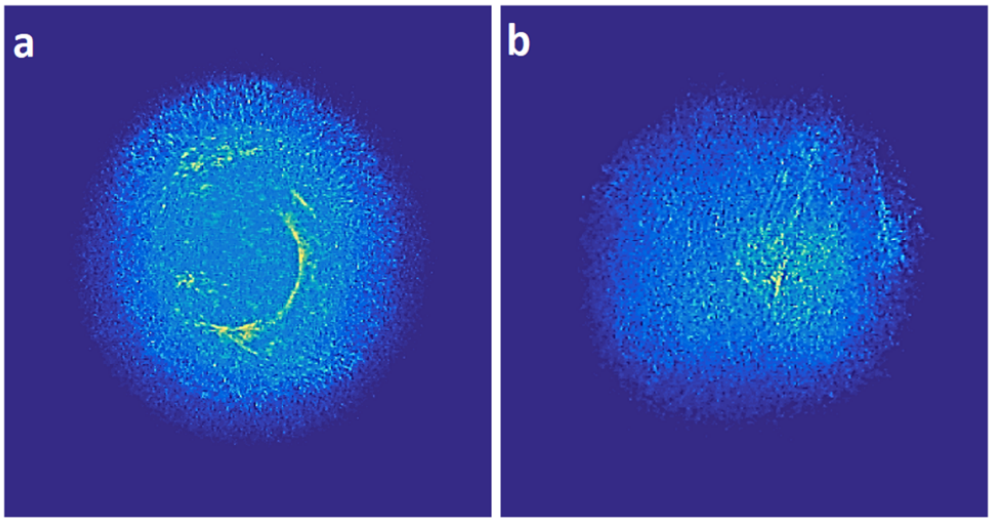
Εικόνα 26: Μέση διασταυρούμενη συσχέτιση για 100 διαφορετικές συνθήκες φωτισμού συναρτήσει του ποσοστού ελαττωμάτων της όψης εξόδου. Δεξιά στον άξονα y είναι το ποσοστό ασυσχέτιστων bits ανά εικόνα .

Όπως βλέπουμε , για τους τρόπους χαμηλής τάξης (<100) , η αύξηση του ποσοστού ατελειών οδηγεί σε μείωση της μέσης τιμής του συντελεστής συσχέτισης που αντικατοπτρίζει το πόσο μεγάλη επίδραση έχει η όψη εξόδου στο σύστημα . Συγκεκριμένα , από μια αρχική τιμή 0.25 παρατηρείται πτώση σε τιμή κάτω του 0.05 . Οι τρόποι χαμηλής τάξης ανεξαρτήτως της κατανομής ισχύος φαίνεται ότι παρουσιάζουν μειωμένη χωρική πολυπλοκότητα. Αυτό επιβεβαιώνεται επίσης και από τον υπολογισμό του ποσοστού των μέσων εξαγώγιμων ανεξάρτητων bit ανά εικόνα που φαίνεται στην εικόνα με κόκκινα κυκλάκια. Δεδομένου ότι η απόσταση μεταξύ κάμερας και PUF είναι σταθερή , αυτή η μέτρηση συνδέεται άμεσα με την εντροπία κάθε εικόνας και άρα και με την χωρική πολυπλοκότητα. Παρατηρείται μια αύξηση συναρτήσει και του ποσοστού ατελειών που μπορεί να φτάσει μέχρι και 20%.

Αντιθέτως , αν χρησιμοποιήσουμε τρόπους υψηλής τάξης (μαύρα πεντάγωνα στο σχήμα) δεν παρατηρούμε την ίδια τάση .Ανεξαρτήτως του ποσοστού των ατελειών όπως βλέπουμε η συσχέτιση παραμένει χαμηλή και συγκεκριμένα μικρότερη του 0.05 . Είναι σχεδόν μια ευθεία και όπως φαίνεται οι ατέλειες την επηρεάζουν απειροελάχιστα. Αυτό μπορεί να αποδοθεί στην έμφυτη χωρική πολυπλοκότητα που παρουσιάζουν οι τρόποι υψηλής τάξης . Η χωρική

κατανομή ομοιάζει με κηλίδες . Άρα μπορούμε να εξάγουμε ασφαλώς το συμπέρασμα ότι ένα PUF που βασίζεται σε ίνα με όψη εισόδου αρκετά ατελή , προκαλεί τρόπους διάδοσης υψηλής τάξης . Όσον αφορά την εντροπία των εικόνων συγκριτικά με ένα PUF που έχει πολωμένη είσοδο αλλά ατελή έξοδο παρουσιάζουν περίπου την ίδια απόδοση .

Η φυσική μη κλωνοποιησιμότητα ενισχύεται όταν υπάρχουν ατέλειες και στις 2 όψεις εισόδου και εξόδου της ίνας. Τα αριθμητικά αυτά αποτελέσματα επιβεβαιώθηκαν και πειραματικά χρησιμοποιώντας μια ίνα που η μία όψη είχε γυαλιστεί με ένα σύστημα γυαλίσματος διαμαντιών . Στις εικόνες βλέπουμε τις αποκρίσεις του PUF που αποκτήθηκαν χρησιμοποιώντας τη γυαλισμένη όψη σαν είσοδο και έξοδο αντίστοιχα.



Εικόνα 27 : Πειραματικές εικόνες από εξόδους του PUF όπου η όψη εισόδου (αριστερά) είναι πολύ ελαττωματική και η όψη εξόδου γυαλισμένη και αντίστροφα (δεξιά) (Charis Mesaritakis M. A., 2018)[3]

Με σύνολα δεδομένων παρόμοια με αυτά που είδαμε παραπάνω στις εικόνες 4b,4c παρατηρήθηκε και για τις 2 περιπτώσεις ίδια απόδοση . Οι μέσες αποστάσεις hamming βρέθηκαν 93 +- 15.9 για την αριστερή εικόνα και 95.7 +- 16.7 για την δεξιά εικόνα . Αφού λοιπόν αυτά τα πειραματικά αποτελέσματα είναι παρόμοια με αυτά της προσομοίωσης συμπεραίνουμε ότι η χωρική πολυπλοκότητα ακολουθεί την πολυπλοκότητα της όψης της ίνας. Αυτό πρακτικά σημαίνει ότι είτε έχουμε μια ατελή όψη εισόδου είτε μια ατελή όψη εξόδου , οι τρόποι διάδοσης μπορούν να αναμειχθούν και να αλλάξουν ισχύ ανεξαρτήτως του αν η είσοδος ή η έξοδος είναι ατελής και παρουσιάζει ελαττώματα.

Συμπέρασμα

Κατόπιν σύγκρισης του συγκεκριμένου σχήματος με τυπικά οπτικά PUFs μπορούμε να εξάγουμε κάποια συμπεράσματα . Η πειραματικές αλλά και οι μετρήσεις της προσομοίωσης καθιστούν σαφές ότι προσφέρει λιγότερες πιθανότητες κλωνοποίησης από ένα τυπικό οπτικό PUF . Αυτή η πιθανότητα κλωνοποίησης αναφέρεται σε καλοπροαίρετους κατασκευαστές δηλαδή πρακτικά είναι η ακούσια πιθανότητα κλωνοποίησης. Ταυτόχρονα , η απόδοση είναι επίσης καλύτερη , γεγονός που οφείλεται στην συνύπαρξη φυσικών μηχανισμών ανάμειξης όπως οι ατέλειες στις όψεις της ίνας αλλά και ελαττώματα μέσα στην ίνα που ενισχύουν την πιθανότητα μη κλωνοποίησης από κακοπροαίρετους αυτή τη φορά κατασκευαστές. Παρόλο που το πείραμα εκτελέστηκε χρησιμοποιώντας ογκώδη οπτικά εξαρτήματα , η αρχή της

λειτουργίας του προσφέρεται για εφαρμογή σε μια ενσωματωμένη φωτονική πλατφόρμα , καθιστώντας δυνατή την «μικρογραφία» του , τη μείωση δηλαδή του όγκου του.

PUFS που βασίζονται σε ενσωματωμένες νευρομορφικές συσκευές

Σε αυτή την ενότητα θα αναλύσουμε ένα καινοτόμο σενάριο φωτονικού PUFπου μπορεί να υλοποιηθεί μέσω οποιασδήποτε νευρομορφικής αρχιτεκτονικής. Οι υλοποιήσεις που μοιάζουν με RNN(επαναλαμβανόμενο νευρωνικό δίκτυο)φαίνεται να παρέχουν πρόσθετα πλεονεκτήματα ασφαλείας. Θα χρησιμοποιηθεί ένα ενσωματωμένο φωτονικό RC (Reservoir Computing) βασισμένο σε έναν ROSS (Recurrent Optical Spectrum Slicer). Στην προκειμένη το ασφαλές φυσικό χαρακτηριστικό που χρησιμοποιείται , είναι η αναπόφευκτη πρόκληση μεταβλητότητας των σύνθετων βαρών κατά τη διαδικασία κατασκευής στο κρυφό στρώμα του RC. Το προτεινόμενο σχήμα πέρα από την παροχή χαρακτηριστικών ασφαλείας παραμένει ένας φωτονικός νευρομορφικός επεξεργαστής και επομένως είναι σε θέση να παρέχει ταυτόχρονα υψηλή ταχύτητα και χαμηλής ισχύος επεξεργασία .

Αρχή λειτουργίας του νευρομορφικού PUF

Το προτεινόμενο νευρομορφικό PUFμπορεί να πραγματοποιηθεί με οποιοδήποτε τύπο νευρωνικού δικτύου . Τα RNN και RC είναι τα καλύτερα για τη συγκεκριμένη υλοποίηση . Αυτό συμβαίνει διότι υπάρχει μια σύνθετη δυναμική σχέση μεταξύ της εξόδου τους και του κρυφού στρώματος. Στην αρχιτεκτονική RCθέλουμε ένα γνωστό ζευγάρι χρονικών ιχνών $\{X_{in}Y_{out}\}$ που συνδέονται μαθηματικά .Ένα χαρακτηριστικό παράδειγμα είναι η ακολουθία NARMA (μη γραμμικός αυτοπαλινδρομικός κινούμενος μέσος όρος) . Εμφανίζει παράγοντα μνήμης m ως ακολούθως :

$$Y_{out}(i) = 0.3\, Y_{out}(i-1) + 0.05\, Y_{out}(i-1) * \sum_{k=1}^{m} Y_{out}\,(i-k) + 1.5\, X_{in}(i-m) + 0.1$$

Το X_{in} λαμβάνεται από μια τυχαία κατανομή . Το ζευγάρι αυτό στην περίπτωση μας θεωρείται η πρόκληση (είσοδος) και θεωρείται δημόσια πληροφορία . Το ζευγάρι πρόκλησης μπορεί να ληφθεί από οποιοδήποτε σύνολο δεδομένων που το RCεπεξεργάζεται ήδη (όπως χρονοσειρές , δεδομένα τηλεπικοινωνιών) απλοποιώντας έτσι την ενσωμάτωση του σε πραγματικά συστήματα.

Το ίδιο το PUFείναι μια φυσική ενσωμάτωση ενός RC του οποίου hardware τα καθορισμένα βάρη στο κρυφό στρώμα $W_{int} = W_{ideal} \pm dW$ αποκλίνουν από ένα ιδανικό πρωτότυπο W_{ideal} λόγω κατασκευαστικών ατελειών dW .Τα ακριβή εσωτερικά βάρη W_{int}θεωρούνται μυστικά (δεν είναι δηλαδή δημόσια) και πρέπει να είναι ανθεκτικά στη φυσική κλωνοποίηση καθώς δεν μπορούν να εξαχθούν εύκολα ακόμη και από νόμιμους χρήστες ειδικά όταν οι αρχιτεκτονικές είναι πυκνές.

Με την παρακάτω εξίσωση μπορούμε να υπολογίσουμε την κατάσταση του κάθε κόμβου :

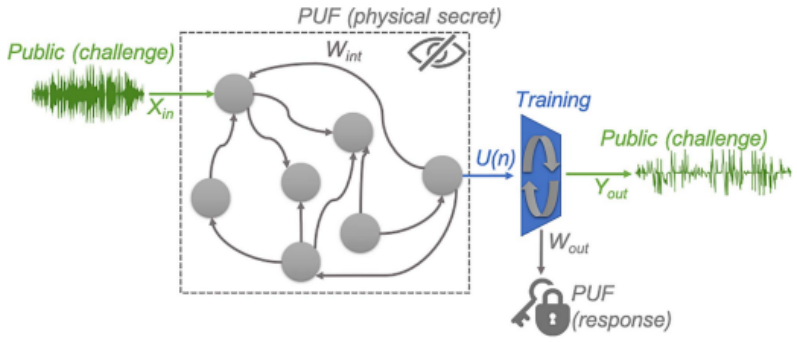
$$U(i) = f[U(i-k_i) * W_{int} + X_{in}(i)] + n(i) \quad (1)$$

ΌπουU(n) ορίζεται το διάνυσμα κατάστασης ,f είναι μια μη γραμμική συνάρτηση ενεργοποίησης , n είναι προσθετικός λευκός Gaussiavός θόρυβος και k_iη καθυστέρηση που εκφράζεται στον αριθμό των δειγμάτων για κάθε διασυνδεδεμένο κόμβο.

Παρατηρούμε ότι το διάνυσμα κατάστασης είναι δυναμικά συνδεδεμένο με τον πίνακα W_{int}μέσω της μη γραμμικής συνάρτησης ενεργοποίησης f .Χρησιμοποιώντας συμβατική νευρωνική εκπαίδευση , τα βάρη εξόδου του RC W_{out} ρυθμίζονται έτσι ώστε να μιμούνται την ακολουθία NARMA ώστε $Y_{out}(i) = W_{out} * U(i)$

Αυτό σημαίνει ότι το W_{out}ρυθμίζεται επίσης από τις ακριβείς τιμές του W_{int}Αν το W_{int}ποικίλλει σε σχέση με το W_{ideal} η διαδικασία εκπαίδευσης θα εξακολουθεί να επιτρέπει το RCνα συγκλίνει στη σωστή ακολουθία Y_{out}αλλά σε κάθε περίπτωση θα χρησιμοποιήσει ένα διαφορετικό σύνολο W'_{out}για να το πετύχει αυτό διότι το RCείναι ένα σύνθετο δυναμικό σύστημα του οποίου οι καταστάσεις εξαρτώνται από την εσωτερική συνδεσιμότητα του.

Άρα το W'_{out} μπορεί να θεωρηθεί η απόκριση του PUF για μια γνωστή είσοδο . Στην εικόνα βλέπουμε την λογική της υλοποίησης:



Εικόνα 28: Λογική υλοποίησης νευρομορφικού PUF

(Charis Mesaritakis D. D., 2022)

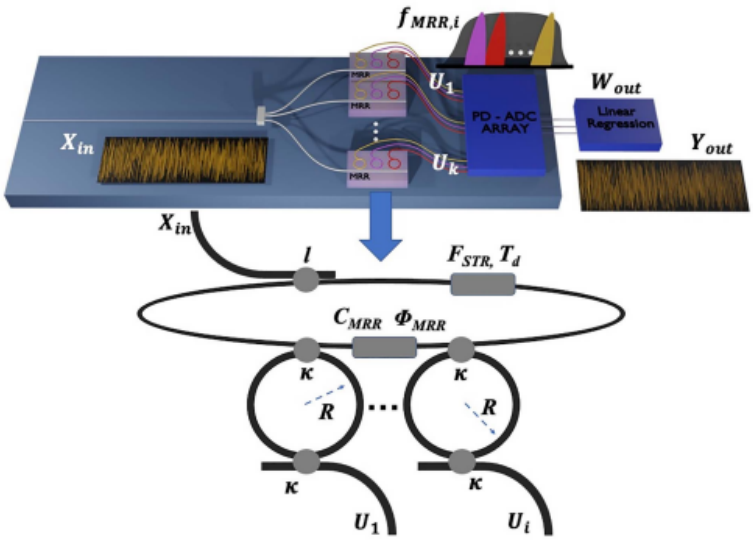
Η πρόκληση του PUFείναι οι ακολουθίες εκπαίδευσης X_{in}και Y_{out}. Το μη κλωνοποιήσιμο χαρακτηριστικό του PUFείναι τα σύνθετα οπτικά βάρη του RC W_{int}. Η απόκριση του PUFείναι τα βάρη ψηφιακής εξόδου στη γραμμική παλινδρόμηση W_{out} που συνδέονται άμεσα με το Y_{out} και το W_{int} .

Ανάλογα λοιπόν με τον αριθμό των ζευγαριών που χρησιμοποιούνται για την εκπαίδευση του RC, η συγκεκριμένη υλοποίηση μπορεί να λειτουργεί είτε ως αδύναμο είτε ως δυνατό PUF . Αν δηλαδή χρησιμοποιήσουμε μεγάλο αριθμό τέτοιων ζευγαριών το PUF θα είναι δυνατό.

Φωτονικό RC

Θα υλοποιηθεί ένα RC παρόμοιο με το ROSS. Αυτό έχει 5 κόμβους επανάληψης και κάθε κόμβος έχει 5 φίλτρα . Αυτά τα φίλτρα θεωρούμε ότι λειτουργούν σαν MRR(μικροί δακτύλιοι προσθήκης ή πτώσης που λειτουργούν σαν φίλτρα)και οι θύρες πτώσης των MRR χρησιμοποιούνται σαν έξοδοι του σχήματος αυτού . Ακολουθούνται από φωτοανιχνευτές (PDs) , μετατροπείς αναλογικού σε ψηφιακό (ADC) και ένα σχήμα ψηφιακής γραμμικής

παλινδρόμησης για εκπαίδευση. Στην εικόνα φαίνεται το προτεινόμενο σχήμα της υλοποίησης.



Εικόνα 29: Σχήμα της προτεινόμενης υλοποίησης (Charis Mesaritakis D. D., 2022)[2]

Αυτό το σχήμα RC βασίζεται στην φασματική αποσύνθεση του εισερχόμενου σήματος από τους κόμβους επανάληψης που λειτουργούν ως επαναλαμβανόμενα σύνθετα φίλτρα. Κάθε MRRστοχεύει ένα συγκεκριμένο κομμάτι του εισερχόμενου φάσματος και έτσι ο καθένας παράγει μια χρονική έξοδο που είναι διαφορετική από τους υπόλοιπους . Το σχήμα προσομοιώνεται αριθμητικά χρησιμοποιώντας μια προσέγγιση που βασίζεται στη μεταφορά ενός πίνακα. Οι παράμετροι που μπορούν να βελτιστοποιηθούν ώστε να πετύχουμε καλύτερη απόδοση είναι οι εξής : η δύναμη ανατροφοδότησης (F_{STR}) , η καθυστέρηση (T_d) , ο συντελεστής σύζευξης (κ) που ρυθμίζει το εύρος ζώνης του κάθε MRR , ο παράγοντας ποιότητας , η κεντρική συχνότητα κάθε MRR (f_{MRR}) , η φάση εντός του MRR(Φ_{MRR}) και ο συντελεστής μετάδοσης (C_{MRR}). Η έξοδος του κάθε MRRσε ένα απλό κόμβο επανάληψης περιγράφεται από την εξίσωση :

$$U_i(\omega) = X_{in}(\omega) \cdot H(\omega)_{drp,i} \cdot \; a/b$$

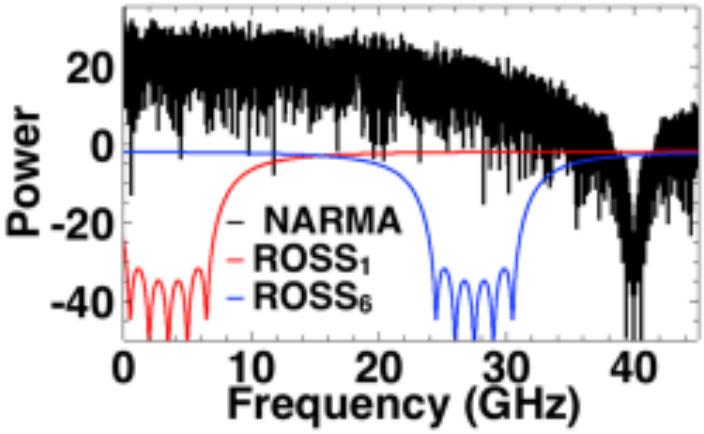
$$a = \prod_{m=1}^{i-1} E(\omega)_{thr,m} \cdot \sum_{m=1}^{k-1} C_{MRR,\,m} e^{-j\Phi_{MRR,m}} \sqrt{1-l^2}$$

$$b = 1 + l1\sqrt{F_{STR}} \prod_{m=1}^{k} \times e^{-i(\omega\, Td + \sum \Phi_{MRR})} H(\omega)_{thr,m}$$

(Charis Mesaritakis D. D., 2022)

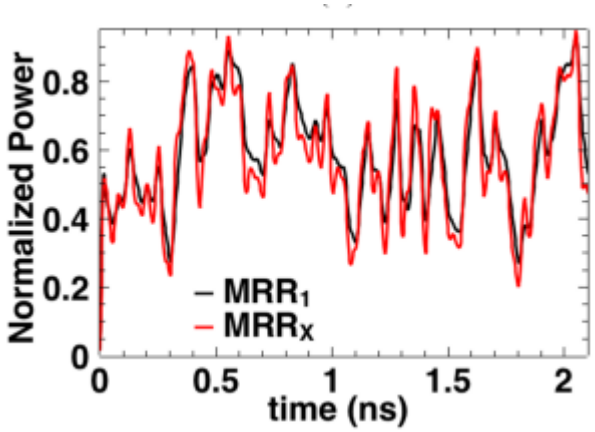
Για τη δημιουργία του απαιτούμενου δημοσίου ζευγαριού χρόνου-ίχνους , χρησιμοποιήθηκε μια ψευδό-τυχαία γεννήτρια που παρέχει Νδείγματα για το X_{in}που λαμβάνονται από μια ομοιόμορφη κατανομή στο εύρος {-1,1}.Χρησιμοποιώντας την εξίσωση (1) υπολογίστηκε η ακολουθία NARMA (Y_{out}) . Τα δείγματα του X_{in} χρησιμοποιούνται για τη διαμόρφωση του

πλάτους ενός οπτικού φορέα με μήκος κύματος λ=1550nm, ένα ρυθμό συμβόλων 40 Gsymbol/sec , 20 dB λόγο εξάλειψης και μέγιστη οπτική ισχύ με εύρος από 1mWμέχρι 40mW. Οι φωτοανιχνευτές στην έξοδο θεωρείται ότι έχουν ένα εύρος ζώνης που ταιριάζει με το ρυθμό συμβόλων του σήματος (40GHz).Τα παραγόμενα φωτορεύματα υπόκεινται σε τυπικές επιδράσεις θορύβου ώστε να αποτελούν μια ρεαλιστική πηγή θορύβου (n) .Στην παρακάτω εικόνα βλέπουμε τη φασματική αποσύνθεση ως προϊόν πολλαπλού φιλτραρίσματος :



Εικόνα 30: Διάγραμμα φασματικής αποσύνθεσης (Charis Mesaritakis D. D., 2022)[2]

Το εύρος ζώνης του σήματος απεικονίζεται παράλληλα με την απόκριση πλάτους μέσω της θύρας για δύο τυπικούς κόμβους επανάληψης. Η φασματική αποσύνθεση οδηγεί σε διαφοροποιημένα χρονικά ίχνη στην έξοδο του κάθε MRR :



Εικόνα 31: Διάγραμμα διαφοροποιημένων χρονικών ιχνών (Charis Mesaritakis D. D., 2022)[2]

Τα ψηφιοποιημένα χρονικά ίχνη τροφοδοτούνται σε έναν αλγόριθμο παλινδρόμησης κορυφογραμμής . Επιπλέον , αναμένεται ότι οι μεταβολές θερμοκρασίας θα επηρεάσουν την απόδοση του συστήματος λόγω των αλλαγών συχνότητας συντονισμού που προκαλούνται από το θερμό-οπτικό φαινόμενο . Αλλά αυτό δεν παίζει μεγάλο ρόλο καθώς σε πραγματικά πειράματα με πραγματικά chipsυπάρχουν τρόποι να αντιμετωπισθεί επιτυχώς.

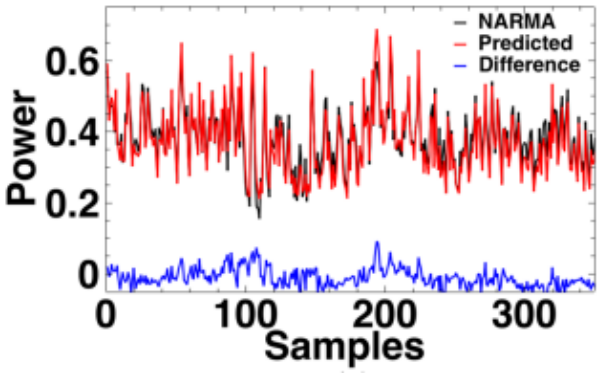
Το RC τροφοδοτήθηκε με ένα λόγο N_{train} προς τα συνολικά δείγματα N του X_{in}και εκπαιδεύτηκε πάνω σε αυτά για την παραγωγή του Y_{out} .Η απόδοση της πρόβλεψης

αξιολογείται χρησιμοποιώντας (NSME) που είναι το κανονικοποιημένο μέσο τετραγωνικό σφάλμα μεταξύ του πραγματικού Y_{out}και της εξόδου του RC , Y'_{out}. Στη συνέχεια , τα ψηφιακά βάρη διατηρήθηκαν σταθερά και τροφοδοτήθηκε το RC με 1000 διαδοχικά δείγματα από το X_{in}με στόχο να μιμηθεί επιτυχώς το Y_{out} ($NSME_{test}$). Για αυτή τη διαδικασία σαρώθηκαν όλες οι προαναφερθείσες παράμετροι ώστε να επιτευχθεί βέλτιστη απόδοση κατά την εξαγωγή συμπερασμάτων . Αυτές οι παράμετροι είναι οι ακόλουθες και απεικονίζονται στον πίνακα 1:

Parameter	Typical Value	PUF deviations [29*]
κ (coupling coefficient)	0.25	constant
F_{str} *(feedback strength)*	0.9	constant
T_d *(loop delay)*	25ps	constant
T_{MRR} *(inter-MRR delay)*	2.5ps	constant
f_{MRR} *(inter-MRR frequency separation)*	1GHz	N. D (m=f_{ideal}, σ=0.1)
C_{MRR} *(inter-MRR connection strength)*	0.95	N. D (m=0.97, σ=0.1)
n_{eff}(waveguide)	3.4	U.D (-0.015, 0.015)
α (propagation losses)	10 m^{-1}	constant
R (ring radius)	55μm	constant
m (NARMA memory)	10	-
N (NARMA length)	4000	-

Πίνακας 1: Παράμετροι και τιμές τους (Charis Mesaritakis D. D., 2022)[2]

Στην εικόνα που ακολουθεί βλέπουμε τα Y_{out} και Y'_{out}καθώς και την απόλυτη διαφορά μεταξύ του Y_{out}και του Y'_{out}(μπλε χρώμα).

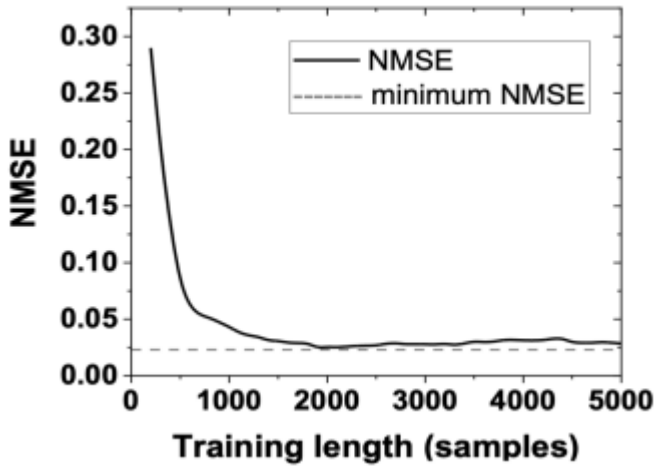


(Charis Mesaritakis D. D., 2022)[2]

Εικόνα 32 : Διάγραμμα των Y_{out} και Y'_{out} και από κάτω (με μπλε) η απόλυτη διαφορά τους

Το $NSME_{test}$υπολογίστηκε $NSME_{test}$= 0.023 , γεγονός που δείχνει ότι είναι πολύ καλό . Το RCαυτό προσφέρει βελτιωμένα αποτελέσματα σε σχέση με άλλα φωτονικά RCταυτόχρονα χρησιμοποιώντας λιγότερους φυσικούς κόμβους αποδεικνύοντας ότι τα νευρωνικά δίκτυα που βασίζονται σε ROSSείναι κατάλληλα και για μη τηλεπικοινωνιακές δουλειές.

Το πολύ χαμηλό $NSME_{test}$δείχνει ότι το RCσυγκλίνει σε μια σταθερή λύση για την εργασία αυτή και άρα τα ψηφιακά βάρη στο στάδιο της παλινδρόμησης συγκλίνουν επίσης στις τελικές τους τιμές .Προκειμένου να υπολογιστεί το ελάχιστο δυνατό N_{train}που προσφέρει αυτή τη σύγκλιση στην παρακάτω εικόνα υπολογίστηκε το $NSME_{test}$συναρτήσει του αριθμού δειγμάτων που χρησιμοποιείται για εκπαίδευση N_{train} .



Εικόνα 33: Διάγραμμα του NMSE συναρτήσει του αριθμού δειγμάτων (Charis Mesaritakis D. D., 2022)[2]

Όπως παρατηρούμε , για N_{train}μεγαλύτερο του 1600 η απόδοση είναι σταθερή . Άρα είναι ασφαλές να πούμε ότι ένα N_{train} = 2000 αρκεί και επομένως αυτό θα χρησιμοποιηθεί στην ακόλουθη ανάλυση.

Προσομοίωση

Προκειμένου να αξιολογηθεί η εγκυρότητα της συγκεκριμένης υλοποίησης , απαιτείται μια ρεαλιστική νευρομορφική υλοποίηση ώστε τα dWνα αντιστοιχούν σε πραγματικές φυσικές

ατέλειες . Λόγω της υψηλής αντίθεσης του πυριτίου στην πλατφόρμα μονωτή οι συσκευές είναι πολύ ευαίσθητες σε γεωμετρικές αλλαγές που συνεπάγεται συνήθως εσωτερικές διακυμάνσεις στο πλάτος και το πάχος του κυματοδηγού . Το μέγεθος των διακυμάνσεων εξαρτάται από την λιθογραφική τεχνική που χρησιμοποιείται και από την ποιότητα της γκοφρέτας. Σε κάθε περίπτωση αυτό οδηγεί σε τυχαίες μεταβολές των απωλειών του κυματοδηγού και έχουν επίπτωση στον αποτελεσματικό δείκτη διάθλασης του κυματοδηγού που μπορεί να φτάσει μέχρι και $\Delta n_{eff} = 0.015$.

Σε αυτό το RC οι κυματοδηγοί εντός των MRRέχουν μήκος L = 200μmκαι έτσι η διακύμανση του δείκτη διάθλασης αντιστοιχεί σε μια διαφορά φάσης για τον κυματοδηγό κάθε κόμβου της τάξεως του $\Delta\Phi$= (2π/λ) *L * Δn_{eff}= 12π περίπου . Αυτή η διακύμανση επηρεάζει επίσης τους κυκλικούς κυματοδηγούς που χρησιμοποιούνται στους MRR. Δεδομένης της μεγαλύτερης τους επιφάνειας ($R_{MRR} = 55\mu m$) και L=345μm το ίδιο Δn_{eff}θα οδηγήσει σε ακόμα ισχυρότερες διακυμάνσεις φάσης της τάξεως του $\Delta\Phi$ = 20,9 π περίπου . Αυτές οι ολισθήσεις φάσης θα επηρεάσουν τρομερά τη συχνότητα συντονισμού κάθε MRRκαι θα προκαλέσουν έντονες διακυμάνσεις μεταξύ διαφορετικών κόμβων ROSS. Αυτές οι επιδράσεις δεν μπορούν να προβλεφθούν ή να τροποποιηθούν , είναι δηλαδή εγγενείς και επομένως λειτουργούν ως το αναγκαίο τυχαίο και αδύνατο να αντιγραφεί χαρακτηριστικό της παραγωγής του PUF, καθιστώντας την αναπαραγωγή της συσκευής ακόμα πιο δύσκολη .

Για να δούμε τις προαναφερθείσες αποκλίσεις και την επίδραση αυτών στα νευρωνικά βάρη στο RCPUF, μοντελοποιήθηκαν αριθμητικά 5.5 * 10^5 στιγμιότυπα με τις ίδιες παραμέτρους μοντελοποίησης με το ιδανικό RCπου περιγράφηκε εκτός από 3 παραμέτρους . Αυτές είναι ο συντελεστής μετάδοσης του κυματοδηγού C_{MRR}, η μετατόπιση φάσης Φ_{MRR}και η συχνότητα συντονισμού για κάθε MRRf_{MRR}. Τα στιγμιότυπα είναι πολλά σε αριθμό ώστε να παρέχουν ένα ικανοποιητικό επίπεδο εμπιστοσύνης για τις στατιστικές δοκιμές . Η μεταβολή αυτών των παραμέτρων φαίνεται στον πίνακα 1 και προκύπτει από την τραχύτητα του κυματοδηγού .

Προφανώς όλα τα ίδια φαινόμενα μπορούν να επηρεάσουν όλες τις παραμέτρους του RCαλλά εδώ επικεντρωνόμαστε σε 3 παραμέτρους ώστε να υπολογίσουμε την απόδοση υπό τις δεδομένες αυστηρές συνθήκες . Αν και η μετατόπιση φάσης του MRRθα επηρεάσει αρκετά τη συχνότητα συντονισμού , στη συγκεκριμένη προσέγγιση υπολογίζουμε την απόκλιση συχνότητας μόνο στο 10% .

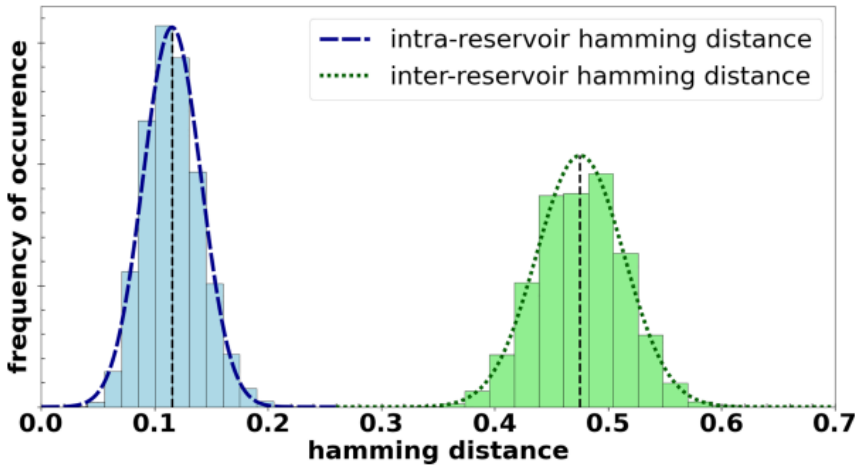
Η αξιολόγηση πραγματοποιείται ως εξής . Χρησιμοποιείται η ίδια πρόκληση σε όλα τα στιγμιότυπα του RC(X_{in}, Y_{out}) . Αφού εκπαιδεύτηκε κάθε RCυπολογίζονται τα βάρη εξόδου W_{out}.Τα βάρη υπολογίζονται ώστε να ελέγξουμε το $NSME_{test}$και να διασφαλίζεται η σύγκλιση . Από κάθε βάρος , μόνο τα 3 πιο σημαντικά δεκαδικά ψηφία κρατήθηκαν . Οι αριθμοί κυμαίνονται στο εύρος από -1 μέχρι 1 και κβαντίζονται ώστε να καταλήξουμε σε ένα μόνο bitανά βάρος . Έτσι , κάθε MRRστο RCPUFμπορεί να παράγει κλειδιά από bitsίσα με τον αριθμό των tapsκαι επομένως το κάθε PUFνα παράγει ένα κλειδί ανά πρόκληση μεγέθους 256 bits.

Απόδοση του RCPUF

Για τα αδύναμα PUFδηλαδή τα PUFπου παράγουν μία απόκριση πρέπει να αξιολογήσουμε 2 ιδιότητες , την ευρωστία και την πιθανότητα κλωνοποίησης . Η ευρωστία υπολογίζεται ως η διαφορά μεταξύ των αποκρίσεων αν εφαρμοστεί η ίδια πρόκληση στο ίδιο PUFκαι σχετίζεται με την ανθεκτικότητα του συστήματος στον εξωτερικό θόρυβο . Στην προκειμένη χρησιμοποιούνται shot και θερμικός θόρυβος στους φωτοανιχνευτές . Επομένως η απόδοση

βασίζεται στην οπτική ισχύ εισόδου και την ταχύτητα απόκτησης στο επίπεδο ανίχνευσης. Όσον αφορά στην μη κλωνοποιησιμότητα , αυτή υπολογίζεται ως η διαφορά μεταξύ των αποκρίσεων που προέρχονται από διαφορετικά PUFsπάνω στα οποία έχει εφαρμοστεί η ίδια πρόκληση .Στην περίπτωση μας , τα διαφορετικά PUFsπροέρχονται από έναν κατασκευαστή του οποίου οι δυνατότητες αντιγραφής περιορίζονται από την τεχνολογική πλατφόρμα . Άρα και οι 2 ιδιότητες ικανοποιούνται .

Στην εικόνα βλέπουμε τις κατανομές από τις κανονικοποιημένες αποστάσεις Hamming.



Εικόνα 34 : Διάγραμμα κατανομών των κανονικοποιημένων αποστάσεων Hamming (Charis Mesaritakis D. D., 2022)[2]

Η intra-distanceπου φαίνεται με γαλάζιο αντιστοιχεί σε διαδοχικές αποκρίσεις από το ίδιο RCPUFπου εκπαιδεύτηκε 10000 φορές για την ίδια πρόκληση αλλά υπόκειται σε θόρυβο κατά την ανίχνευση . Η μέγιστη ισχύς εισόδου ρυθμίζεται στα 20 mWενώ πριν την εκπαίδευση υπολογίστηκαν κατά μέσο όρο 100 φορές οι αναλογικές καταστάσεις του RCώστε να ενισχυθεί το SNR. Αφού εφαρμόστηκε Gaussianfit(διακεκομμένες μπλε γραμμές) και η μέση κανονικοποιημένη απόσταση Hammingγια την intra-distanceυπολογίστηκε στα 0.12 ± 0.03 . Αυτές οι τιμές συνδέονται με το SNRστις φωτοδιόδους. Στο δεύτερο ιστόγραμμα που φαίνεται με πράσινο απεικονίζεται η κανονικοποιημένη απόσταση Hammingγια αποκρίσεις που προέρχονται από $5.5*10^5$PUFs στα οποία έχει εφαρμοστεί η ίδια πρόκληση αλλά υπόκεινται σε θόρυβο κατά την ανίχνευση . Κάθε PUFδιέφερε σε σχέση με το ιδανικό σύμφωνα με τον πίνακα 1 . Εδώ , η Gaussianfit(πράσινες τελείες) μας δίνει μια μέση τιμή inter-distance0.48± 0.04 . Αυτές οι τιμές συνδέονται με τις κατασκευαστικές ατέλειες . Αυτό δείχνει ότι οι εγγενείς οριακές διαφορές στο κρυφό στρώμα του RCπροβάλλονται στο στρώμα εξόδου προσφέροντας σημαντικά υψηλότερη απόσταση συγκριτικά με την περίπτωση intra. Μια πραγματικά τυχαία διαδικασία αναμένεται να δώσει μία τιμή 0.5 στην inter-distanceεπομένως η συγκεκριμένη υλοποίηση φαίνεται ότι αποτελεί μια πραγματική στοχαστική διαδικασία . Οι κατανομές έχουν μηδενική επικάλυψη αλλά η ασφάλεια δεν πρέπει να αρκεστεί μόνο σε αυτό .

Για να αξιολογήσουμε αν κάθε απόκριση του PUFφτιάχνει μια τυχαία ακολουθία εφαρμόστηκε το ψευδό-τυχαίο NISTtest. Σε αντίθεση με συμβατικές περιπτώσεις , εδώ οι αποκρίσεις δεν παράγονται από μία μόνο γεννήτρια αλλά προέρχονται από διαφορετικά PUFs . Η επιτυχία στο NISTtestσηματοδοτεί ότι η πρόσβαση σε αποκρίσεις από ένα προηγούμενο RCPUFδεν δίνουν καμία πληροφορία για τις μελλοντικές αποκρίσεις του

RCPUF. Για να τροφοδοτηθούν τα δεδομένα στο NISTtest, και οι 5.5 * 10^5 μοναδικές δυαδικές αποκρίσεις των PUFsενώθηκαν σχηματίζοντας 1000 δυαδικές συμβολοσειρές με την κάθε μία να έχει περίπου μήκος 140Kbit . Έτσι είναι εφικτό να έχουμε ένα μεγάλο σύνολο δεδομένων ώστε να πραγματοποιήσουμε 10 δοκιμές NISTSTS με επίπεδο εμπιστοσύνης α=0.01 . Τα αποτελέσματα των testαυτών φαίνονται στον πίνακα 2 που ακολουθεί :

Test	Success rate	Outcome/Optimal Value
Frequency	100%	success
Block Frequency	100%	success
Cumulative Sums	100%	success
Runs	98.9%	success
Longest Runs	99.7%	success
Rank	99.4%	success
FFT	98.9%	success
Non-Periodic Template Matching	100%	success
Overlapping Template Matching	98.6%	success*
Approximate entropy	98.7%	success
Serial	99.5%	success
Universal Statistical	98.5%	success *
Random Excursions	97.3%	success *
Random Excursion Variant	97.3%	success *
Linear Complexity	92%	success *

Πίνακας 2 : Τεστ που εφαρμόστηκαν για την αξιολόγηση του NISTSTS (Charis Mesaritakis D. D., 2022)[2]

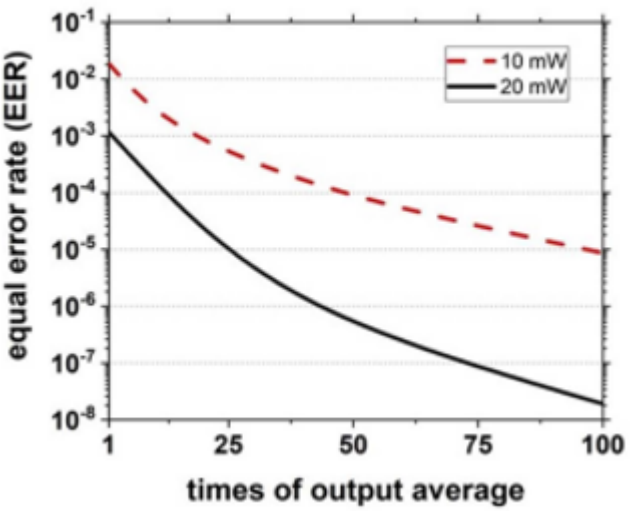
Όπως φαίνεται η συγκεκριμένη υλοποίηση PUFείναι κρυπτογραφικά συμβατή για όλες αυτές τις δοκιμές (χωρίς αστερίσκο). Οι δοκιμές με αστερίσκο (5 δοκιμές) απαιτούν ένα μέγεθος δυαδικής συμβολοσειράς τουλάχιστον 1 Gbitώστε να διασφαλιστεί η απαραίτητη στατιστική ακρίβεια . Προκειμένου να επιτευχθεί αυτό το μέγεθος για αυτές τις 5 δοκιμές ,

πραγματοποιήθηκαν μεταθέσεις των αρχικών $5.5*10^5$αποκρίσεωνμεγέθους 256 bits . Δηλαδή δεν περιέχονται νέες ή τροποποιημένες αποκρίσεις , απλά έγιναν αλλαγές της σειράς τους από την αρχική . Έτσι , η συγκεκριμένη υλοποίηση περνά και τις 5 αυτές δοκιμές με ένα βαθμό εμπιστοσύνης α=0.01 . Άρα είναι επιτυχές για όλες τις δοκιμές όπως φαίνεται και στον πίνακα.

Έλεγχος ταυτότητας στο RCPUF

Ένα αδύναμο PUFμπορεί να χρησιμοποιηθεί σαν διακριτικό ελέγχου ταυτότητας . Η αρχή γνωρίζει και αποθηκεύει την δυαδική απόκριση του PUFστη φάση εγγραφής. Όταν μια συσκευή θέλει να ταυτοποιηθεί , η απόκριση που παράγει συγκρίνεται με την αποθηκευμένη. Έτσι , μέσω των κατανομών που είδαμε στην εικόνα , μπορεί να υπολογιστεί η πιθανότητα ενός ψευδώς αρνητικού (να απορριφθεί ένα σωστό PUF) και ενός ψευδώς θετικού (να γίνει αποδοχή ενός άλλουPUF) . Κάθε κατανομή προσαρμόζεται θεωρώντας ότι είναι Gaussianκαι το όριο για τον καθορισμό του ελέγχου ταυτότητας (θετικό ή αρνητικό) τίθεται στο σημείο τομής. Αυτές οι πιθανότητες είναι ίσες και συμβολίζονται ως ERR(ίσο ποσοστό σφάλματος) . Στην περίπτωση μας , οι κατανομές intraκαι inter έχουν τιμή ERR = $1.9*10^{-8}$δηλαδή σχεδόν αμελητέα .

Η απόδοση της υλοποίησης αυτής επηρεάζεται από το SNR. Στην παρακάτω εικόνα υπολογίζεται το ERRσυναρτήσει του αριθμού των μέσων όρων για 2 διαφορετικά επίπεδα μέγιστη ισχύος P_{max}.



Εικόνα 35: Διάγραμμα ERR συναρτήσει του αριθμού των μέσων όρων εξόδου για 2 διαφορετικές τιμές μέγιστης ισχύος . (Charis Mesaritakis D. D., 2022)[2]

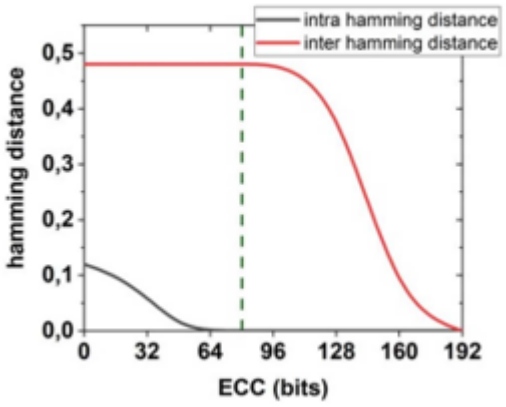
Αυξάνοντας τον αριθμό των μέσων όρων το ERRπέφτει αρκετά για κάθε περίπτωση .Η αύξηση του SNRέχει ως αποτέλεσμα την μείωση της μέσης τιμής της intraαπόστασης Hamming .Αυτό βέβαια αυξάνει λίγο την καθυστέρηση της συσκευής , πράγμα όμως που είναι χαμηλής σημασίας λόγω της απίστευτα γρήγορης λειτουργίας της νευρομορφικής συσκευής , συγκεκριμένα μεγαλύτερη των 40 Gsymbol/sec . Ας δούμε τι συμβαίνει αν αυξήσουμε την μέγιστη ισχύ εισόδου από 10 σε 20 mW. Το ERRβλέπουμε πάλι ότι μειώνεται . Για παράδειγμα , διπλασιάζοντας την ισχύ εισόδου για 50 μέσους όρους , το ERRπέφτει από 10^{-4} σε $8*10^{-7}$.Λαμβάνοντας υπόψιν ότι η inter-distanceσχετίζεται με την προσπάθεια κλωνοποίησης από

κακόβουλους κατασκευαστές , το ERRστην περίπτωση μας πολύ εύκολα πέφτει κάτω από 10^{-6} . Αυτή η πιθανότητα είναι παρόμοια με τα ογκώδη οπτικά PUFs.

Αποθήκευση κρυπτογραφικού κλειδιού στο RCPUF

Όταν θέλουμε να χρησιμοποιήσουμε το PUFγια αποθήκευση κρυπτογραφικού κλειδιού θα πρέπει η απόσταση intra Hamming να είναι 0 . Αυτό σημαίνει ότι χρησιμοποιώντας την ίδια πρόκληση επάνω στο ίδιο PUFθα παίρνουμε πάντα την ίδια απόκριση παρά την ύπαρξη θορύβου. Χρειαζόμαστε για αυτό το λόγο μέτρα όπως ο κώδικας διόρθωσης σφαλμάτων (ECC). Αυτό δεν επιφέρει έξτρα βάρος στη συσκευή .

Έτσι , τροποποιείται η ακολουθία παραγωγής αποκρίσεων , υπολογίζοντας ECC bits πολλών μηκών . Όταν χρειάζεται η επαναπαραγωγή μιας απόκρισης δηλαδή στην περίπτωση της ίδιας πρόκλησης πάνω στο ίδιο PUF , αυτά τα ECC bits χρησιμοποιούνται για τη διόρθωση των bitsπου αλλοιώθηκαν λόγω θορύβου. Όπως είναι αναμενόμενο , η προσθήκη ECCστην λειτουργία του PUFεπηρεάζει επίσης τα αλλοιωμένα bitsπου προέρχονται από χρήση ενός διαφορετικού στιγμιοτύπου του PUF. Επίσης , μειώνει των αριθμό των αλλοιωμένων bitsπου προέρχονται από χρήση ενός διαφορετικού PUF. Λαμβάνοντας υπόψιν αυτά , συμπεριλήφθηκαν ECC bits ποικίλων μηκών και υπολογίστηκε ξανά η μέση απόσταση Hammingγια τα σύνολα δεδομένων intraκαι inter.Χρησιμοποιήθηκε η τεχνική BCHγια την διόρθωση σφαλμάτων . Αν ο αριθμός των αλλοιωμένων bitsείναι μεγαλύτερος από αυτόν που μπορεί να διορθώσει ο κώδικας , τότε δεν διορθώνεται κανένα bit.



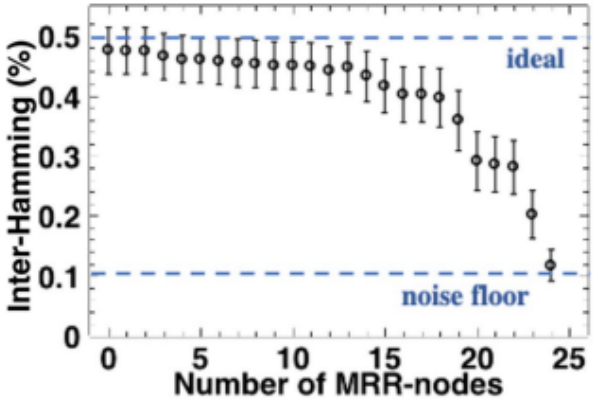
Εικόνα 36: Αποστάσεις Hamming intra και inter συναρτήσει του αριθμού των ECC bits (Charis Mesaritakis D. D., 2022)[2]

Παρατηρούμε ότι για περισσότερα από 100 ECC bitsη inter Hamming distance πέφτει τρομερά , πράγμα που σημαίνει ότι αυξάνεται πολύ η πιθανότητα ενός ψευδώς θετικού ελέγχου ταυτότητας . Από την άλλη , για λιγότερα από 60 ECC bits τα αλλοιωμένα bits λόγω θορύβου αυξάνονται . Συνεπώς , αυτό το σχήμα δεν είναι κατάλληλο για εφαρμογές παραγωγής κλειδιών . Η βέλτιστη περιοχή όπως βλέπουμε είναι ανάμεσα στα 64 και τα 96 ECC bits . Αυτή η τιμή συνδέεται άμεσα με το SNR ,συμπεραίνοντας ότι για χαμηλότερη οπτική ισχύ , δεν θα υπήρχε ένα τέτοιο σημείο .

Ανθεκτικότητα στην αντιγραφή

Η φυσική μη κλωνοποιησιμότητα του PUFθα πρέπει να συνοδεύεται από ένα μηχανισμό που ο χώρος των παραμέτρων του είναι τόσο μεγάλος ώστε να αποτρέπει εξαντλητικές επιθέσεις .

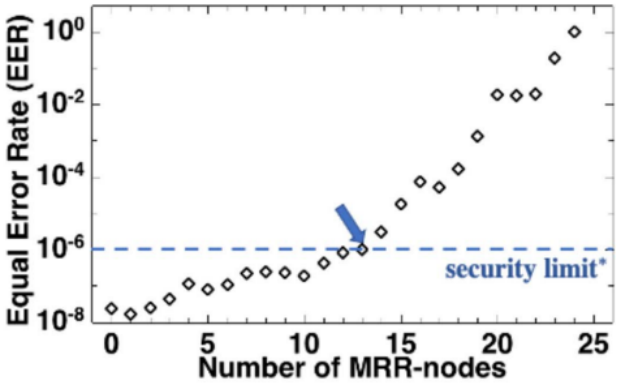
Έτσι , υλοποιήθηκε ένα πρωτότυπο PUFμε μέγιστη ισχύ 20mWκαι 100 μέσους όρους και 24 κόμβους . Με βάση αυτό , παρήχθησαν πολλά setαπό PUFsόπου σε κάθε set ένας αριθμός X από κόμβους (MRRs) είναι ίδιοι με τους κόμβους του πρωτοτύπου , γνωστοί δηλαδή στον επιτιθέμενο . Κάθε setαποτελείται από 1000 PUFsκαι ο αριθμός X των όμοιων κόμβων κυμαίνεται από 0 μέχρι 24 . Πρακτικά το 0 σημαίνει ότι όλοι οι κόμβοι είναι διαφορετικοί ενώ το 24 σημαίνει ότι όλοι οι κόμβοι είναι ίδιοι με το πρωτότυπο. Η εξωτερική απόσταση Hamming υπολογίζεται συναρτήσει του αριθμού των κόμβων .



Εικόνα 37: Διάγραμμα της απόστασης inter Hamming συναρτήσει του αριθμού κόμβων (Charis Mesaritakis D. D., 2022)[2]

Όπως παρατηρούμε μια εξωτερική απόσταση μεγαλύτερη του 0.4 μπορεί να διατηρείται ακόμη και αν ο αντίπαλος έχει βρει τις ιδιότητες 20 κόμβων.

Παρακάτω βλέπουμε το EERσυναρτήσει του αριθμού των κόμβων.



Εικόνα 38: Διάγραμμα του ERR συναρτήσει του αριθμού των κόμβων (Charis Mesaritakis D. D., 2022)

Το όριο ασφαλείας που έχει τεθεί είναι το ERRνα ισούται με 10^{-6}. Αυτό σημαίνει ότι θα πρέπει ο επιτιθέμενος να έχει ακριβή γνώση τουλάχιστον 14 κόμβων από τους 24(ποσοστό 58%) ώστε η ασφάλεια να τίθεται σε κίνδυνο και το ERRνα είναι μεγαλύτερο του 10^{-6} .

Ο χώρος των παραμέτρων ισούται με 256^{14} = 5.1 * 10^{33} . Αυτή η τιμή μπορεί να αυξηθεί περισσότερο αυξάνοντας τον αριθμό των κόμβων του RC . Σε ένα ρεαλιστικό σενάριο 50 κόμβων , ο αριθμός αυτός αυξάνεται σε 256^{29}= 7*10^{64} δεδομένου του ίδιου ERR και του ίδιου ποσοστού κόμβων που ο αντίπαλος λαμβάνει γνώση. Αν σε αυτό τον αριθμό προστεθεί και η εκπαίδευση γραμμικής παλινδρόμησης για δείγμα 2000 για κάθε επίθεση μίμησης , μια εξαντλητική επίθεση δεν είναι πρακτικά εφικτή.

Το συμπέρασμα είναι ότι η αύξηση των κόμβων καθιστά τέτοιου είδους επιθέσεις υπερβολικά δύσκολες . Αν η εκπαίδευση δικτύου λαμβάνει χώρα σε έναν επεξεργαστή , η πολυπλοκότητα κλιμακώνεται πολυωνυμικά για το σύστημα αλλά εκθετικά για τον επιτιθέμενο . Με παράλληλη ψηφιακή επεξεργασία μπορεί να διατηρηθεί η ταχύτητα παραγωγής κλειδιών .

Κεφάλαιο 5: PUFs βασισμένα σε πλατφόρμες πυριτίου

Στα προηγούμενα κεφάλαια έγινε ανάλυση στο πεδίο των οπτικών PUFs . Υπάρχουν όμως και άλλοι τύποι PUFs με τον μεγαλύτερο να αποτελούν τα PUFs βασισμένα σε πλατφόρμες πυριτίου (Silicon cast PUFs). Θα γίνει ανάλυση κάποιων παραδειγμάτων αυτής της κατηγορίας και στη συνέχεια θα γίνει σύγκριση με τα οπτικά ώστε να εξαχθούν τα κατάλληλα συμπεράσματα.

Τα Silicon cast PUFs είναι μια υποκατηγορία των ηλεκτρονικών PUFs .Τα ενσωματωμένα κυκλώματα παρουσιάζουν φυσικές ανωμαλίες κατά τη διαδικασία παραγωγής τους . Τα PUFs πυριτίου είναι απτά πιο πολυσυζητημένα PUFs για την παραγωγή μοναδικών ψηφιακών υπογραφών που λειτουργούν σαν το δακτυλικό αποτύπωμα του ενσωματωμένου κυκλώματος.

Η διαδικασία παραγωγής επηρεάζεται κυρίως από πολλούς παράγοντες. Σε μεγάλης κλίμακας ηλεκτρονικά κυκλώματα η επιρροή αυτή είναι πολύ σημαντική . Η αξιοπιστία και η σταθερότητα της εξόδου ενός silicon PUF επηρεάζεται πέραν του ιδίου του PUF και από περιβαλλοντικούς παράγοντες. Η διακύμανση των περιβαλλοντικών συνθηκών επηρεάζει τη λειτουργία του κυκλώματος και συνεπώς την έξοδο του PUF ή της συσκευής στην οποία είναι ενσωματωμένο .Τέτοιες μπορεί να είναι η θερμοκρασία , η τροφοδοσία ρεύματος αλλά ακόμη και η γήρανση του κυκλώματος.

Τα PUFs πυριτίου ενσωματώνονται σε πυρίτιο για να πετύχουμε τους στόχους που θέλουμε και να εκμεταλλευτούμε την διαδικασία παραγωγής . Είναι τα πιο απλά PUFs καθώς δεν απαιτείται καμία τροποποίηση στη διαδικασία παραγωγής για να μπορούμε να τα χρησιμοποιήσουμε . Εκμεταλλεύονται τις παραλλαγές κατασκευής των transistor και καλωδίων που διαφέρουν από ένα κύκλωμα σε ένα άλλο ακόμη και αν αποτελούν μέρους της ίδιας γκοφρέτας πυριτίου. Το arbiter PUF που είναι το πρώτο PUF πυριτίου .

Με γνώμονα τις πηγές παραλλαγής , τα PUFs πυριτίου χωρίζονται σε 3 κύριες κατηγορίες :

1) Τα PUFs που βασίζονται στην καθυστέρηση
2) Τα PUFs που βασίζονται σε μνήμη
3) Τα αναλογικά ηλεκτρονικά PUFs

PUFs βασισμένα στην καθυστέρηση

Arbiter PUF (PUF διαιτητής)

Το PUF «διαιτητής» είναι ένα τύπος PUF βασισμένου σε πλατφόρμα πυριτίου που βασίζεται στην καθυστέρηση . Η ιδέα πίσω από αυτή την κατασκευή είναι η εξής :

Εισάγεται σαφώς μια συνθήκη αγώνα μεταξύ δύο ψηφιακών μονοπατιών σε ένα τσιπ πυριτίου . Και οι δύο διαδρομές καταλήγουν σε ένα κύκλωμα «διαιτησίας» που θα επιλύσει τον αγώνα και θα μετρήσει ποιο από τα δύο μονοπάτια ήταν πιο γρήγορο και θα βγάλει σαν έξοδο την ανάλογη δυαδική τιμή . Σε περίπτωση που έχουν σχεδιαστεί ώστε να έχουν την ίδια ονομαστική καθυστέρηση δεν μπορεί να προσδιοριστεί με σαφήνεια βάσει της συγκεκριμένης σχεδίασης . Υπάρχουν δύο πιθανά σενάρια.

Σενάριο 1 :

Ακόμη και αν σχεδιαστικά εισάγουμε τις ίσες ονομαστικές καθυστερήσεις και για τα δύο μονοπάτια , η πραγματική καθυστέρηση δεν θα είναι ίση . Αυτό συμβαίνει εξαιτίας των τυχαίων μεταβολών που παρουσιάζονται στο τσιπ πυριτίου . Έτσι θα υπάρξει μια τυχαία διαφορά καθυστέρησης μεταξύ των δύο μονοπατιών η οποία θα καθορίσει και το αποτέλεσμα του αγώνα . Αυτές οι μεταβολές είναι τυχαίες ανά συσκευή , όμως είναι σταθερές για μια συγκεκριμένη συσκευή . Οπότε η διαφορά καθυστέρησης και συνεπώς η έξοδος έχουν να κάνουν αποκλειστικά με τη συσκευή.

Σενάριο 2 :

Υπάρχει μια μικρή αλλά όχι αμελητέα πιθανότητα ότι κατά τύχη και οι δύο καθυστερήσεις είναι σχεδόν ίσες. Σε αυτή την περίπτωση , όταν στείλουμε ταυτόχρονα δύο σήματα και στις δύο διαδρομές , υπάρχει η πιθανότητα να φτάσουν στον διαιτητή την ίδια στιγμή . Εάν συμβεί αυτό ο διαιτητής εισέρχεται σε μια κατάσταση όπου η λογική έξοδος του κυκλώματος είναι προσωρινά απροσδιόριστη . Μετά από ένα σύντομο αλλά τυχαίο χρόνο , ο διαιτητής φεύγει από αυτήν την κατάσταση και εξάγει μια τυχαία δυαδική τιμή η οποία δεν έχει να κάνει καθόλου με τον αγώνα . Στην προκειμένη , η έξοδος δεν έχει να κάνει καθόλου με τη συσκευή και δεν είναι σταθερή . Αυτό το φαινόμενο του θορύβου είναι ο λόγος που οι αποκρίσεις των arbiter PUFs είναι αναξιόπιστες .

Ας δούμε την υλοποίηση των δύο μονοπατιών καθυστέρησης σαν αλυσίδες από switchblocks . Ένα switch block συνδέει δύο σήματα εισόδου στα δύο εξόδου σε μια από τις δύο πιθανές κατευθύνσεις , ευθεία ή σταυρωτά με βάση ένα bit επιλογής της κατεύθυνσης . Κάθε switch block έχει 2 εξόδους και 3 εισόδους οι οποίες είναι : οι 2 έξοδοι του προηγούμενου σταδίου και το bit της πρόκλησης. Οι είσοδοι του πρώτου switch block συνδέονται με ένα συνηθισμένο σήμα ενεργοποίησης και οι έξοδοι του τελευταίου switch block συνδέονται στο arbiter block που θα καθορίσει ποιο σήμα έφτασε πρώτο και άρα θα παράγει το ανάλογο bit απόκρισης.

Ο πιο απλός τρόπος να φτιάξουμε κάτι τέτοιο, είναι με ένα ζεύγος πολυπλεκτών 2 προς 1. Ενώνοντας τα μπλοκ διακοπτών , χρειαζόμαστε n bits για τη διαμόρφωση οποιουδήποτε από τα 2^n πιθανά ζευγάρια μονοπατιών καθυστέρησης. Αυτή η ρύθμιση n-bit θα αποτελεί την πρόκληση του arbiter PUF. Επειδή οι καθυστερήσεις εισόδου-εξόδου των διαμορφώσεων ενός switch blocks δεν είναι ίσες και επηρεάζονται από μεταβολές κατά τη διαδικασία , κάθε πρόκληση από τις 2^n προκλήσεις που διαθέτουμε οδηγεί σε μια νέα συνθήκη αγώνα που πρέπει να επιλυθεί από τον διαιτητή. Η έξοδος που θα μας δώσει ο διαιτητής θεωρείται η απόκριση του arbiter PUF στην συγκεκριμένη πρόκληση . Αυτές οι 2^n διαφορετικές διαμορφώσεις δεν είναι ανεξάρτητες , αφού βασίζονταισε ένα αριθμό από παραμέτρους καθυστέρησης που είναι γραμμικές ως προς n.

Το κύκλωμα arbiter μπορεί να επιτευχθεί με πολλούς τρόπους , με πιο απλό αυτό των SR NAND latch .

Ιδανικά , η απόκριση του arbiter PUF καθορίζεται αποκλειστικά από την τυχαία επίδραση των μεταβολών κατά τη διαδικασία στις παραμέτρους καθυστέρησης του κυκλώματος . Αυτό μπορεί να συμβεί αν πληρούνται οι δύο παρακάτω προϋποθέσεις :

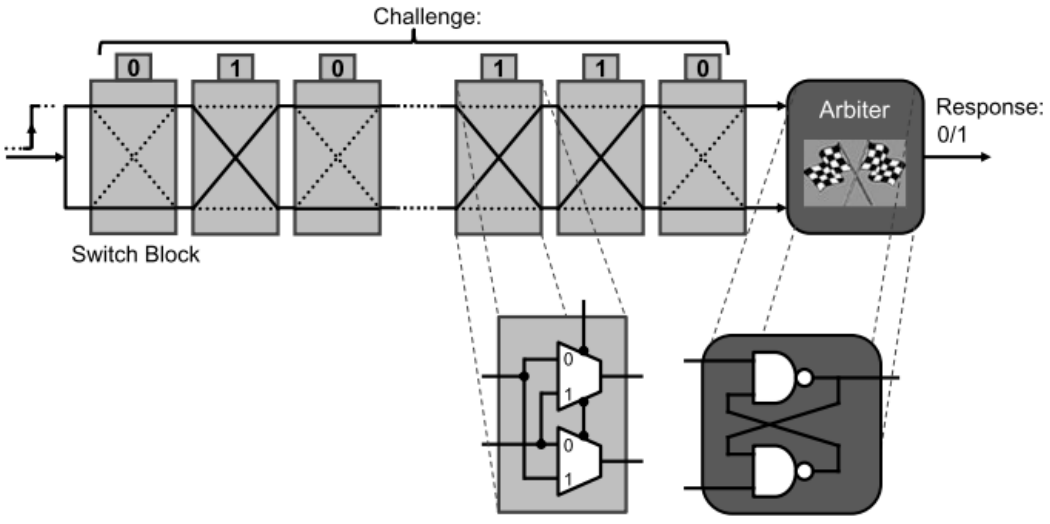
1 Οι γραμμές καθυστέρησης πρέπει να έχουν σχεδιαστεί ώστε να είναι απολύτως συμμετρικές και οποιαδήποτε διαφορά στην καθυστέρηση να προκύπτει από τις τυχαίες μεταβολές της διαδικασίας.

2 Το κύκλωμα arbiter είναι δίκαιο , δηλαδή δεν ευνοεί καμία είσοδο σε βάρος κάποιας άλλης εισόδου .

Αν έστω μία από τις παραπάνω προϋποθέσεις δεν ικανοποιείται , τότε οι αποκρίσεις που θα δώσει το arbiter PUF θεωρείται ότι θα είναι χαμηλής μοναδικότητας .

Ο σχεδιασμός ενός εντελώς αμερόληπτου arbiter PUF θεωρείται πολύ σημαντικός καθώς απαιτεί έλεγχο της υλοποίησης σε χαμηλό επίπεδο .
FPGAS
Επειδή πολλές φορές μπορεί η αμεροληψία να μη μπορεί να επιτευχθεί , υπάρχουν κάποιες τεχνικές για την εξουδετέρωση της μεροληψίας . Μπροστά από το arbiter PUF τοποθετείται ένα ρυθμιζόμενο κύκλωμα καθυστέρησης , το οποίο μπορεί να εξουδετερώσει την ντετερμινιστική μεροληψία των μονοπατιών καθυστέρησης ή του διαιτητή .
Για παράδειγμα αν ο διαιτητής ευνοεί το πάνω μονοπάτι καθυστέρησης , το κύκλωμα ρυθμιζόμενης καθυστέρησης θα δώσει στο κάτω μονοπάτι ένα προβάδισμα . Αυτό μπορεί να επιτευχθεί αλλάζοντας έναν αριθμό από τα bit πρόκλησης στην αρχή της αλυσίδας του μπλοκ διακοπτών ώστε να εξουδετερωθεί η μεροληψία .

Στο παρακάτω σχήμα βλέπουμε την κατασκευή ενός arbiter PUF.



Εικόνα 39 : Σχήμα ενός Arbiter PUF

(Fahem Zerrouki, 2022)[5]

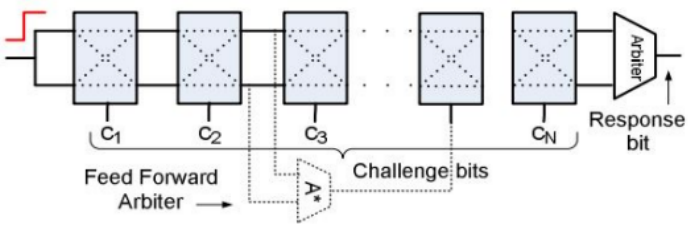
Η βασική κατασκευή ενός arbiter PUF με μια αλυσίδα από n switch blocks μπορεί να μας παρέχει όπως αναφέραμε 2^n διαφορετικές προκλήσεις . Όμως ο αριθμός των παραμέτρων καθυστέρησης που καθορίζουν τις αποκρίσεις ενός arbiter PUF έχει γραμμική σχέση με το n. Αυτό σημαίνει στην πράξη ότι το σχήμα θα είναι είτε μια ευθεία είτε μια καμπύλη . Αυτό όμως σημαίνει ότι αυτές οι 2^n διαφορετικές προκλήσεις δεν μπορούν να παράγουν ανεξάρτητες αποκρίσεις . Το πρόβλημα είναι ότι αν κάποιος μάθει τις παραμέτρους καθυστέρησης και μπορέσει να μοντελοποιήσει την αλληλεπίδραση με τα bit πρόκλησης , μπορεί να προβλέψει τα bit απόκρισης σε τυχαίες προκλήσεις με ακρίβεια , ακόμα και μη έχοντας πρόσβαση στο PUF. Οι αποκρίσεις του arbiter PUF μπορούν να θεωρηθούν απρόβλεπτες μόνο αν ένα τέτοιο μοντέλο δεν είναι εφικτό να φτιαχτεί με ακρίβεια .

Παρατηρήθηκε ότι το απλό arbiter PUF μπορεί πράγματι να μοντελοποιηθεί εύκολο . Οι επιθέσεις μοντελοποίησης προϋποθέτουν ένα απλό αλλά ακριβές προσθετικό μοντέλο καθυστέρησης για το arbiter PUF . Έτσι , η καθυστέρηση ενός ψηφιακού κυκλώματος μοντελοποιείται ως το άθροισμα των καθυστερήσεων των σειριακών συνιστωσών του . Για τις απλές αλυσίδες switchblocks αυτό αποδεικνύεται αρκετά ακριβές. Οι άγνωστες παράμετροι καθυστέρησης μπορούν να μαθευτούν από την παρατήρηση ζευγαριών πρόκλησης-απόκρισης του PUF. Κάθε τέτοιο ζευγάρι συνιστά μια γραμμική ανισότητα και χρησιμοποιείται για την απόκτηση όσο το δυνατόν ακριβέστερης προσέγγισης . Επιπλέον , οι άγνωστες παράμετροι δεν χρειάζεται καν να υπολογιστούν ρητά , καθώς με έναν αλγόριθμο μηχανικής μάθησης υπολογίζονται αυτόματα .

Ο σκοπός τέτοιων επιθέσεων μοντελοποίησης είναι να προβλεφθούν οι αποκρίσεις με τη μέγιστη δυνατή ακρίβεια έχοντας εκπαιδευτεί όσο το δυνατόν με λιγότερα παραδείγματα .

Feed forward arbiter PUF

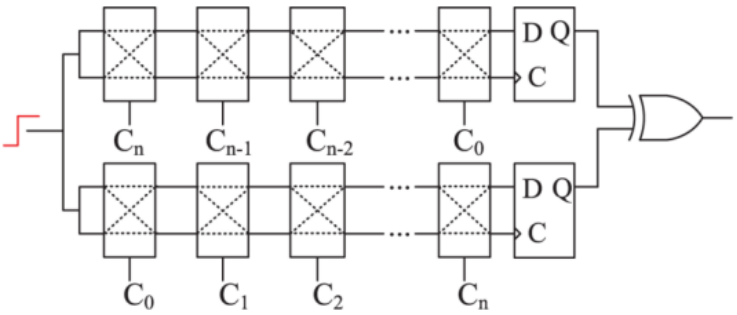
Στο arbiter PUF εκμεταλλευόμαστε τη γραμμικότητα των μονοπατιών καθυστέρησης . Όμως αυτό έχει αποδειχθεί ότι είναι ευάλωτο σε επιθέσεις μηχανικής μάθησης. Έτσι εφευρέθηκε το Feed forward arbiter PUF ή FF APUF που αποτελεί μια προέκταση του βασικού arbiter PUF όπου κάποια από τα bit πρόκλησης παράγονται εγγενώς από έναν ενδιάμεσο arbiter . Αυτές οι προκλήσεις είναι κρυμμένες από τον αντίπαλο. Στην εικόνα βλέπουμε ένα FF APUF με έναν Feed forward arbiter.



Εικόνα 40 :Feed Forward APUF με 1 feed forward Arbiter (Fahem Zerrouki, 2022)[5]

XOR PUF

Μια άλλη υλοποίηση χρησιμοποιώντας arbiter είναι το XOR Arbiter PUF. Το XOR PUF συνδυάζει πολλές σειρές του βασικού arbiter PUF , παίρνει την έξοδο του κάθε arbiter PUF και την κάνει XOR ώστε να προκύψει ένα bit απόκρισης . Σε αυτή την υλοποίηση μετράμε δύο βασικές παραμέτρους .Η πρώτη είναι το μήκος του αριθμού των μπλοκ εναλλαγής (switch blocks) της πρόκλησης . Η δεύτερη είναι ο αριθμός των σειρών που δείχνει το μέγεθος εισόδου της XOR. Στην εικόνα βλέπουμε ένα 2 XOR PUF με 2 σειρές από n switch blocks.

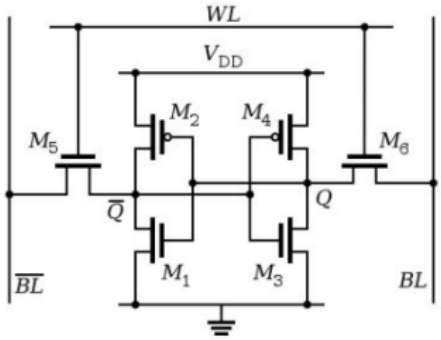


Εικόνα 41:Σχήμα ενός XOR PUF (Fahem Zerrouki, 2022)[5]

PUFs βασισμένα στη μνήμη

Η απόκριση αυτών των PUFs εξαρτάται από την αρχική κατάσταση των δομών μνήμης . Με την ενεργοποίηση , οι δομές τίθενται σε ασταθή κατάσταση και η απόκριση αντιστοιχεί στην σταθερή κατάσταση που θα προκληθεί από μια είσοδο ενός εξωτερικού σήματος δεδομένων .Ας δούμε το παράδειγμα του SRAM PUF.

Το SRAM PUF είναι η πρώτη εγγενής κατασκευή PUF που βασίζεται στην κατάσταση ενεργοποίησης μιας μνήμης SRAM ενός FPGA. Βασίζονται στο περιθώριο στατικού θορύβου (SNM) που απαιτεί κελί μνήμης για την αλλαγή της λογικής τιμής. Ένα τέτοιο κελί είναι κατασκευασμένο ώστε να οδηγεί σε δύο σταθερές καταστάσεις. Κατά την ενεργοποίηση, δίνεται τυχαία η τιμή των κελιών 0 ή 1από το SNM. Η τυχαιότητα οφείλεται στη διαδικασία κατασκευής του κελιού της SRAM. Ως πρόκληση του SRAM PUF χρησιμοποιείται ένα εύρος τοποθεσιών μνήμης ενός block της SRAM και οι αποκρίσεις είναι οι αρχικές τιμές όλων των κελιών της SRAM που συνέθεσαν την πρόκληση . Στην εικόνα βλέπουμε τη σχεδίαση ενός κελιού SRAM PUF με 6 transistors .

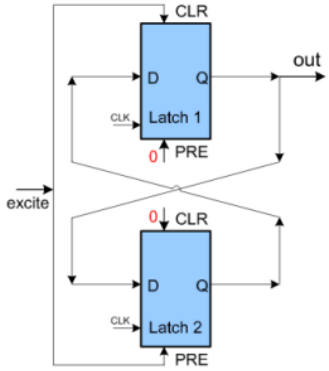


Εικόνα 42: Σχήμα ενός κελιού του SRAM PUF (Fahem Zerrouki, 2022)[5]

Όπως είπαμε , οι αρχικές τιμές των κελιών ελέγχονται από τον κατασκευαστή του κυκλώματος . Αυτό τα καθιστά άχρηστα για FPGAs. Τα SRAM PUFs χρησιμοποιούνται μόνο σε FPGAs που υποστηρίζουν SRAM μνήμη που παίρνει τιμή κατά την ενεργοποίηση .Για το λόγο αυτό προτάθηκαν κάποιες αλλαγές .

Butterfly PUF

Αλλάζοντας τον αντιστροφέα με flip-flops ή latches (κρατάνε μία δυαδική τιμή 0 ή 1) φτιάχνεται ένα διασταυρούμενο κύκλωμα που αποκαλείται Butterfly PUF. Στην εικόνα βλέπουμε ένα BPUF.



Εικόνα 43: Σχήμα ενός Butterfly PUF (Fahem Zerrouki, 2022)[5]

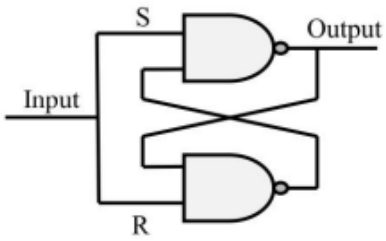
Εδώ βλέπουμε τα 2 latches όπου κάθε latch είναι ενα διασταυρούμενο κύκλωμα . Αυτό το κύκλωμα έχει 2 διαφορετικές σταθερές καταστάσεις λειτουργίας 0 ή 1 και μία ασταθή κατάσταση λειτουργίας . Η ασταθής κατάσταση μπορεί να οριστεί ώς αυτή μετά την οποία το κύκλωμα συγκλίνει πίσω σε μία από τις σταθερές καταστάσεις . Αυτή την τυχαία ανάθεση τιμήςτης σταθερής κατάστασης από την ασταθή εκμεταλλεύεται το BPUF για να παράξει το μυστικό κλειδί . Αυτή η ανάθεση συγκρίνεται με την κατάσταση του κελιού SRAM μετά την ενεργοποίηση .

Όπως τα SRAM PUFs , οι αρχικές τιμές των flip-flops σε ένα FPGA μετά την ενεργοποίηση μπορούν να χρησιμοποιηθούν σαν PUF . Αυτά λέγονται D flip-flop PUFs. Και πάλι λόγω κατασκευαστικών παραλλαγών όταν το κύκλωμα ανάβει η κατάσταση εξόδου κάθε flip-flop παίρνει μια τυχαία τιμή 0 ή 1 . Η τυχαιότητα που υπάρχει κατά την ενεργοποίηση στις τιμές του flip-flop είναι περιορισμένη και συνεπώς δεν μπορεί να χρησιμοποιηθεί απευθείας . Χρειάζεται λοιπόν μια αύξηση στην ποιότητα των αποκρίσεων μετά την επεξεργασία . Το πλεονέκτημα του D flip-flop είναι ότι μπορεί εύκολα εφαρμόζεταισε ένα ενσωματωμένο κύκλωμα αλλά δύσκολα εντοπίζεται . Άρα είναι κατάλληλο για να μη μπορεί να υποστεί αντίστροφη μηχανική.

Τα SRAM και D flip-flop PUFs χρειάζονται ενεργοποίηση για να παράγουν τα bit απόκρισης . Αυτό σημαίνει ότι κάθε φορά που θα θέλουμε να έχουμε μια απόκριση θα πρέπει να τα ενεργοποιούμε ξανά.

Σε αντίθεση με τις προηγούμενες σχεδιάσεις , το SR-Latch ή σκέτο Latch PUF παράγει την απόκριση του όταν η είσοδος ενεργοποιείται ταυτόχρονα . Αποτελείται από 2 διασταυρούμενες πύλες NOR . Χρησιμοποιώντας την μετασταθερή κατάσταση αυτών των

πυλών μπορούν να παραχθούν αποκρίσεις χωρίς στην πραγματικότητα να ενεργοποιήσουμε τη συσκευή . Στην εικόνα βλέπουμε ένα κελί SR-Latch.



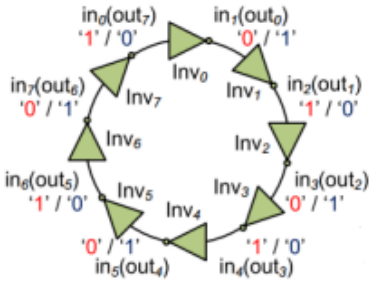
Εικόνα 44 : Κελί ενός SR Latch

Όταν η είσοδος ενεργοποιείται με την άκρη που βλέπουμε , αρχίζει η ταλάντωση του SR-Latch και εισέρχεται σε μία μετασταθερή κατάσταση . Αφού σταματήσει η ταλάντωση γίνεται σταθερό . Λόγω κατασκευαστικών παραλλαγών , η κατάσταση στην οποία θα πέσει το SR-Latch είναι άγνωστη και χρησιμοποιείται ως bit απόκρισης . Ένα τέτοιο PUF δεν είναι κατάλληλο για υλοποιήσεις χαμηλού κόστους .

Τα PUFs που είδαμε παραπάνω , διαθέτουν έναν μικρό αριθμό ζευγαριών πρόκλησης-απόκρισης. Αυτός ο αριθμός είναι ανάλογος του μεγέθους τους . Έτσι αν θέλουμε να τα κατηγοριοποιήσουμε ως weak ή Strong PUFs λόγω αυτού θα ήταν weak. Τα strong PUFs περιέχουν ένα μεγάλο αριθμό ζευγαριών πρόκλησης-απόκρισης .

BistableRing PUF

Είναι πάλι ένα PUF που βασίζεται σε μνήμη αλλά θεωρείται strong PUF. Όπως βλέπουμε και στην εικόνα , αποτελείται από ένα ζυγό αριθμό από αντιστροφείς που συνδέονται μεταξύ τους σχηματίζοντας ένα δακτύλιο .



Εικόνα 45 : Σχήμα ενός Bistable Ring PUF

(Fahem Zerrouki, 2022)[5]

Στο συγκεκριμένο παράδειγμα υπάρχουν 8 αντιστροφείς . Κατά της ενεργοποίηση της συσκευής , κάθε αντιστροφέας προσπαθεί να δώσει την έξοδο του από μία αρχική κατάσταση 0 ή 1. Στην εικόνα που βλέπουμε πάνω , υπάρχουν 2 πιθανές τελικές καταστάσεις : 10101010 ή 01010101 . Έτσι , το αποτέλεσμα του τελευταίου αντιστροφέα είναι και το bit απόκρισης που παράγεται σε συνάρτηση με την κατάσταση στην οποία πέφτει ο δακτύλιος , και αυτή η αρχική κατάσταση συσχετίζεται με την απόκριση . Σε μια αρχιτεκτονική που προτάθηκε , ο αριθμός των αντιστροφέων διπλασιαζόταν ώστε να χρησιμοποιηθεί ως ισχυρό PUF. Έτσι θα

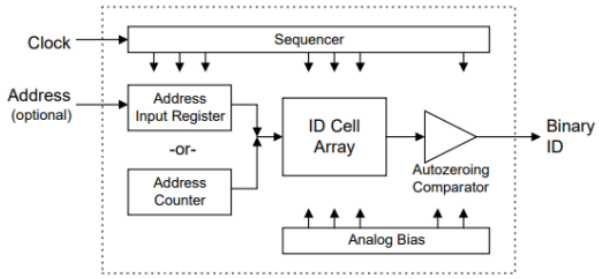
μπορούσαμε να έχουμε εκθετικό αριθμό ζευγαριών πρόκλησης-απόκρισης . Δυστυχώς , τα Bistable Ring PUFs είναι ευάλωτα σε επιθέσεις μηχανικής μάθησης.

Αναλογικά ηλεκτρονικά PUFs

Τα αναλογικά ηλεκτρονικά PUFs βασίζονται στο ότι η απόκριση που δημιουργείται από αυτά εξαρτάται από αναλογικές κινήσεις των ηλεκτρονικών εξαρτημάτων. Τέτοιες είναι η αντίσταση , η χωρητικότητα κλπ. Ας δούμε κάποια παραδείγματα αναλογικών ηλεκτρονικών PUFs.

ICID (IntegratedCircuitIdentification) PUF

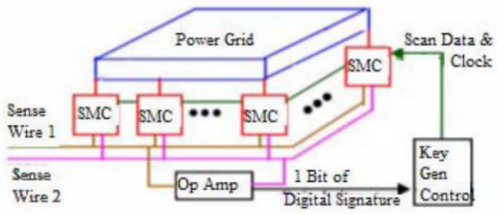
Αυτό το PUF αποτελείται από transistors με πανομοιότυπες σχεδιάσεις που είναι διατεταγμένα σε ένα διευθυνσιοδοτήσιμο πίνακα. Κάθε transistor οδηγεί ένα φορτίο αντίστασης λόγω των κατωφλιών τάσης . Λόγω των ακαθαρσιών στα κανάλια πυριτίου , τα κατώφλια τάσης θεωρείται συνάρτηση τυχαίας τοποθέτησης των ατόμων στα κανάλια πυριτίου. Ως πρόκληση θεωρείται ο αριθμός των transistors και η τάση στο φορτίο που μετριέται , μετατρέπεται σε bit απόκρισης.



Εικόνα 46: Σχήμα ενός ICID PUF[5]

PowerGrid PUF

Οι πτώσεις τάσης και οι ισοδύναμες αντιστάσεις επηρεάζονται από τυχαίες διακυμάνσεις στη διαδικασία παραγωγής . Στο ηλεκτρικό δίκτυο ενός κυκλώματος παρουσιάζονται διακυμάνσεις αντίστασης . Πάνω σε αυτές βασίζεται το PowerGrid PUF . Τα PowerGrid PUFs είναι επίσης ευάλωτα σε επιθέσεις μηχανικής μάθησης . Στην εικόνα βλέπουμε το κύκλωμα για τη δημιουργία απόκρισης χρησιμοποιώντας το δίκτυο ηλεκτρικής ενέργειας.

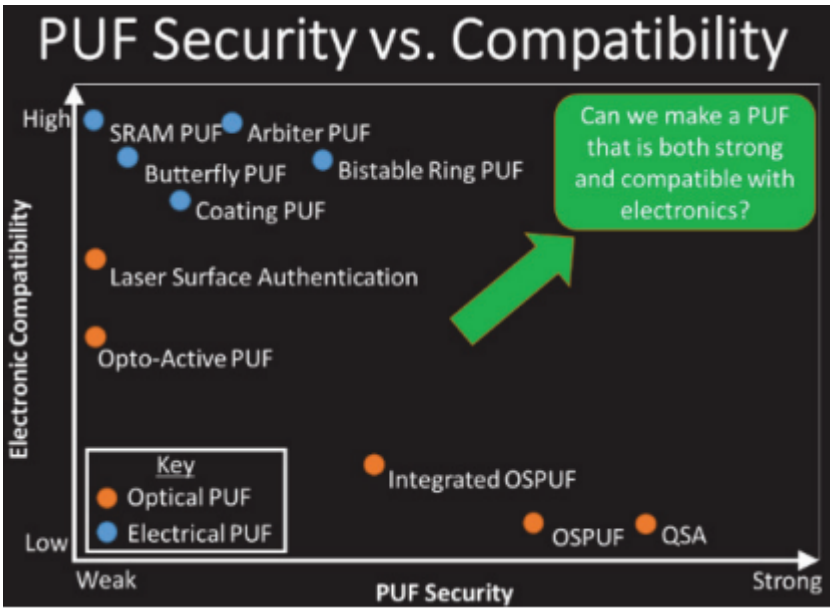


Εικόνα 47: Σχήμα ενός Power Grid PUF (Ouchani, 2022)[5]

Φωτονικά PUFs πυριτίου

Αφού είδαμε πολλά παραδείγματα από PUFs βασισμένα σε πλατφόρμες πυριτίου , θα ήταν ενδιαφέρουν να αναλύσουμε τα φωτονικά PUFs πυριτίου .

Οι ηλεκτρονικές προσεγγίσεις που είδαμε προσφέρουν τη συμβατότητα της ενσωμάτωσης ενός PUF στο hardware και πολλές τέτοιες συσκευές αποδεικνύονται δυνατά PUFs και συνεπώς ο όγκος πληροφορίας στη συσκευή είναι μεγάλος. Παρόλαυτά , οι επιθέσεις μηχανικής μάθησης είναι αρκετά ικανές ώστε να σπάσουν ακόμα και δυνατά ηλεκτρονικά PUFs. Εδώ έρχεται να παίξει το ρόλο του το φως . Το φως λόγω της πλούσιας φύσης και των αλληλεπιδράσεων του με τα μέσα , μας βοηθάει να καταλήγουμε σε εσωτερικά δυνατές συσκευές. Οι οπτικές προσεγγίσεις αποδεικνύονται αρκετά ανθεκτικές απέναντι σε επιθέσεις μηχανικής μάθησης , είναι όμως λόγω των εξαρτημάτων που χρησιμοποιούνται δύσκολα να συσκευαστούν μαζί με ηλεκτρονικά είδη. Για να έχουμε μια εικόνα , ας δούμε τον πίνακα που συγκρίνει τη συμβατότητα με την ασφάλεια πολλών ειδών PUFs.

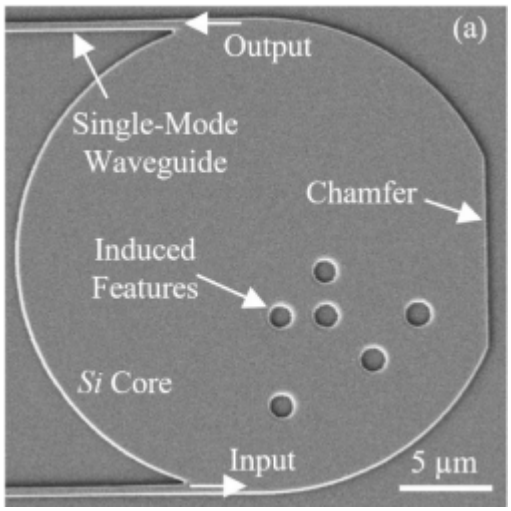


Πίνακας 3: Συμβατότητα συναρτήσει ασφάλειας για πολλά είδη PUF (Fabio Pavanello, 2021)[4]

Όπως καταλαβαίνουμε , υπάρχουν πολλά δυνατά PUFs που όμως δεν είναι συμβατά με τα ηλεκτρονικά hardware και αντίστροφα. Οπότε πρακτικά πρέπει να θυσιάσουμε κάτι για να πάρουμε κάτι άλλο.

Τα μη γραμμικά φωτονικά PUFs πυριτίου σχεδιάστηκαν για να βρεθεί μια ικανή ισορροπία μεταξύ της τεράστιας ασφάλειας που προσφέρουν τα οπτικά κλειδιά σε συνδυασμό με την ηλεκτρονική συμβατότητα των κυκλωμάτων CMOS. Τέτοιες συσκευές είναι συμβατές και με τις 2 προσεγγίσεις κατασκευής επίπεδων ημιαγωγών που χρησιμοποιούνται για ηλεκτρονικά CMOS και hardware οπτικών επικοινωνιών.

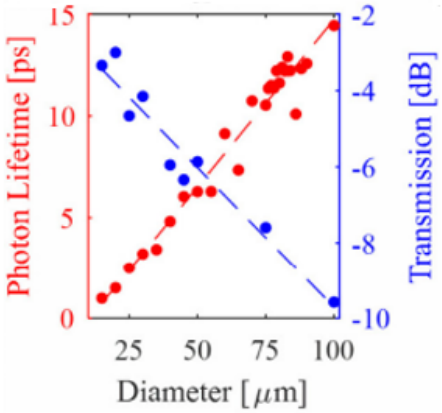
Ένα τυπικό PUF πυριτίου αποτελείται από μια επίπεδη λοξοτμημένη κοιλότητα ενός μικρού δίσκου διαστάσεων περίπου 30μm σε διάμετρο και 250 nm σε ύψος.



Εικόνα 48: Λοξοτμημένη κοιλότητα ενός μικρού δίσκου

(Fabio Pavanello, 2021)[4]

Ας δούμε όμως πως καταλήξαμε στο συμπέρασμα ότι η διάμετρος του δίσκου θα πρέπει να είναι περίπου 30μm. Οι μεγαλύτερες κοιλότητες προσφέρουν το θετικό ότι η ζωή των φωτονίων είναι μεγαλύτερη και συνεπώς μπορούν να παρουσιάζουν υψηλότερη πολυπλοκότητα στη συμπεριφορά τους. Ταυτόχρονα όμως ακριβώς επειδή είναι μεγαλύτερες παρουσιάζουν και υψηλότερες απώλειες από την είσοδο μέχρι την έξοδο . Αντίστοιχα οι μικρότερες κοιλότητες θα έχουν λιγότερες απώλειες αλλά η ζωή των φωτονίων θα είναι μικρότερη και συνεπώς θα έχουμε λιγότερη πιθανή πολυπλοκότητα . Πρέπει λοιπόν να βρεθεί μια χρυσή τομή για την αντιστάθμιση διάρκειας ζωής και απωλειών. Στην εικόνα της προσομοίωσης αποτυπώνονται η ζωή φωτονίου και οι απώλειες για ένα εύρος από διαμέτρους κοιλότητας :



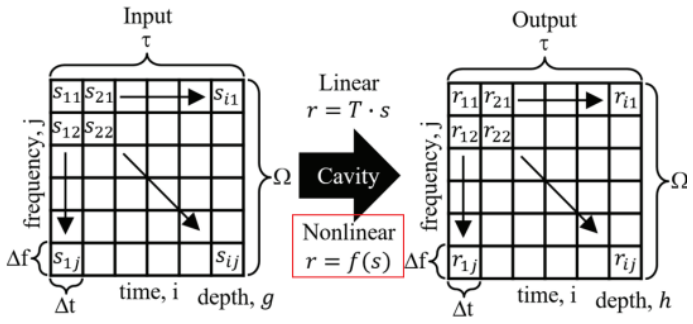
(Fabio Pavanello, 2021)[4]

Εικόνα 49: Ζωή φωτονίου συναρτήσει της διαμέτρου του δίσκου . Δεξιά στον άξονα y το ποσό των απωλειών που έχει κατά της διάρκεια της ζωής του.

Οι ιδιότητες της μη κλωνοποιησιμότητας και της απροβλεπτότητας επιτυγχάνονται μέσω των μικρών μεταβολών στη γεωμετρία της συσκευής που δημιουργούνται κατά την παραγωγή σε

συνδυασμό με το χαοτικό σχεδιασμό αντηχητικής ακτίνας της κοιλότητας. Φως από τηλεπικοινωνιακό laser συνδέεται με την χαοτική οπτική μικροκοιλότητα χρησιμοποιώντας μονότροπους οδηγούς στο ίδιο επίπεδο με το PUF. Αυτό το θεωρούμε την πρόκληση . Για να πάρουμε την απόκριση χρησιμοποιείται τυπικό τηλεπικοινωνιακό hardware . Ο λόγος του σχεδιασμού με λοξότμηση είναι ότι έτσι μπορούμε να συνδέσουμε τους κυματοδηγούς εισόδου και εξόδου και αρκετές χωρικές λειτουργίες μέσα στο αντηχείο .

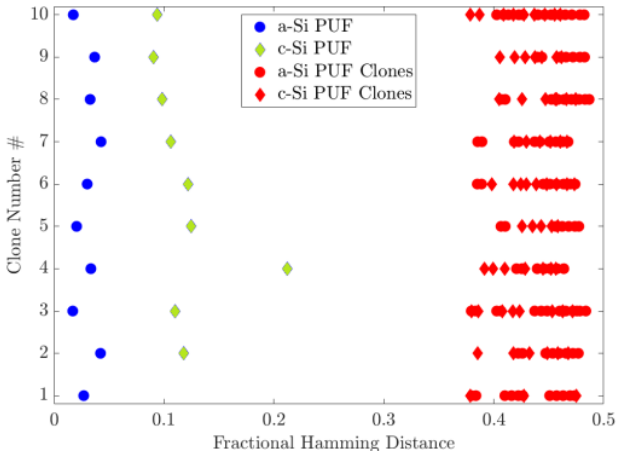
Τα ενσωματωμένα φωτονικά PUF βασίζονται στη χαοτική φύση της κοιλότητας και στις με γραμμικές οπτικές αλληλεπιδράσεις που συμβαίνουν σε αυτήν για να αντλήσουν μεγάλο μέγεθος πληροφοριών . Η μη γραμμικότητα παρέχει μια σύνθετη συνάρτηση χαρτογράφησης μεταξύ της φασματοχρονικής εισόδου και της εξόδου του συστήματος . Ένα απλό γραμμικό σύστημα βασίζεται απλά στην μετάδοση ενός απλού πίνακα . Η διαφορά φαίνεται στην παρακάτω εικόνα:



Εικόνα 50: Διαφορά γραμμικού συστήματος έναντι μη γραμμικού

Για να ελεγχθεί η μη κλωνοποιησιμότητα ας δούμε πως αντιδρούν δύο διαφορετικές υλοποιήσεις φωτονικών PUFs . Τα 2 μοντέλα που εξετάζονται είναι το c-Si (crystalline silicon) και το a-Si (amorphous silicon) . Στις συσκευές c-Si , 10 ακριβή αντίγραφα (κλώνοι) παρήχθησαν στην μικροκοιλότητα του c-Si στην ίδια γκοφρέτα πυριτίου κατασκευασμένα με τον ίδιο τρόπο . Αντίστοιχα στις συσκευές a-Si παρήχθησαν 10 αντίγραφα από την μικροκοιλότητα του a-Si .

Εφαρμόζεται λοιπόν η ίδια πρόκληση σε ακριβή αντίγραφα της ίδιας συσκευής και συγκρίνουμε τις φωτονικές αποκρίσεις του PUF. Φυσικά υπολογίζουμε το πολύ χρήσιμο μετρικό της κλασματικής απόστασης Hamming (FHD) . Η FHD μεταξύ της συσκευής και της αναμενόμενης απόκρισης θεωρείται μια όμοια κατανομή ενώ η FHD μεταξύ της συσκευής και των κλώνων θεωρείται ανόμοια κατανομή .Οι μετρήσεις και στις 2 διαφορετικές υλοποιήσεις δείχνουν ξεκάθαρο διαχωρισμό μεταξύ των αποκρίσεων της κάθε συσκευής και όλων των κλώνων όπως βλέπουμε και στην εικόνα:



(Fabio Pavanello, 2021)[4]

Εικόνα 51: Κλασματική απόσταση Hamming μεταξύ των συσκευών και της αναμενόμενης απόκρισης καθώς και μεταξύ των συσκευών και των κλώνων

Είναι ξεκάθαρο ότι η μη κλωνοποιησιμότητα επιτυγχάνεται . Για να ποσοτικοποιήσουμε την διαφορά στην επίδοση μεταξύ των φωτονικών PUF c-Si και του a-Si ορίζουμε ως Qτον παράγοντα ποιότητας απόδοσης.

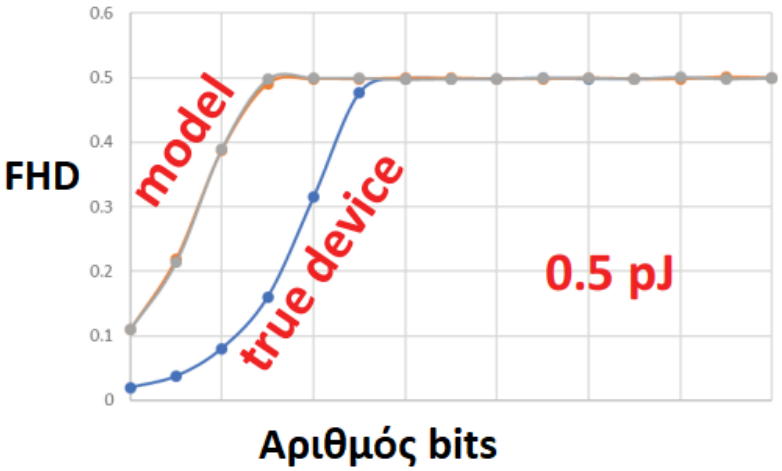
$$Q = \frac{\mu_{inter} - \mu_{intra}}{\sigma_{inter} - \sigma_{intra}} \qquad [4]$$

Αυτός ο παράγοντας υπολογίζει τη διαφορά στους μέσους όρους των όμοιων και ανόμοιων κατανομών και διαιρεί αυτή την τιμή με το άθροισμα των τυπικών αποκλίσεων των κατανομών . Ο παράγοντας αυτός για το c-Si υπολογίζεται 8,8 ενώ για το a-Si υπολογίζεται 11,08 και συνεπώς δείχνει την καλύτερη απόδοση του a-Si .

Μια τελευταία αλλά εξίσου σημαντική παράμετρος που πρέπει να εξετάσουμε είναι η αντίσταση που παρουσιάζουν τέτοιες υλοποιήσεις σε επιθέσεις μηχανικής μάθησης . Τόσο οι άμεσες όσο και οι πλευρικές επιθέσεις στις συσκευές με βαθιά νευρωνικά δίκτυα δείχνουν ότι οι συσκευές αυτές επιδεικνύουν αντίσταση σε τέτοιες επιθέσεις .

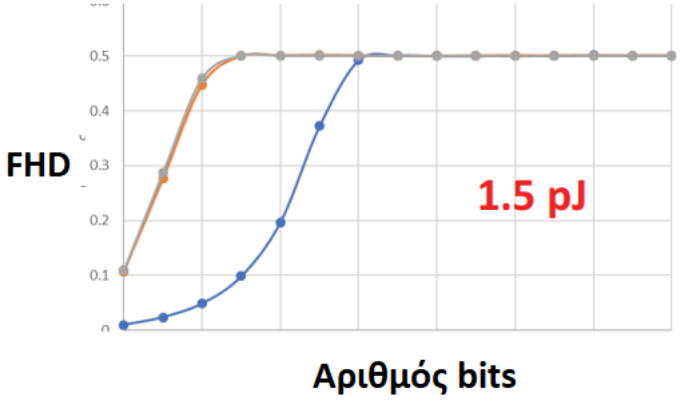
Παρατηρείται ένα ενδιαφέρουν φαινόμενο , όσο αυξάνουμε την ενέργεια του παλμού και ενισχύουμε την οπτική μη γραμμικότητα , τόσο μεγαλώνει η απόσταση FHD μεταξύ του μοντέλου της μηχανικής επίθεσης και της πραγματικής συσκευής . Για να γίνει κατανοητό με νούμερα , ας εξετάσουμε τα ποσοστά ψευδούς αποδοχής και ψευδούς απόρριψης . Συγκεκριμένα , στην υλοποίηση c-Si αν εφαρμόσουμε ενέργεια παλμού 0.36 nJ , η πιθανότητα ψευδούς αποδοχής και απόρριψης είναι της τάξεως του 10^{-22} και είναι ήδη αρκετά ικανοποιητική . Ανεβάζοντας την ενέργεια του παλμού από 0.36nJ σε 1.7nJ αυτό το ποσοστό πέφτει ακόμη παραπάνω και υπολογίζεται σε 10^{-27} .

Οι υλοποιήσεις a-Si παρουσιάζουν μια τάξη μεγέθους μεγαλύτερη μη γραμμικότητα και συνεπώς επιτυγχάνουν μια λίγο καλύτερη επίδοση όσον αφορά την αντίσταση στις επιθέσεις μηχανικής μάθησης . Ας δούμε ένα παράδειγμα σε μια υλοποίηση a-Si.



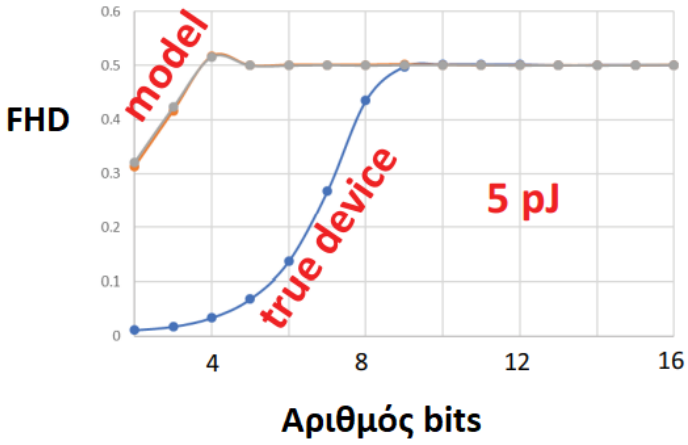
Εικόνα 52: Κλασματική απόσταση Hamming συναρτήσει του αριθμού των bits για ενέργεια παλμού 0.5pJ (Fabio Pavanello, 2021)[4]

Η διαφορά της ακρίβειας πρόβλεψης των bit του κλειδιού από το μοντέλο μηχανικής μάθησης σε σχέση με την πραγματική συσκευή αποτυπώνεται από το μέγεθος του ανοίγματος των καμπυλών που βλέπουμε . Εδώ έχει εφαρμοστεί ενέργεια παλμού 0.5 pJ. Αν ανεβάσουμε την ενέργεια του παλμού στα 1.5 pJ αναμένεται αυτή η διαφορά να αυξηθεί ακόμη περισσότερο όπως και συμβαίνει.



Εικόνα 53: Κλασματική απόσταση Hamming συναρτήσει του αριθμού των bits για ενέργεια παλμού 1.5pJ (Fabio Pavanello, 2021)[4]

Τέλος , αν αυξηθεί η ενέργεια του παλμού στα 5 pJ , αυτό το άνοιγμα γίνεται αρκετά μεγαλύτερο .



Εικόνα 54: Κλασματική απόσταση Hamming συναρτήσει του αριθμού των bits για ενέργεια παλμού 5pJ (Fabio Pavanello, 2021)[4]

Συμπέρασμα:

Συμπεραίνουμε άρα την σημασία της οπτικής μη γραμμικότητας που παρουσιάζει η υλοποίηση καθώς ανεβάζοντας λίγο την ενέργεια του παλμού το άνοιγμα μεγαλώνει αρκετά. Συγκριτικά με τις υλοποιήσεις c-Si όπου χρησιμοποιούσαμε παλμούς με ενέργεια της τάξεως των nJ , στις υλοποιήσεις a-Si βλέπουμε ότι μπορούμε να πετύχουμε την ίδια αντίσταση σε μηχανικές επιθέσεις αλλά με σημαντικά λιγότερη ενέργεια της τάξεως των pJ.

Πλεονεκτήματα των φωτονικών έναντι των ηλεκτρονικών PUFs

Τρεις λόγοι που τα φωτονικά PUFs υπερτερούν των ηλεκτρονικών είναι συνοπτικά η αυξημένη πολυπλοκότητα τους , η υψηλή αξιοπιστία τους και η ανθεκτικότητα τους σε επιθέσεις μηχανικής μάθησης .

Μειονεκτήματα των ηλεκτρονικών ισχυρών PUFs

Το μεγαλύτερο μειονέκτημα αυτού του είδους των PUFείναι ότι οι επιθέσεις μοντελοποίησης μπορούν να είναι αρκετά αποτελεσματικές απέναντι τους. Υπάρχουν δύο ειδών τέτοιες επιθέσεις :

1) Βασικές επιθέσεις μοντελοποίησης σε ισχυρά PUFs
2) Επιθέσεις μοντελοποίησης με επιπλέον πληροφορία πλευρικού καναλιού

Η πρώτη κατηγορία αποτελεί τις πιο απλές και βασικές μορφές μιας επίθεσης μοντελοποίησης . Η λογική τους έγκειται στην συλλογή ενός σχετικά μικρό υποσυνόλου των ζευγαριών πρόκλησης-απόκρισης ενός δεδομένου ισχυρού PUF. Αυτό το υποσύνολο χρησιμοποιείται για την εκπαίδευση ενός αλγορίθμου μηχανικής μάθησης. Έτσι , αν η φάση της μάθησης είναι επιτυχής , ο αλγόριθμος και το εκπαιδευμένο μοντέλο μπορούν να προβλέψουν αριθμητικά το PUFστο οποίο επιτίθενται με αρκετά υψηλή ακρίβεια . Ένα επιτυχώς εκπαιδευμένο τέτοιο μοντέλο αποκαλείται ψηφιακός κλώνος του PUF.
Οι περισσότερες επιθέσεις μοντελοποίησης σε ισχυρά ηλεκτρονικά PUFsβασίζονται στη γνώση του επιτιθέμενου της βασικής σχεδίασης του κυκλώματος του PUFστο οποίο επιτίθενται και μόνο οι κατασκευαστικές παραλλαγές θεωρούνται άγνωστες. Αυτές οι

παραλλαγές πρέπει να προκύψουν μετά από τον αλγόριθμο μηχανικής μάθησης από τα ζευγάρια προκλήσεων-αποκρίσεων που συλλέχθηκαν .

Η δεύτερη κατηγορία αποτελεί μια πιο αναπτυγμένη μορφή μοντελοποίησης ισχυρών PUF . Ο αντίπαλος μπορεί να έχει γνώση περισσότερων πολύτιμων πληροφοριών . Για παράδειγμα η σταθερότητα των ζευγαριών πρόκλησης-απόκρισης δηλαδή τα αλλοιωμένα bitsαπό το θόρυβο στις αποκρίσεις όταν εφαρμόζεται η ίδια πρόκληση πολλές φορές μπορούν να δώσουν τέτοιες πολύτιμες πληροφορίες. Ένα χαρακτηριστικό παράδειγμα είναι το XORArbiterPUF (PUFδιαιτητής). Σε μια τέτοια αρχιτεκτονική μπορεί να ενισχυθεί η απόδοση του αλγορίθμου μηχανικής μάθησης από εκθετική σε πολυωνυμική . Επίσης , άλλες παράμετροι όπως η κατανάλωση ρεύματος ενός κυκλώματος κατά τη λειτουργία του αν συνδυαστούν με έναν κατάλληλο αλγόριθμο μηχανικής μάθησης μπορούν να δημιουργήσουν πολυωνυμικά αποτελεσματικές επιθέσεις σε PUFsπου χωρίς πλευρικά κανάλια θα φαινόταν εκθετικά δύσκολο να υποστούν μηχανική μάθηση .

Υπάρχουν λίγες μορφές ισχυρών ηλεκτρονικών PUFsπου μπορούν να αποφύγουν τέτοιες επιθέσεις αλλά παρουσιάζουν άλλα μειονεκτήματα . Για παράδειγμα ένας τέτοιος τύπος PUFμε πολύ υψηλό περιεχόμενο πληροφορίας είναι τα SHICPUFs. Όλα τα ζευγάρια προκλήσεων-αποκρίσεων εδώ είναι θεωρητικά ανεξάρτητα από την πληροφορία . Όμως τα μειονεκτήματα τους όπως το ότι πιάνουν πολύ χώρο ($1cm^2$) και οι αργές ταχύτητες διαβάσματος τους δεν τα καθιστούν την καλύτερη επιλογή συνολικά .

Μειονεκτήματα των φωτονικών PUFs

Βέβαια ,σε μια τέτοια διαμόρφωση η ασφάλεια επιτυγχάνεται σε βάρος των διαστάσεων της συσκευής , της πολυπλοκότητας δοκιμής καθώς και της μειωμένης αξιοπιστίας καθώς παρουσιάζει υψηλή ευαισθησία στην ευθυγράμμιση του laserμε το PUF. Πέραν αυτών , το γεγονός ότι δεν μπορεί να ενσωματωθεί σε κυκλώματα CMOSσυνεπάγεται αυξημένο κόστος .

Παρόλο που υπάρχουν προσεγγίσεις για να μειωθεί ο όγκος της συσκευής χωρίς αυτό να επηρεάζει την εσωτερική πολυπλοκότητα (π.χ. δέσμες laserμε διαφορετικές διαμέτρους όπως θα δούμε στην επόμενη ενότητα ή βελτιστοποιημένες διαστάσεις των μικροσφαιρών) , δεν είναι εφικτή η συρρίκνωση των διαστάσεων κατά τέτοιο βαθμό μεγέθους ώστε να επιτρέπεται η συμπαγής ενσωμάτωση . Όσον αφορά τους μετασχηματισμούς που εφαρμόζονται μετά την απόκτηση του μοτίβου κηλίδων (όπως ο μετασχηματισμός Gabor) έχουν προταθεί και άλλες λύσεις. Ωστόσο δεν θεωρούνται επαρκείς για να μπουν τα ισχυρά φωτονικά PUFsστην αγορά .

Από την άλλη , οι τελευταίες μελέτες δείχνουν ότι είναι δυνατή η κατασκευή φωτονικών ενσωματωμένων PUFsσε πλατφόρμες συμβατές με CMOSκαι ταυτόχρονα ανθεκτικές απέναντι σε επιθέσεις μηχανικής μάθησης και επιθέσεις πλευρικού καναλιού. Εδώ καθοριστικό ρόλο παίζει η μη γραμμικότητα . Αυξημένη ισχύς εισόδου οδηγεί σε μεγαλύτερα λάθη στην πρόβλεψη των αποκρίσεων μοντελοποιώντας τη συμπεριφορά του PUFμέσω αναπτυγμένων βαθιών νευρωνικών δικτύων .

Πλεονεκτήματα των φωτονικώνPUFs

Σε σύγκριση με τα ηλεκτρονικά , τα φωτονικά PUFs προσφέρουν την πλούσια φύση τους προς εκμετάλλευση και επιτρέπουν την πολύπλοκη ανάμειξη σημάτων εκτός από την αναλογική τους διάδοση , ιδιαίτερα αν γίνεται εκμετάλλευση μη γραμμικών φαινομένων .Είναι τρομερά ανθεκτικά έναντι επιθέσεων μηχανικής μάθησης σε αντίθεση με τα τυπικά ηλεκτρονικά PUFs(όπως το PUFδιαιτητής) που μπορούν να προβλεφθούν μέχρι και με 99% επιτυχία .

Η αποτελεσματικότητα των φωτονικών έναντι σε επιθέσεις μηχανικής μάθησης οφείλεται στην σύνθετη απόκριση κηλίδων που δίνουν σαν έξοδο και στο πολύ μεγάλο χώρο παραμέτρων (για παράδειγμα μέχρι και $2.37*10^{10}$ ασυσχέτιστες μεταξύ τους προκλήσεις) προκύπτουν από την φωτονική διαμόρφωση που πρότεινε ο Pappu.

Η ενσωματωμένη φωτονική που βασίζεται σε πλατφόρμες συμβατές με CMOSπιστεύεται ότι είναι η λύση προς μία κλιμακούμενη χρήση φωτονικών PUFs λόγω της ενισχυμένης τους σύμπτυξης , υψηλής αξιοπιστίας και μειωμένου κόστους σε σύγκριση με τις ογκώδεις οπτικές προσεγγίσεις καθώς και ηλεκτρονικές προσεγγίσεις που βασίζονται σε transistors. Αυτό συμβαίνει λόγω του ότι αυτές οι προσεγγίσεις υποφέρουν από πολλά προβλήματα . Τέτοια είναι η γήρανση , οι θερμικές διακυμάνσεις για τις οποίες απαιτείται βαριά χρήση κωδικών διόρθωσης σφάλματος , πράγμα που δεν είναι εφικτό όσον αφορά την κατανάλωση ενέργειας και κόστους , ειδικά για συσκευές IoT. Τα PUFsπου είναι φτιαγμένα σε ενσωματωμένες φωτονικές πλατφόρμες , έχουν ισχυρότερη ανθεκτικότητα σε τέτοια προβλήματα όπως η γήρανση του κυκλώματος , πράγμα που αποτελεί ένα κύριο παράγοντα προβλημάτων στα ηλεκτρονικά PUFsδιότι απαιτούν πολύ υψηλή ικανότητα διόρθωσης σφαλμάτων.

Συμπέρασμα :

Μετά από ανάλυση των PUFs βασισμένων σε πλατφόρμες πυριτίου και σύγκριση τους με τα οπτικά PUFs έγινε εξαγωγή κάποιων συμπερασμάτων . Τα οπτικά PUFs διακρίνονται από υψηλότερη πολυπλοκότητα , χαρακτηριστικό που τα καθιστά πιο ασφαλή από τα ηλεκτρονικά . Είναι επίσης πολύ πιο ανθεκτικά σε επιθέσεις μηχανικής μάθησης από τα αντίστοιχα ακόμη και δυνατά ηλεκτρονικά PUFs . Ωστόσο , αντιμετωπίζουν προβλήματα συμβατότητας με τον ηλεκτρονικό εξοπλισμό . Για την εξισορρόπηση της ασφάλειας με τη δυνατή συμβατότητα κατάλληλα αποδεικνύονται τα μη γραμμικά φωτονικά PUFs βασισμένα στο πυρίτιο .

Κεφάλαιο 6: Παραμετροποιήσεις και βελτιώσεις στα οπτικά PUFs

Έχοντας δει την λειτουργία των οπτικών PUFs και τα πλεονεκτήματα τους , είναι χρήσιμο να πάμε ένα βήμα παρακάτω και να δούμε αν είναι εφικτό και υπό ποιες συνθήκες αυτά τα οπτικά PUFs να γίνουν αποδοτικότερα .

Σε αυτή την ενότητα θα αναλύσουμε κρίσιμες παραμέτρους ενός laser που επηρεάζουν την αποτελεσματικότητα ενός PUF. Θα δούμε πως μπορούμε να αυξήσουμε το χώρο προκλήσεων καθώς και την πολυπλοκότητα σκέδασης . Ο στόχος είναι να αυξηθεί ο αριθμός των ασυσχέτιστων μεταξύ τους ζευγαριών προκλήσεων-αποκρίσεων (CRPs).

Η επίδραση των πολλαπλών ακτινών

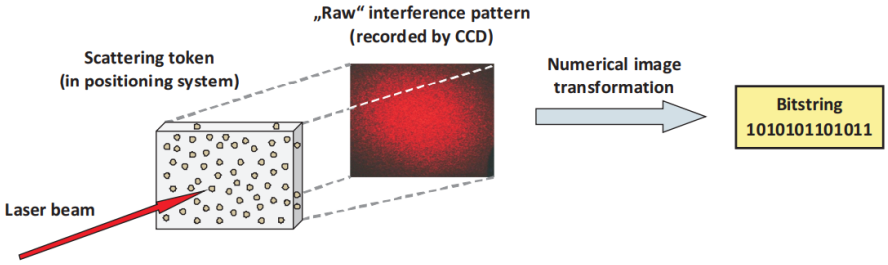
Όπως αναφέραμε σε προηγούμενο κεφάλαιο (Κεφάλαιο 4) , όσο μεγαλύτερος είναι ο χώρος προκλήσεων τόσο το καλύτερο για ένα PUF . Ένας τρόπος να αυξήσουμε το χώρο προκλήσεων στα οπτικά PUFs είναι η χρήση πολλών ακτινών laser με διαφορετικές συχνότητες . Για παράδειγμα ένα κόκκινο και ένα πράσινο laser . Λόγω της διαφοράς τους στα μήκη κύματος , το μοτίβο που θα πάρουμε από ένα πράσινο laser που πέφτει σε ένα σημείο με μια συγκεκριμένη γωνία πρόσπτωσης είναι διαφορετικό από ένα κόκκινο laser που πέφτει ακριβώς στο ίδιο σημείο με το πράσινο και με την ίδια γωνία πρόσπτωσης. Αν λοιπόν χρησιμοποιήσουμε 2 τέτοια lasers μπορούμε να κάνουμε την πρόκληση να αποτελείται και από τα 2 σημεία πρόσπτωσης καθώς και από τις 2 γωνίες πρόσπτωσης. Έτσι μπορούμε να ενισχύσουμε το χώρο προκλήσεων τετραγωνικά .

Υπάρχει πρόβλημα όμως με αυτή την προσέγγιση αν οι δομές διασποράς που χρησιμοποιούμε είναι γραμμικές . Σε τέτοια περίπτωση το μοτίβο που θα πάρουμε δεν είναι παρά το άθροισμα των 2 μοτίβων που θα προκληθούν από κάθε πρόκληση ξεχωριστά. Αν C είναι η πρόκληση , p το σημείο πρόσπτωσης και Θ η γωνία πρόσπτωσης τότε έχουμε : $C_i^{\kappa\acute{o}\kappa\kappa\iota\nu o} = \left(\vec{p}_{\kappa\acute{o}\kappa\kappa\iota\nu o}, \Theta_{\kappa\acute{o}\kappa\kappa\iota\nu o}\right)$και $C_i^{\pi\rho\acute{a}\sigma\iota\nu o} = \left(\vec{p}_{\pi\rho\acute{a}\sigma\iota\nu o}, \Theta_{\pi\rho\acute{a}\sigma\iota\nu o}\right)$ [14] (Ulrich Rührmair, 2013) . Συγκεκριμένα , για την πρόκληση C_iη ένταση του κάθε pixel ισούται ακριβώς με το άθροισμα των εντάσεων της πρόκλησης $C_i^{\kappa\acute{o}\kappa\kappa\iota\nu o} + C_i^{\pi\rho\acute{a}\sigma\iota\nu o}$. Επιπλέον , αν χρησιμοποιούμε 2 ξεχωριστά laser , το κόκκινο και το πράσινο φως δεν είναι συνεκτικά και συνεπώς δεν έχουμε την πολύπλοκη παρεμβολή που θέλουμε .

Ένας αντίπαλος , μπορεί αρχικά να διαβάσει τα μοτίβα παρεμβολών για όλες τις προκλήσεις ξεχωριστά από το κόκκινο και το πράσινο laser. Στη συνέχεια χρειάζεται απλά να προσθέσει τα μοτίβα που βρήκε από τις προκλήσεις του κόκκινου με αυτά που βρήκε από τις προκλήσεις του πράσινου. Συνεπώς , αν χρησιμοποιήσουμε 2 lasers έχουμε το πλεονέκτημα ότι αυξάνουμε αποτελεσματικά το χώρο προκλήσεων κατά παράγοντα του 2. Το μειονέκτημα όμως είναι ότι χρειάζεται μεγάλη προσπάθεια υλοποίησης καθώς πρέπει και τα 2 laser να είναι ανεξάρτητα τοποθετημένα. Σε πρακτικό επίπεδο το token μπορεί να αλλάζει θέσεις αλλά τα laser μένουν ακίνητα λόγω του βάρους τους. Αφού θέλουμε 2 laser που να παράγουν ανεξάρτητες προκλήσεις αυτή η μέθοδος δεν βρίσκει εφαρμογή. Η ίδια λογική ισχύει και για k αριθμό lasers. Άρα εν ολίγοις , με k ακτίνες laser αυξάνουμε το χώρο προκλήσεων κατά παράγοντα k αλλά είναι ακριβό.

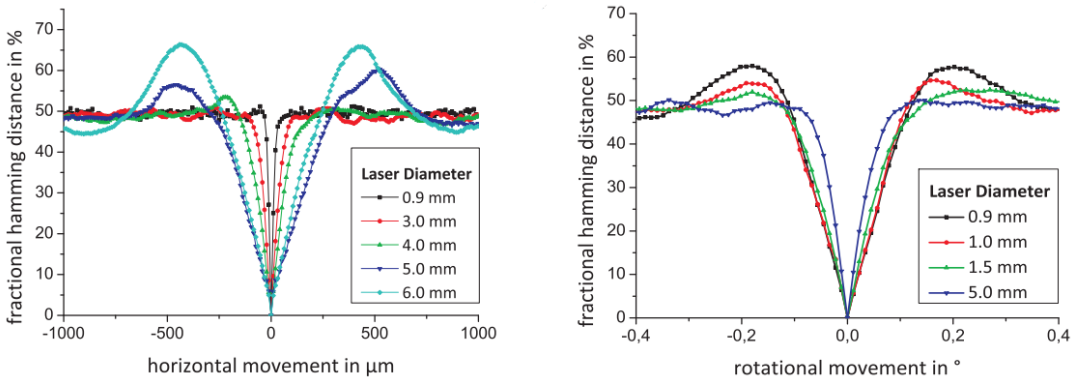
Η επίδραση της διαμέτρου του laser

Η ευαισθησία της εξόδου του PUF μπορεί να επηρεαστεί από τη διάμετρο του laser με 2 τρόπους . Ο πρώτος είναι να πειράξουμε το σημείο πρόσπτωσης στους άξονες x και y . Ο δεύτερος είναι να μεταβάλλουμε τη γωνία πρόσπτωσης του . Η ευαισθησία είναι μια καλή μέτρηση για την ασφάλεια ενός οπτικού PUF διότι καθορίζει τον αριθμό των ανεξάρτητων ζευγαριών πρόκλησης-απόκρισης του PUF και συνεπώς την ανθεκτικότητα του απέναντι σε επιθέσεις ανάγνωσης. Η διάμετρος μπορεί να ρυθμιστεί αν απλά εστιάσουμε το laser. Στην εικόνα βλέπουμε ότι το σημείο εστίασης βρίσκεται στην επιφάνεια του PUF.



Εικόνα 55: Σχηματική απεικόνιση ενός μη ενσωματωμένου PUF (Pappu R. , 2001) (Pappu R. S., 2002)[11] [12]

Η κεντρική θέση του token τίθεται ως σημείο αναφοράς . Το token είναι σφαίρες γυαλιού 300-400μm . Μετακινούμε το PUF με το σύστημα τοποθέτησης σε ισόχωρες εναλλαγές και τραβάμε φωτογραφίες από τα μοτίβα κηλίδων . Στις ακατέργαστες εικόνες εφαρμόζεται μετασχηματισμός Gabor . Έτσι παίρνουμε τις μετασχηματισμένες εικόνες . Στη συνέχεια υπολογίζονται οι αποστάσεις Hamming στην μετασχηματισμένη εικόνα της θέσης αναφοράς. Μια απόσταση Hamming 0.5 σημαίνει ότι υπάρχει πλήρης αποσυσχέτιση των μετασχηματισμένων εικόνων . Παρακάτω βλέπουμε τα αποτελέσματα :



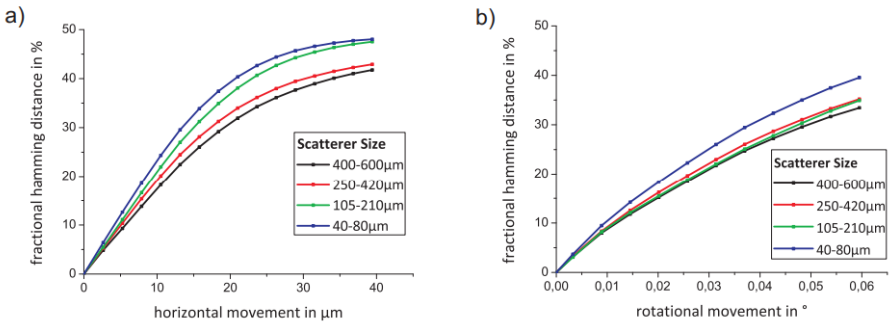
Εικόνα 56: Διαγράμματα κλασματικών αποστάσεων Hamming σε σχέση με οριζόντια κίνηση (αριστερή εικόνα) και με περιστροφική κίνηση (δεξιά εικόνα) (Ulrich Rührmair, 2013)[14]

Για να υπάρχουν ασυσχέτιστα ζευγάρια πρόκλησης-απόκρισης θα πρέπει να κρίνουμε κατά πόσο γρήγορα οι καμπύλες όχι μόνο φτάνουν αλλά«κάθονται» στο 0.5 της απόστασης Hamming . Όσο πιο γρήγορα συμβαίνει αυτό , τόσο πιο ανεξάρτητα και ασυσχέτιστα μεταξύ τους ζευγάρια υπάρχουν . Για παράδειγμα στην αριστερή εικόνα βλέπουμε ότι για διάμετρο 6.0mm η καμπύλη αργεί αρκετά να καθίσει ενώ για διάμετρο 0.9 mm οριακά δεν κάνει καμπύλη. Αυτό μας οδηγεί στο συμπέρασμα ότι μικρές διάμετροι οδηγούν σε γρήγορη αποσυσχέτιση για οριζόντιες (αλλά και κάθετες κινήσεις) .Στην δεξιά εικόνα όμως συμβαίνει το ανάποδο . Όπως παρατηρούμε για μια διάμετρο 0.9mm η καμπύλη είναι η μεγαλύτερη ενώ όσο μεγαλώνει η διάμετρος τόσο η καμπύλη μικραίνει . Άρα σε περιστροφική κίνηση συμβαίνει το ακριβώς ανάποδο απ'ότι σε μια οριζόντια ή κάθετη κίνηση . Αυτό σημαίνει ότι η επιλογή της κατάλληλης διαμέτρου laser είναι ένα πρόβλημα βελτιστοποίησης και εξαρτάται από τη διάταξη που χρησιμοποιούμε καθώς και από τα υλικά που φτιάχνεται το token . Συνεπώς , σε κάθε εφαρμογή οπτικών PUF αντιμετωπίζεται διαφορετικά για να επιτευχθεί η βέλτιστη δυνατή ασφάλεια. Στην προκειμένη , οι διάμετροι laser μεταξύ 1.5 και

2.5 mm θεωρούνται ιδανικές . Αυτό προφανώς συμβαίνει για να ικανοποιούμε ταυτόχρονα και τις οριζόντιες αλλά και τις περιστροφικές κινήσεις στο βέλτιστο δυνατό βαθμό . Υπολογίζεται ότι μια τέτοια διάμετρος μπορεί να αυξήσει το χώρο προκλήσεων κατά ένα παράγοντα της τάξεως του 3 με 5 .

Η επίδραση του μεγέθους των σκεδαστών

Θεωρητικά μια ιδανική πολυπλοκότητα της διαδικασίας σκέδασης αναμένεται για μέγεθος παρόμοιο με αυτό του μήκους κύματος του χρησιμοποιούμενου φωτός του laser. Το μοτίβο παρεμβολής εξαρτάται κυρίως από τα μεγέθη και τα σχήματα των σωματιδίων . Αυτό είναι γνωστό και ως Mie-regime. Η κατανομή του ηλεκτρομαγνητικού πεδίου εντός του PUF προϋποθέτει την επίλυση των εξισώσεων του Maxwell που είναι αριθμητικά πολύ απαιτητική διαδικασία . Όταν το μέγεθος των σωματιδίων είναι αρκετά μεγαλύτερο από το οπτικό μήκος κύματος , τότε μπορούμε να αποφύγουμε την πολυπλοκότητα των εξισώσεων Maxwell χρησιμοποιώντας κάποιες απλοποιημένες μεθόδους . Μια τέτοια μέθοδος είναι οι προσεγγίσεις ιχνηλάτησης ακτινών .Από την άλλη , για σωματίδια ή ανομοιογένειες του δείκτη διάθλασης αρκετά μικρότερα του μήκους κύματος το σκεδαζόμενο πεδίο φωτός μπορεί να περιγραφεί με τη σκέδαση Rayleigh που είναι απλούστερη. Στην περίπτωση ενός μεγάλου συνόλου αντικειμένων πολύ μικρότερων του μήκους κύματος οι απλοί σκεδαστές δεν επιλύονται καθόλου οπτικά. Το μέσο τότε περιγράφεται από ένα δείκτη διάθλασης με μέσο όρο όγκου και παρουσιάζει πάλι χαμηλή οπτική πολυπλοκότητα. Ουσιαστικά , η ιδέα είναι ότι όσο μικρότεροι είναι οι σκεδαστές , τόσο υψηλότερη πολυπλοκότητα μπορούμε να πετύχουμε . Για να κατανοήσουμε αυτό το γεγονός , ας δούμε τι αποτέλεσμα έχουν τα πειράματα όπου χρησιμοποιήθηκε εύρος μεγεθών της τάξεως των 400-600μm, 250-420μm , 105-210μm και 40-80μm . Σαν μέτρο για τον υπολογισμό της εσωτερικής πολυπλοκότητας της διαδικασίας σκέδασης χρησιμοποιείται και πάλι η ευαισθησία του μοτίβου κηλίδων σε διακυμάνσεις των συντεταγμένων και των γωνιών . Στην εικόνα που ακολουθεί βλέπουμε πόσο γρήγορα αποσυσχετίζονται οι εικόνες:



Εικόνα 57: Ρυθμός αποσυσχέτισης εικόνων σε οριζόντια και περιστροφική κίνηση (Ulrich Rührmair, 2013)[14]

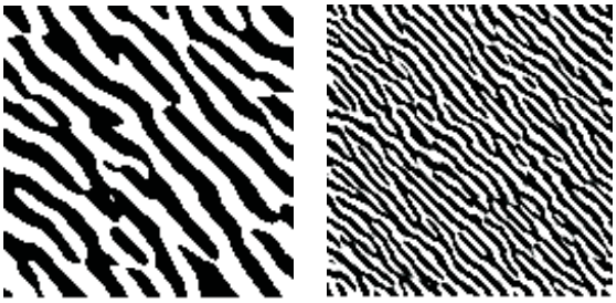
Όπως προκύπτει από τα ευρήματα , μικρότεροι σκεδαστές οδηγούν σε γρηγορότερη αποσυσχέτιση των εξόδων του PUF για μεταβολές του σημείου πρόσπτωσης και της γωνίας πρόσπτωσης από μεγαλύτερου μεγέθους σκεδαστές. Επίσης ο χώρος προκλήσεων μπορεί να γίνει μεγαλύτερος χρησιμοποιώντας μικρότερους μεγέθους σκεδαστές. Χρησιμοποιώντας σκεδαστές μεγέθους 40-80μm σε αντίθεση με αυτούς που χρησιμοποίησε ο Pappu μεγέθους 500-800μm όπως είδαμε στο κεφάλαιο 3 (Pappu R. S., 2002) [12] μπορούμε να πετύχουμε

βελτίωση του μεγέθους του χώρου προκλήσεων . Διπλασιάζεται στις οριζόντιες κατευθύνσεις και ομοίως στις κάθετες κατευθύνσεις αλλά και στις αλλαγές γωνίας . Αυτό σημαίνει ότι συνολικά πετυχαίνουμε μια βελτίωση που τον καθιστά τον χώρο προκλήσεων 8 φορές μεγαλύτερο . Και αυτό έχοντας χρησιμοποιήσει σκεδαστές της τάξεως των μm . Εικάζεται ότι σε κλίμακα nm θα μπορούσαν να επιτευχθούν ακόμα καλύτερα αποτελέσματα . Συμπερασματικά , δεδομένου ότι οι μικροί σκεδαστές είναι μια απλή και φθηνή λύση για την αύξηση της ασφάλειας στα οπτικά PUFs , θα πρέπει σε πρακτικές υλοποιήσεις να διαλέγονται όσο το δυνατόν μικρότεροι δεδομένων των δυνατοτήτων κατασκευής , κόστους και σταθερότητας .

Βελτίωση της εντροπίας των αποκρίσεων

Σύμφωνα με το μοντέλο που παρουσίασε ο Pappu [12] , οι εικόνες που παίρνουμε δεν χρησιμοποιούνται αυτούσιες ως αποκρίσεις μιας και είναι μεγάλες και ασταθείς . Χρησιμοποιούμε πάνω τους έναν αριθμητικό μετασχηματισμό για να πάρουμε μικρότερες και πιο σταθερές δυαδικές συμβολοσειρές. Συγκεκριμένα όπως είδαμε χρησιμοποιείται ο μετασχηματισμός Gabor . Έτσι διαβάζοντας τις ακατέργαστες εικόνες σειρά σειρά και θέτοντας ένα κατώφλι για τη μετατροπή σε δυαδικά δεδομένα 0 και 1 παράγουμε το κρυπτογραφικό κλειδί. Σε αυτήν την προσέγγιση παρουσιάζονται 2 μειονεκτήματα.

Το πρώτο μειονέκτημα είναι ότι οι μετασχηματισμένες εικόνες παρουσιάζουν ισχυρές κανονικότητες που μοιάζουν με λωρίδες ζέβρας. Αυτό σημαίνει ότι προκύπτουν ισχυρά μοτίβα στα κρυπτογραφικά κλειδιά . Στην πράξη δημιουργούνται τακτικά εναλλασσόμενες μεσαίου μήκους ακολουθίες διαδοχικών μονάδων και μηδενικών στα κλειδιά που παράγονται .Τέτοιες κανονικότητες μπορούμε να δούμε στις 2 εικόνες που ακολουθούν ,όπου για την κάθε μία έχουν χρησιμοποιηθεί διαφορετικές παράμετροι στον μετασχηματισμό Gabor :



Εικόνα 58: Εικόνες που παρουσιάζουν τακτικά εναλλασσόμενες κανονικότητες για διαφορετικές παραμέτρους στον μετασχηματισμό Gabor (Ulrich Rührmair, 2013)[14]

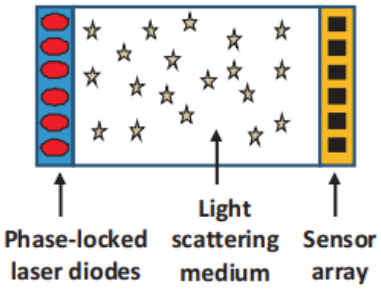
Για την αντιμετώπιση του προβλήματος , προτάθηκε η επιλογή ενός τυχαίου υποσυνόλου των bits της εικόνας Gabor. Όμως το πρόβλημα με αυτό είναι ότι μαζί με τις τιμές των bits αυτές καθ’αυτές θα πρέπει να αποθηκεύονται και οι θέσεις των συγκεκριμένων τιμών . Οπότε αυξάνονται οι απαιτήσεις αποθήκευσης . Επιπλέον , δεν υπάρχει ακριβής τρόπος για την επιλογή bits που είναι σταθερά και φέρουν ταυτόχρονα μεγάλο όγκο πληροφορίας . Έτσι , αυτή η μέθοδος δεν αντιμετωπίζει εν τέλει το πρόβλημα και χρειαζόμαστε άλλο μετασχηματισμό εξ’αρχής.

Το αποτέλεσμα πειραματικά είναι όπως αναμενόταν ότι όλοι οι μετασχηματισμοί μπορούν σημαντικά να αυξήσουν την δυαδική εντροπία των αποκρίσεων του PUF . Ωστόσο , όλοι οι μετασχηματισμοί παρουσιάζουν ελαφρώς χειρότερη ευρωστία από το μετασχηματισμό του Gabor . Αυτό μπορεί στην πράξη να μην δημιουργεί πρακτικά προβλήματα όμως θα πρέπει να επινοηθεί ένας μετασχηματισμός ώστε να καλύπτει όλα τα πιθανά σενάρια για κάθε εφαρμογή.

Έτσι επινοήθηκε μια νέα μέθοδος η οποία ονομάζεται adaptedhigh-boosttransform (AHB) η οποία προσφέρει την ίδια σταθερότητα με το μετασχηματισμό Gabor αλλά προκαλεί πολύ λιγότερες κανονικότητες στις μετασχηματισμένες εικόνες. Στη μέθοδο AHB χρησιμοποιείται ένας πυρήνας συνέλιξης ο οποίος συγκρίνει την ένταση ενός pixel σε σχέση με τη γειτονιά του. Η μετατροπή σε δυαδικό κλειδί δημιουργείται όπως και στον μετασχηματισμό Gabor , δηλαδή με ένα φίλτρο κατωφλίου . Έτσι υπολογίζεται ο αριθμητικός μέσος όρος της έντασης των pixel στη γειτονιά ενός κεντρικού pixel . Αν η ένταση αυτού του κεντρικού pixel αθροιζόμενη με μια ρυθμισμένη μετατόπιση είναι μεγαλύτερη απτό μέσο όρο της γειτονιάς του pixel , τότε το pixel θα πάρει την τιμή 0 . Διαφορετικά θα πάρει την τιμή 1.

Υλοποίηση των ενσωματωμένων οπτικών PUFs

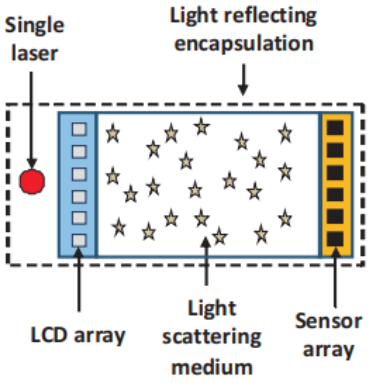
Υπάρχουν 2 προσεγγίσεις . Ο στόχος είναι να σχεδιάσουμε οπτικά PUFs χωρίς να χρειαζόμαστε εξαρτήματα που κινούνται αλλά ταυτόχρονα να εξακολουθούν να επιτρέπουν εκθετικό αριθμό διαφορετικών προκλήσεων . Στην εικόνα βλέπουμε μια ακίνητη διάταξη διόδων laser με k διόδους κλειδωμένης φάσης.



Εικόνα 59: Διάταξη διόδων laser με διόδους κλειδωμένης φάσης (Ulrich Rührmair, 2013)[14]

Αυτό χρησιμοποιείται για να διεγείρει ένα διαταραγμένο τυχαίο μέσο σκέδασης. Οι δίοδοι μπορούν να ενεργοποιηθούν και να απενεργοποιηθούν ανεξάρτητα η μία από την άλλη . Αυτό σημαίνει ότι μπορούμε να έχουμε 2^k διαφορετικές προκλήσεις C_i . Στο δεξί τμήμα του συστήματος μια διάταξη από l αισθητήρες φωτός μετράνε τοπικά τις εντάσεις του φωτός που προκύπτουν. Η απόκρισηR_i αποτελείται από τις εντάσεις στους l αισθητήρες.

Αντίστοιχα , μπορούμε αντί για μια σειρά από διόδους κλειδωμένης φάσης να υλοποιήσουμε την ίδια ιδέα με μια πηγή laser ακολουθούμενη από ένα φθηνό διαμορφωτή φωτός (LCD) .



Εικόνα 60: Ίδια υλοποίηση με την Εικόνα 59 αλλά χρησιμοποιώντας μια πηγή laser και στη συνέχεια ένα LCD αντί για διόδους κλειδωμένης φάσης (Ulrich Rührmair, 2013)[14]

Τα k pixels του LCD μπορούν να ενεργοποιηθούν και να απενεργοποιηθούν ανεξάρτητα το ένα από τα άλλα , που σημαίνει πως και πάλι καταλήγουμε στο να έχουμε 2^k διαφορετικές πιθανές προκλήσεις . Και όλο το σύστημα ενθυλακώνεται από ένα ανακλαστικό στρώμα για τη διευκόλυνση της εσωτερικής διαδικασίας παρεμβολής. Προκειμένου να επιτρέπεται οπτική παρεμβολή αλλά και να δημιουργούνται περίπλοκες συμπεριφορές με γραμμικά μέσα σκέδασης , όλο το φως του laser μέσα στο μέσο σκέδασης θα πρέπει να είναι συνεκτικό , να έχει δηλαδή την ίδια συχνότητα.

Κεφάλαιο 7:Εφαρμογές των οπτικών PUFs

Εφαρμογή των οπτικών PUFs στο blockchain

Όπως αναφέρθηκε , τα οπτικά PUFs αποδεικνύονται πολύ ικανά ως προς την αντίσταση τους στην κλωνοποίηση καθώς και ανθεκτικά σε επιθέσεις μηχανικής μάθησης . Αυτό το γεγονός τα καθιστά ικανά σε συνδυασμό με το blockchain ώστε να επιτύχουμε κυρίως διάφορους στόχους ασφαλείας. Το blockchain έχει την ιδιότητα ότι είναι εγγενώς ανθεκτικό σε τροποποιήσεις και συνεπώς οι εγγραφές δεν μπορούν να τροποποιηθούν χωρίς ταυτόχρονα να αλλοιωθούν όλα τα επόμενα blocks της αλυσίδας. Τα blockchain χρησιμοποιούνται στις μέρες μας κυρίως σαν κατανεμημένα καθολικά , δηλαδή χρειάζεται η συναίνεση των αναπαραγόμενων κοινών και συγχρονισμένων ψηφιακών δεδομένων που είναι κατανεμημένα γεωγραφικά σε πολλούς ιστότοπους .Εφαρμογή βρίσκουν κυρίως σε κρυπτονομίσματα αλλά αυτή η αποκεντρωμένη συναινετική τους ιδιότητα μπορεί να χρησιμοποιηθεί και σε άλλους τομείς όπως η απογραφή και η μεταφορά περιουσιακών στοιχείων , η ψήφος , δεδομένα υγείας κ.λπ.

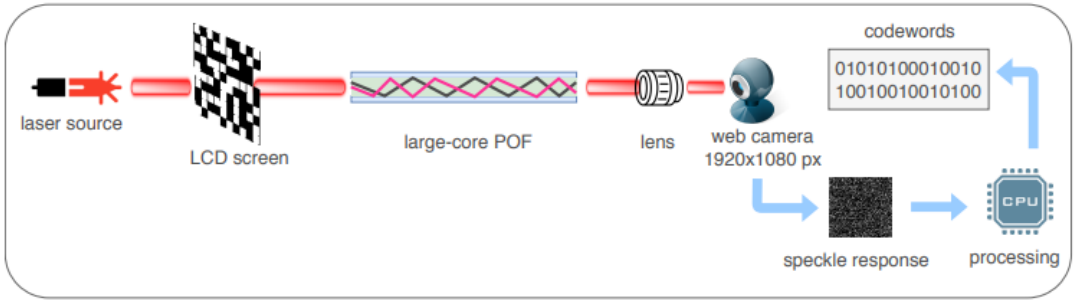
Όταν αναφερόμαστε σε blockchains συνήθως μιλάμε για δημόσια blockchains όπου μπορούν όλοι να συμμετάσχουν , να εκτελέσουν το πρωτόκολλο συναίνεσης και να μοιράζονται το κοινό καθολικό. Αντίθετα , το ιδιωτικό blockchain έχοντας τα πλεονεκτήματα του δημοσίου blockchain , εστιάζει σε περιπτώσεις χρήσης όπου το άνοιγμα στο κοινό συνιστά κίνδυνο ασφαλείας . Η διαφορά με το δημόσιο είναι ότι στο ιδιωτικό blockchain ,μπορεί κανείς να

συμμετάσχει αφού λάβει μια πρόσκληση από κάποιον που έχει τη δικαιοδοσία . Όταν κάποιος γίνει μέλος αποτελεί μέλος του δικτύου και έχει τα ίδια δικαιώματα και υποχρεώσεις με τα υπόλοιπα μέλη.

Ένα σενάριο είναι αν θα μπορούσαμε να συνδυάσουμε τα PUFs με το blockchain ώστε να επιτύχουμε ακόμη υψηλότερα ποσοστά ασφαλείας στα IoT οικοσυστήματα.

Πείραμα και αποτελέσματα

Για το πείραμα θα χρησιμοποιηθούν οπτικά PUFπου βασίζονται σε μια πολυμερή οπτική ίνα μεγάλου πυρήνα . Τα οπτικά PUFεπιλέχθηκαν καθώς παρουσιάζουν καλύτερες επιδόσεις από τα ηλεκτρονικά και τα κλασσικά PUFπυριτίου . Όπως έχει προαναφερθεί , παρουσιάζουν πιο περίπλοκους φυσικούς μηχανισμούς και συνεπώς καθίστανται πιο ασφαλή . Το σχήμα του οπτικού PUF είναι το ακόλουθο.



Εικόνα 61: Σχήμα υλοποίησης οπτικού PUF (Charidimos Chaintoutis1, 2018) [1]

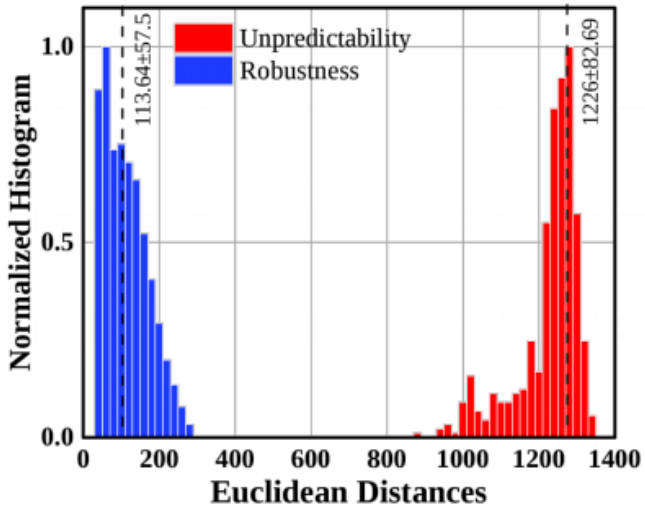
Αριστερά βλέπουμε τη συνεκτική πηγή φωτός (laserHe-Ne 632 nm) , στη συνέχεια ένα μέσο δημιουργίας πρόκλησης (οθόνηLCD ανάλυσης 320x240 pixelsμε 18 μμαπόσταση μεταξύ των pixels) , κατόπιν έχουμε το tokento οποίο στην προκειμένη είναι μια συνηθισμένη πολυμερής οπτική ίνα μεγάλου πυρήνα μεγέθους 1cmκαι τέλος σαν μέσο απεικόνισης μια τυπική κάμερα με πραγματική ανάλυση 1920x1080 pixels .

Στο κεφάλαιο 6 αναλύσαμε την επίδραση που έχουν ορισμένες παράμετροι στις προκλήσεις όπως η γωνία πρόσπτωσης , η διάμετρος της δέσμης φωτός , το προφίλ της χωρικής έντασης της δέσμης φωτός . Στο συγκεκριμένο πείραμα ως παράμετρος για την παραγωγή διαφορετικών προκλήσεων επιλέγεται η μεταβολή του προφίλ χωρικής έντασης της δέσμης φωτός του laser χρησιμοποιώντας την οθόνη LCD . Κάθε πρόκληση χρειάζεται 7 pixels για να φτιαχτεί ώστε να αποκτήσει την απαραίτητη ένταση . Συνολικά λοιπόν έχουμε 32 προκλήσεις και συγκεκριμένα 32 διαφορετικά συμπλέγματα των 7 pixels το καθένα χωρίς επικάλυψη .

Αρχικά , θα πρέπει να ελεγχθεί η απροβλεπτότητα του συστήματος . Αυτό αποτυπώνεται καταγράφοντας τις αποκρίσεις του συστήματος υπό διαφορετικές προκλήσεις . Οι διαφορετικές προκλήσεις όπως είπαμε προκύπτουν από την μεταβολή του χωρικού προφίλ έντασης της δέσμης laser. Συνεπώς παίρνουμε 32 διαφορετικές εικόνες (1 εικόνα από κάθε διαφορετική πρόκληση) ανάλυσης 1920x1080 έκαστη . Αυτά αποτελούν τα δεδομένα απροβλεπτότητας . Για να εξετάσουμε αν το σύστημα είναι απρόβλεπτο θα πρέπει να εξετάσουμε τις διακυμάνσεις που έχουν αυτές οι εικόνες μεταξύ τους.

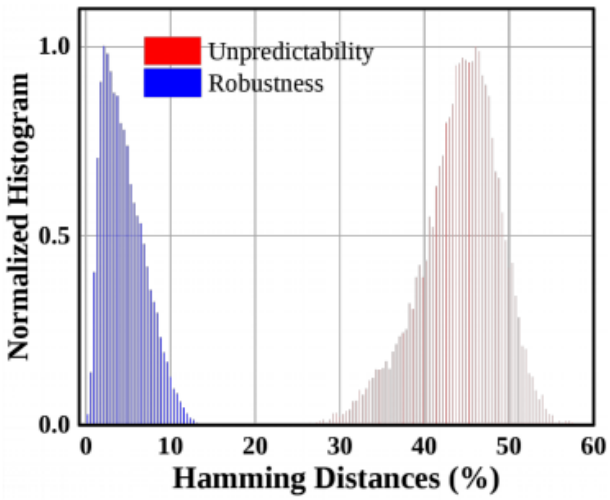
Η ευρωστία του συστήματος και συνεπώς η αντοχή του στο θόρυβο εξετάζεται διατηρώντας τις συνθήκες φωτισμού σταθερές που συνεπάγεται ότι η ίδια πρόκληση εφαρμόζεται στο

ίδιοPUFαποκτώντας 250 εικόνες σε χρονικό πλαίσιο 4 ωρών . Αυτά αποτελούν τα δεδομένα ευρωστίας . Οι ευκλείδειες αποστάσεις των τυποποιημένων εικόνων των δεδομένων απροβλεπτότητας και ευρωστίας παρουσιάζονται στο παρακάτω διάγραμμα .



Εικόνα 62: Διάγραμμα υπολογισμένων ευκλείδειων αποστάσεων (Charidimos Chaintoutis1, 2018) [1]

Στη συνέχεια υπολογίζουμε τις ακόλουθες αποστάσεις Hamming των ακατέργαστων εικόνων (της εξόδου του PUF) .



Εικόνα 63: Διάγραμμα υπολογισμένων αποστάσεων Hamming (Charidimos Chaintoutis1, 2018) [1]

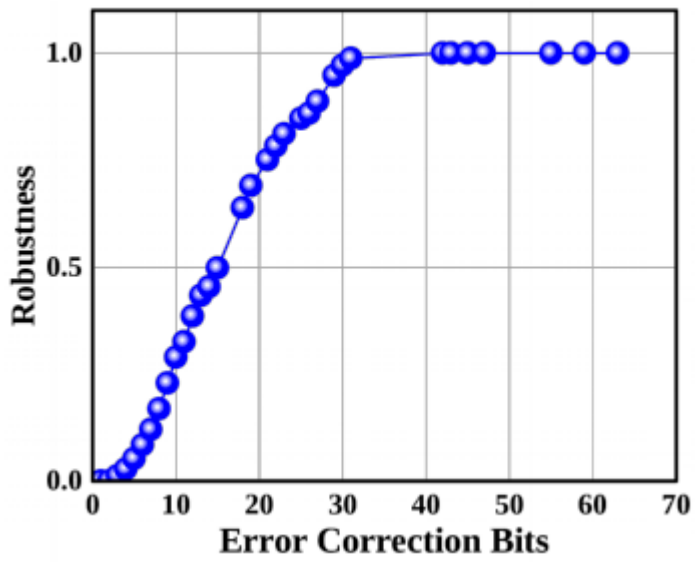
Εφαρμόζοντας την μέθοδο κατακερματισμού Random Binary Hashingθα πάρουμε συμβολοσειρές μεγέθους 255 Bits . Η μέθοδος αυτή συνοπτικά παίρνει την απόκριση του PUFκαι την συμπιέζει ώστε στη συνέχεια να κβαντιστεί θέτοντας ένα κατώφλι πάνω από το οποίο θα δίνεται η τιμή 1 και κάτω από το οποίο θα δίνεται η τιμή 0 .

Παρατηρώντας τα διαγράμματα βλέπουμε ότι οι κατανομές έχουν ξεκάθαρα μηδενική επικάλυψη και μια σημαντική διαφορά μέσης τιμής μεταξύ τους. Με μπλε αποτυπώνονται οι

ανομοιότητες που προέκυψαν λόγω θορύβου υπό ίδιες πειραματικές συνθήκες (ευρωστία) και με κόκκινο αποτυπώνονται οι ανομοιότητες που προκύπτουν μεταξύ εικόνων που καταγράφηκαν υπό διαφορετικές προκλήσεις (απροβλεπτότητα).

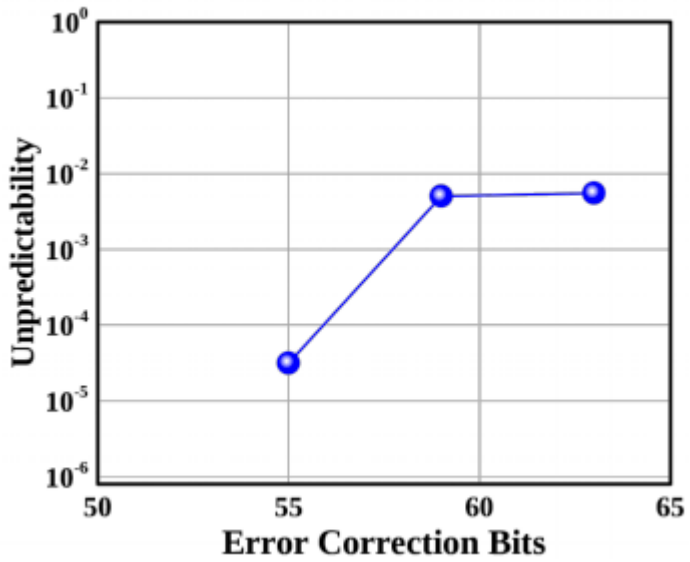
Αυτός ο διαχωρισμός των κατανομών μας επιτρέπει να εξαλείψουμε την πιθανότητα ψευδώς θετικών και ψευδώς αρνητικών .

Χρησιμοποιούνται δύο διακριτές λειτουργίες , η παραγωγή κλειδιών και η επικύρωση κλειδιών . Κατά την παραγωγή κλειδιών , παράγεται ένα κλειδί z μεγέθους 255 bits με μερικά κλειδιά που δημιουργούνται κατά τη διόρθωση σφαλμάτων . Κατά την λειτουργία επικύρωσης κλειδιών δημιουργείται ένα κλειδί z' που προσπαθεί να ανακατασκευάσει το αρχικό κλειδί z . Η πιθανότητα τα κλειδιά να διαφέρουν κλιμακώνεται με τη δυνατότητα διόρθωσης σφαλμάτων . Η διαδικασία αυτή εκτελείται και για τα δεδομένα ευρωστίας και για τα δεδομένα απροβλεπτότητας .Στην παρακάτω εικόνα βλέπουμε την ευρωστία του συστήματος συναρτήσει της δυνατότητας διόρθωσης σφαλμάτων .



Εικόνα 64: Διάγραμμα απεικόνισης ευρωστίας συναρτήσει του αριθμού των ECC bits (Charidimos Chaintoutis1, 2018) [1]

Όπως παρατηρούμε , το σύστημα είναι πλήρως εύρωστο μέχρι τα 30 bits διόρθωσης σφάλματος (ECC) . Στην εικόνα που ακολουθεί αποτυπώνεται η απροβλεπτότητα του συστήματος .



Εικόνα 65: Διάγραμμα απεικόνισης απροβλεπτότητας συναρτήσει του αριθμού των ECC bits (Charidimos Chaintoutis1, 2018) [1]

Το σύστημα είναι πρακτικά απρόβλεπτο για λιγότερα από 55 ECC bits . Η πιθανότητα να πάρουμε το ίδιο κλειδί χρησιμοποιώντας μια διαφορετική πρόκληση είναι της τάξεως του 10^{-5}. Κάτω από τα 55 ECC bits θεωρείται η απροβλεπτότητα είναι μη υπολογίσιμη και θεωρείται πρακτικά 0.

Συνδυάζοντας την πληροφορία που πήραμε και από τα 2 σύνολα δεδομένων καταλήγουμε στο συμπέρασμα ότι το σύστημα μπορεί να θεωρηθεί πλήρως εύρωστο και παράλληλα εντελώς απρόβλεπτο με πιθανότητα πρόβλεψης να κυμαίνεται από 10^{-5} μέχρι 0 .

Συνδυασμός με blockchain

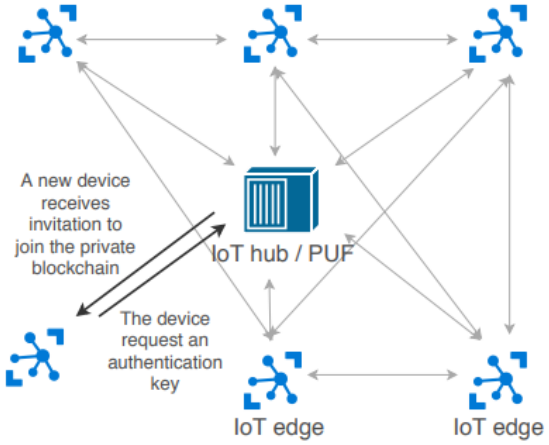
Το blockchain βασίζεται σε μεγάλο βαθμό στην ποιότητα των τυχαίων αριθμών και απαιτεί ασφαλή αποθήκευση ενός κλειδιού ανά χρήστη που θα του επιτρέπει να έχει πρόσβαση στην πληροφορία του καθολικού. Οι ψευδό-τυχαίες γεννήτριες υποφέρουν από εσωτερικές ροές που τις καθιστούν ευάλωτες . Ακόμη , η ποιότητα τους είναι ανάλογη με το μέγεθος και την τιμή τους όπως και οι αποτελεσματικές αληθινές γεννήτριες . Τα PUFsμπορούν να χρησιμοποιηθούν σαν γεννήτριες τυχαίων αριθμών . Οι συμβολοσειρές που παράγουν μπορούν να χρησιμοποιηθούν σαν συμμετρικά κλειδιά ή σαν τυχαίοι αριθμοί εκκίνησης για μια ψευδό-τυχαία γεννήτρια αριθμών χωρίς περαιτέρω επεξεργασία . Στην περίπτωση που θέλουμε τυχαίους αριθμούς για κρυπτογράφηση ασύμμετρων κλειδιών τότε λίγη παραπάνω επεξεργασία χρειάζεται για να επιτευχθούν τα απαραίτητα χαρακτηριστικά του κλειδιού .Έτσι τα οπτικά PUFs θεωρείται ότι μπορούν να αντικαταστήσουν τις παραδοσιακές πηγές παραγωγής τυχαίων αριθμών παράγοντας υψηλού βαθμού κρυπτογραφικά ασφαλείς τυχαίους αριθμούς συμβατούς με τα τυπικά κρυπτοσυστήματα.

Υπάρχουν πολλές ιδέες που μπορούν να υλοποιηθούν χρησιμοποιώντας τα οπτικά PUFsστο blockchain . Μία τέτοια ιδέα είναι για παράδειγμα να χρησιμοποιούμε το blockchain για την αποθήκευση δεδομένων που προηγουμένως έχει διασφαλιστεί η ασφάλεια των κλειδιών καθώς προέρχονται από οπτικά PUFs. Έτσι είναι εφικτή η διασφάλιση ότι τα δεδομένα δεν

έχουν παραβιαστεί ταυτόχρονα με τη δυνατότητα ιχνηλασιμότητας , λογοδοσίας και διαφανών ελεγκτικών δυνατοτήτων.

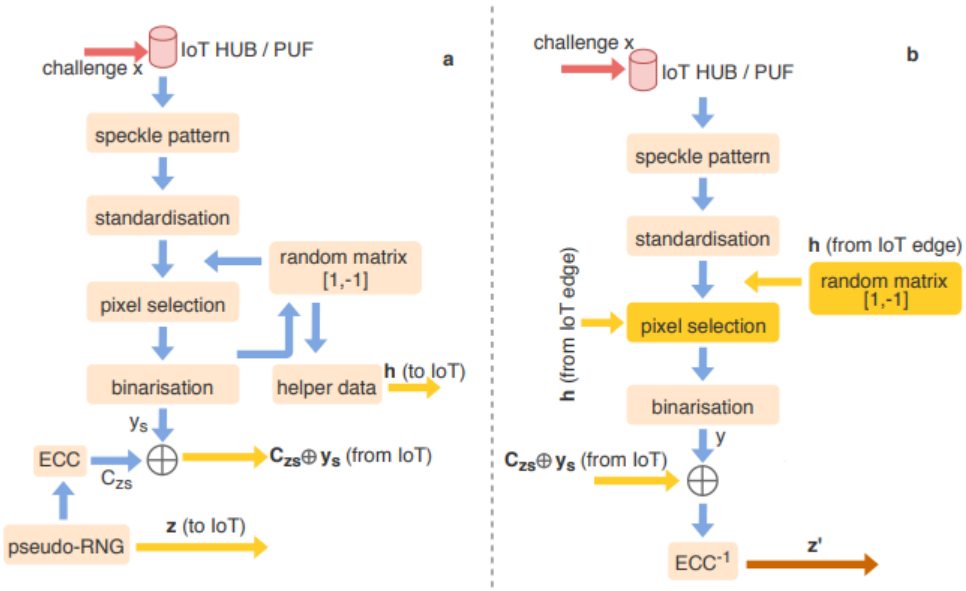
Χρήση των οπτικών PUFsσε συνδυασμό με ιδιωτικό blockchain για την ασφάλεια ενός οικοσυστήματος IoT

Ο στόχος είναι να διασφαλιστεί η ταυτοποίηση και η ακεραιότητα της επικοινωνίας μεταξύ των συσκευών του συστήματος IoTστο δίκτυο . Στην εικόνα βλέπουμε ένα τέτοιο οικοσύστημα.



Εικόνα 66: Σχήμα ενός οικοσυστήματος IoT και των συσκευών του (Charidimos Chaintoutis1, 2018) [1]

Αποτελείται από αρκετές συσκευές αιχμής καθώς και έναν εκκινητή δικτύου (IoT hub) που είναι εξοπλισμένος με το PUF. Όλες οι συσκευές είναι μέλη του ιδιωτικού δικτύου blockchain.Για να μπει μια συσκευή στο δίκτυο θα πρέπει να της αποσταλεί πρώτα μια πρόσκληση από τον εκκινητή δικτύου . Ο έλεγχος ταυτότητας μιας συσκευής αιχμής εκτελείται μέσω της ακόλουθης διαδικασίας που αποτελείται από τις φάσεις εγγραφής (αριστερά) και επαλήθευσης(δεξιά).



Εικόνα 67: Φάση εγγραφής μιας συσκευής αιχμής (αριστερά) και φάση ταυτοποίησης (δεξιά) (Charidimos Chaintoutis1, 2018) [1]

Όταν μια νέα συσκευή αιχμής θέλει να μπει στο οικοσύστημα , πραγματοποιείται η διαδικασία εγγραφής . Ο εκκινητής δικτύου επιλέγει τυχαία μια πρόκληση χαπό τις διαθέσιμες προκλήσεις . Η απόκριση παράγεται χρησιμοποιώντας Random Binary Hashingκαι παίρνουμε μια συμβολοσειρά από bits y_s μεγέθους m . Κατά τη διαδικασία εγγραφής παράγονται επίσης τα βοηθητικά δεδομένα τα οποία είναι ένας διαγώνιος τυχαίος πίνακας και ένας πίνακας επιλογής pixels. Την ίδια στιγμή παράγεται και ένα ψευδό-τυχαίο κλειδί zμήκους l. Στη συνέχεια μέσω της διόρθωσης σφαλμάτων (ECC) το κλειδί z μετατρέπεται σε C_{zs} μήκους m . Τέλος , υπολογίζεται το XOR των $C_{zs} \oplus y_s$. Στη συσκευή αιχμής στέλνονται τα $C_{zs} \oplus y_s$, το κλειδί z και τα βοηθητικά δεδομένα h .

Η φάση επαλήθευσης της διαδικασίας ταυτοποίησης φαίνεται στο δεξιό μέρος της εικόνας . Η συσκευή αιχμής έχει στην κατοχή της τα δεδομένα $C_{zs} \oplus y_s$, το κλειδί zκαι τα βοηθητικά δεδομένα hπου παρήχθησαν από την προηγούμενη φάση . Αυτά χρησιμοποιούνται ως είσοδοι και παίρνουμε μια απόκριση (ένα μοτίβο κηλίδων) και στη συνέχεια μέσω Binary Hashing μια συμβολοσειρά από bits$y$ μεγέθους m. Τέλος , υπολογίζεται το $y \oplus C_{zs} \oplus y_s$και μέσω της αντίστροφης επιδιόρθωσης σφαλμάτων εξάγεται το κλειδί z' . Αν τα κλειδιά z και z' είναι ίσα τότε η συσκευή αιχμής ταυτοποιείται. Σε αντίθετη περίπτωση αφαιρείται από το ιδιωτικό blockchain.

Κάθε συσκευή αιχμής είναι μοναδικά ταυτοποιημένη και τα κλειδιά ταυτοποίησης δεν αποθηκεύονται στο κέντρο ελέγχου καθώς παράγονται κατόπιν ζήτησης . Αυτό σημαίνει ότι ακόμη και αν ο κόμβοςIoT τεθεί σε κίνδυνο , ο εισβολέας δεν θα πάρει τον έλεγχο κανενός κλειδιού αφού δεν αποθηκεύονται εκεί . Αν παραβιαστεί μια συσκευή αιχμής , ο εισβολέας δεν θα μπορέσει να μάθει τα κλειδιά των άλλων συσκευών . Έτσι κι αλλιώς δεδομένης της ιδιότητας του blockchainπου προϋποθέτει συναίνεση , ο εισβολέας δεν θα μπορέσει να επηρεάσει σημαντικές αποφάσεις καθώς η πλειοψηφία των συσκευών θα παραμένει απαραβίαστη . Επιπλέον , αν χρησιμοποιούνται τα ίδια κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων προς ή από τον κόμβο IoT, η αυθεντικότητα και η ακεραιότητα των δεδομένων που παράγονται από τη συγκεκριμένη συσκευή μπορεί να αποδειχθεί κρυπτογραφικά και να συνδεθεί ξανά με την επαληθευμένη συσκευή. Τέλος , η αδυναμία ενός εισβολέα να επηρεάσει τις πληροφορίες μέσα στο block , μπορεί να θωρακίσει τη διαδικασία ελέγχου ταυτότητας και να παρέχει αξιόπιστα αποδεικτικά στοιχεία για παραβιάσεις ασφαλείας και να ενισχύσει τη δυνατότητα ελέγχου.

Φωτονική ψευδό-τυχαία γεννήτρια αριθμών χρησιμοποιώντας PUF βασισμένο σε κυματοδηγό για έλεγχο ταυτότητας στο Internet of Things

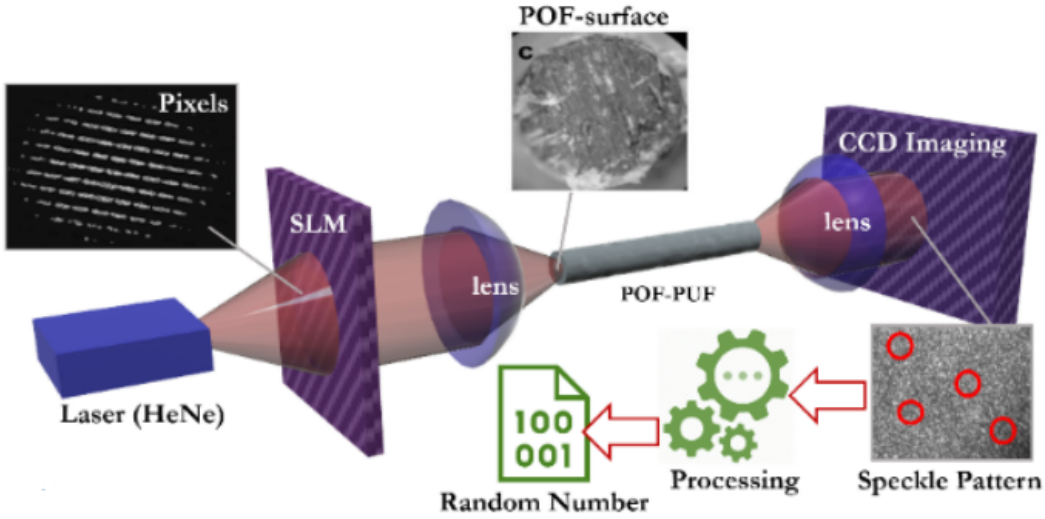
Στο κεφάλαιο 4 παρουσιάστηκε ένα οπτικό PUFβασισμένο σε έναν κυματοδηγό με μεγάλου μεγέθους πυρήνα . Αποδείχθηκε ότι είναι πολύ ανθεκτικό σε φυσική κλωνοποίηση σε σύγκριση με συμβατικές υλοποιήσεις παρόλο που ορίστηκε να λειτουργεί ως αδύναμο PUF.

Αυτό σημαίνει ότι η ασφάλεια του βασιζόταν μόνο στη φυσική μοναδικότητα του PUFκαι η τυχαιότητα των αποκρίσεων εφαρμόζοντας διαφορετικές προκλήσεις δεν αξιολογήθηκε.

Εδώ θα δούμε την αποτελεσματικότητα ενόςPUFsβασισμένου σε κυματοδηγό όσον αφορά στην στατιστική του ομοιότητα με αληθινές γεννήτριες τυχαίων αριθμών . Αυτό σημαίνει ότι θα πρέπει να παραχθεί ένας εκθετικά μεγάλος αριθμός αποκρίσεων . Η γραμμικότητα των αποκρίσεων παρακάμπτεται μέσω της χρήσης κάποιων τεχνικών μετά-επεξεργασίας και κατακερματισμού κωδικοποίησης της μέγιστης απόστασης (MDC) . Έτσι μπορούμε να εκμεταλλευτούμε τη χωρική πολυπλοκότητα του μοτίβου κηλίδων που παράγεται .Ο στόχος σε σχέση με το PUFπου παρουσιάζεται στο κεφάλαιο 4 , είναι να αποτελείται η συσκευή PUFαπό χαμηλού κόστους άμεσα διαθέσιμα εξαρτήματα ώστε να ελαχιστοποιείται το κόστος και το αποτύπωμα . Έτσι , μειώνοντας τις απαιτήσεις υλικού , καθίσταται κατάλληλο για αρχιτεκτονικές IoT. Προτείνεται η υλοποίηση ενός πρωτοκόλλου αμοιβαίας ταυτοποίησης που γίνεται πιο σκληρό μέσω του οπτικού PUF.

Πειραματικές ρυθμίσεις και επεξεργασία ακατέργαστων αποκρίσεων

Στην εικόνα φαίνεται το σχήμα του πειράματος

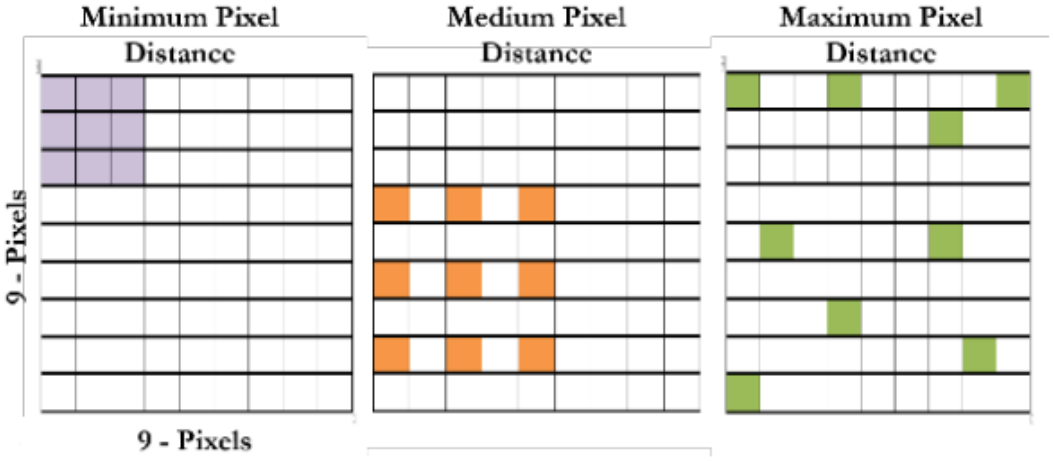


Εικόνα 68: Σχήμα απεικόνισης της προτεινόμενης υλοποίησης (MESARITAKIS, 2020)[8]

Αποτελείται από ένα μονότροπο σωλήνα laser HeNeπου εκπέμπει στα 632.8nmμε ισχύ εισόδου 1mWπου δρα ως μια συνεκτική οπτική πηγή. Στη συνέχεια τοποθετείται μια LCDδιαστάσεων 240x340 που δρα ως SLM(χωρικός διαμορφωτής φωτός) . Κάθε pixelμπορεί είτε να είναι ενεργοποιημένο είτε απενεργοποιημένο (0 ή 1) επιτρέποντας 2^N χωρικές καταστάσεις . Το N αντιστοιχεί στον αριθμό των pixelsπου προβάλλονται στην όψη της ίνας μέσω ενός φακού . Η ρύθμιση έγινε έτσι ώστε να επιτρέπεται η απεικόνιση 9x9 pixelstου SLMστην επιφάνεια του PUF. Ο πυρήνας του PUFαποτελείται από μία εμπορική οπτική ίνα , με πυρήνα 980μm, επένδυση 20μmκαι μήκος ίσο με 3cm. Οι οριακές συνθήκες της ίνας θεωρητικά επιτρέπουν την καθοδήγηση περισσότερων από $2*10^6$εγκάρσιων τρόπων . Στις όψεις τις ίνας εφαρμόστηκε ένα σύστημα τριβής με τυχαία κίνηση με στόχο να προκληθούν τυχαίες ατέλειες στην επιφάνεια τους . Έτσι , σε συνδυασμό με τις ακαθαρσίες εντός της ίνας και τις μηχανικές κάμψεις , ενεργοποιείται η τυχαιοποίηση της διατροπικής κατανομής ισχύος. Δεδομένου του γεγονότος ότι αυτοί οι τρόποι διάδοσης παρουσιάζουν διαφορετική

ταχύτητα φάσης και χωρικό προφίλ , επιτρέπεται η παραγωγή υψηλά πολύπλοκων μοτίβων κηλίδων . Η προβολή των εγκάρσιων τρόπων επιτυγχάνεται μέσω ενός δεύτερου φακού (στην εικόνα φαίνεται μετά το τέλος της ίνας) ενώ το επίπεδο απεικόνισης αποτελείται από CCD ως μονάδα απεικόνισης με 1280x960 pixels . Ένας μικροελεγκτής χαμηλού κόστος ελέγχει ταυτόχρονα και το SLMκαι το CCD.

Βάσει αυτών των δεδομένων , μπορούν να παραχθούν 2^{81}ζευγάρια πρόκλησης-απόκρισης . Ειδικότερα , μέσω των pixelstου SLMμπορούμε να ρυθμίσουμε το χωρικό προφίλ της δέσμης που φωτίζει την όψη της ίνας και συνεπώς να αλλάξουμε την αρχική διατροπική κατανομή ισχύος .Το περιορισμένο μήκος της ίνας (3cm) εμποδίζει την εξισορρόπηση ισχύος . Κάθε χωρικό μοτίβο στην είσοδο οδηγεί σε διαφορετική ανάμειξη των τρόπων στην έξοδο με αποτέλεσμα να έχουμε διακριτά μοτίβα κηλίδων στο επίπεδο απεικόνισης . Έτσι , αποκτήθηκαν πειραματικά 3 διακριτά σύνολα πρόκλησης-απόκρισης που αντιστοιχούν σε διαφορετικά σύνολα pixel του SLM. Στην εικόνα φαίνονται αυτά τα σύνολα.

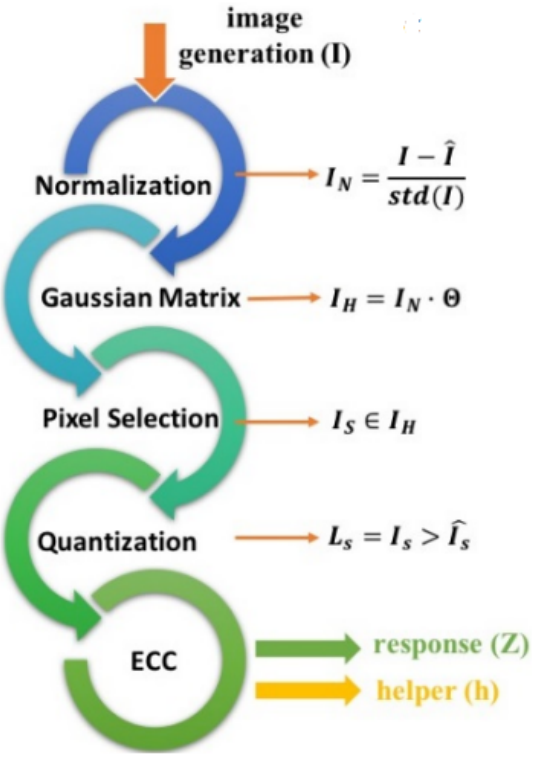


(MESARITAKIS, 2020)

Εικόνα 69: 3 διαφορετικά σύνολα με 3x3 pixelσ το καθένα αλλά με διαφορετικό χωρικό διαχωρισμό μεταξύ τους (MESARITAKIS, 2020)[8]

Όπως βλέπουμε , κάθε σύνολο αποτελείται από 3x3 pixelstων οποίων οι συνδυασμοί επιτρέπουν την εξαγωγή 2^9ζευγαριών πρόκλησης-απόκρισης και συνεπώς 1536 προκλήσεις από ένα σύνολο 2^{81} συνδυασμών. Το πρώτο σύνολο χρησιμοποιεί γειτονικά pixels ώστε να παρέχουν την ελάχιστη χωρική διακύμανση μεταξύ των πιθανών προκλήσεων και έτσι να τεστάρουν το σύστημα υπό αυστηρές συνθήκες . Στο δεύτερο και τρίτο σύνολο όπως βλέπουμε υπάρχει μεγαλύτερος χωρικός διαχωρισμός μεταξύ των pixelsώστε να υπάρχει μικρότερη χωρική επικάλυψη.

Οι καταγεγραμμένες αποκρίσεις τροφοδοτούνται και επεξεργάζονται από έναν προσωπικό υπολογιστή ώστε να ενεργοποιηθεί η δημιουργία τυχαίων αριθμών . Η διαδικασία της μετά-επεξεργασίας βασίζεται στη μέθοδο Random Binary. Η διαδικασία κατακερματισμού (Random Binary Hashing) φαίνεται στην ακόλουθη εικόνα .



Εικόνα 70: Σχήμα απεικόνισης της διαδικασίας κατακερματισμού (MESARITAKIS, 2020)[8]

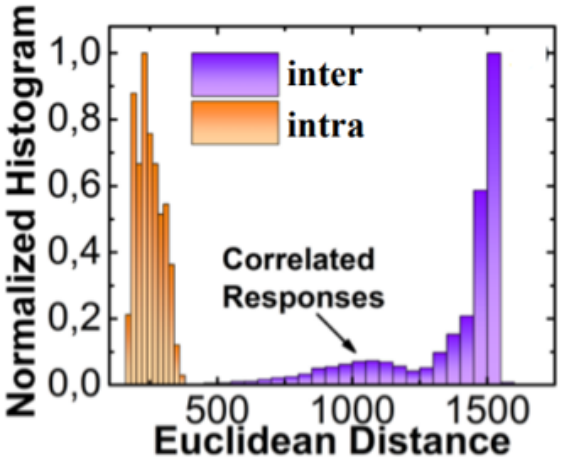
Πραγματοποιείται κανονικοποίηση της έντασης για την κάθε εικόνα , στη συνέχεια πολλαπλασιασμό με έναν τυχαίο πίνακα Θ . Οι τιμές του πίνακα Θ παρουσιάζουν κανονική κατανομή . Ο Θ είναι σταθερός για όλες τις εικόνες επομένως δε συμβάλει στην τυχαιότητα της απόκρισης . Κατόπιν γίνεται τυχαία επιλογή pixels, ακολουθώντας ομοιόμορφη κατανομήI_S.Τα αποτελέσματα κβαντίζονται με βάση τη μέση τιμή τους και εξάγεται μια δυαδική συμβολοσειρά Z από κάθε εικόνα . Τέλος , περιλαμβάνεται ένας τυπικός κώδικας διόρθωσης σφαλμάτων όπως ο BCHώστε να τροποποιηθούν οι επιπτώσεις του θορύβου στο σύστημα .

Πειραματικά αποτελέσματα

Φωτονικό PUFσαν ψευδό-τυχαία γεννήτρια αριθμών

Για να χρησιμοποιηθεί ένα PUFσαν μία γεννήτρια ψευδό-τυχαίων αριθμών θα πρέπει οι αποκρίσεις να είναι ασύνδετες με τις προκλήσεις οι οποίες τις παρήγαγαν και συνεπώς να είναι απρόβλεπτο . Θα πρέπει επίσης η διαδικασία να είναι ανθεκτική στο θόρυβο. Ως προκλήσεις χρησιμοποιούνται όλοι οι συνδυασμοί pixeltου SLM. Παρόλο που ο αριθμός των αποκρίσεων είναι εκθετικά μεγάλος , αναμένεται να εξαρτώνται γραμμικά .

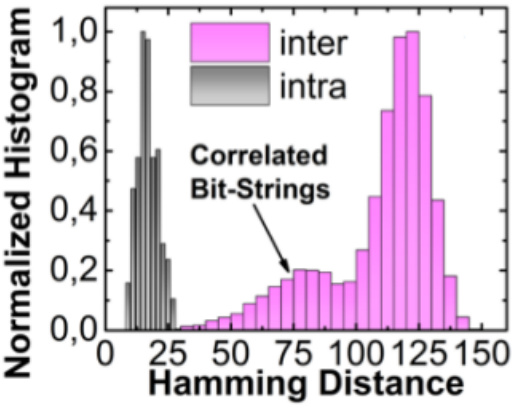
Το πρώτο μετρικό που χρησιμοποιείται είναι η ευκλείδια απόσταση για δύο διακριτά σύνολα δεδομένων . Το πρώτο σύνολο αποτελείται από τις αποκρίσεις , δηλαδή τις εικόνες που παίρνουμε για τις προκλήσεις που εφαρμόζουμε. Το δεύτερο σύνολο αποτελείται από 60 προκλήσεις για τις ίδιες προκλήσεις και αντικατοπτρίζει την ανθεκτικότητα στο θόρυβο . Τα δύο σύνολα φαίνονται στην εικόνα .



Εικόνα 71: Ιστόγραμμα ευκλείδειων αποστάσεων (MESARITAKIS, 2020)[8]

Η intra-distanceπαρουσιάζει μέση τιμή 245 και προέρχεται από μεταβολές στην ένταση των pixelsενώ η inter-distanceείναι αρκετά μεγαλύτερη παρουσιάζοντας μέση τιμή 1474. Παρατηρούμε όμως ότι υπάρχει μια οριακή μικρή επικάλυψη μεταξύ των 2 κατανομών γύρω από την τιμή 500. Αυτό σημαίνει ότι μπορεί να προκύψουν ψευδώς θετικά / αρνητικά . Η inter-distanceπαρουσιάζει ένα μεγάλο εύρος τιμών και αυτό οφείλεται στη γραμμική φύση της διαδικασίας σκέδασης κατά την οποία παράγονται αποκρίσεις . Αυτό συμβαίνει κυρίως όταν ζευγάρια προκλήσεων έχουν ενεργοποιημένα τα ίδια pixelστο SLM. Για την περίπτωση πολλών pixels, η πιθανότητα τα ίδια να είναι ενεργοποιημένα είναι μικρή και αυτός είναι ο λόγος για τον οποίο οι περισσότερες αποκρίσεις σε μια πρόκληση παρουσιάζουν μεγάλη τιμή inter-distanceκαι είναι ασυσχέτιστες. Για να γίνει πιο κατανοητό θα δοθεί ένα παράδειγμα . Αν 2 pixels P_1 ,P_2 είναι ενεργοποιημένα θα δώσουν μία κάπως όμοια απόκριση σε σχέση με το αν μόνο το P_1 ήταν ενεργοποιημένο και το P_2 ήταν απενεργοποιημένο ή αντίστροφα αν μόνο το P_2ήταν ενεργοποιημένο και το P_1ήταν απενεργοποιημένο . Αλλά η απόκριση που θα δώσουν σε σχέση με το αν ήταν και τα 2 απενεργοποιημένα είναι εντελώς ασυσχέτιστη . Επομένως για ένα μεγάλο αριθμό pixelsκαταλαβαίνουμε ότι οι περιπτώσεις ταύτισης των ενεργοποιημένων και απενεργοποιημένων pixelsείναι μικρές (τιμές από 500 έως 1250 περίπου) ενώ οι περιπτώσεις μη ταύτισης είναι σημαντικά περισσότερες (τιμές από 1250 και πάνω).

Αυτή η στατιστική ανωμαλία μπορεί να εξαλειφθεί μέσω της τεχνικής κατακερματισμού εικόνας που εφαρμόζεται στις ακατέργαστες αποκρίσεις . Για να επικυρωθεί αυτό , δημιουργήθηκε ένα σύνολο από συμβολοσειρές μήκους 256 bitsκατακερματίζοντας την κάθε απόκριση με τη διαδικασία που περιγράψαμε παραπάνω. Το ίδιο Θ και το ίδιο I_sχρησιμοποιήθηκε για όλες τις αποκρίσεις . Στην εικόνα που ακολουθεί βλέπουμε τις αποστάσεις Hamming (bits που αλλοιώθηκαν) για τις κατακερματισμένες εκδοχές των αποκρίσεων των 2 συνόλων δεδομένων intraκαι inter.

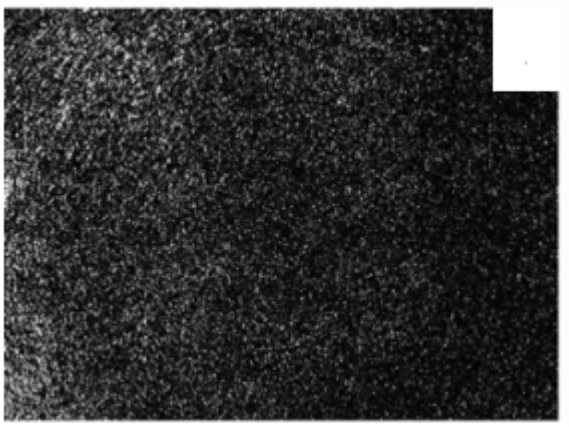


Εικόνα 72: Ιστόγραμμα αποστάσεων Hamming (MESARITAKIS, 2020)[8]

Είναι ξεκάθαρο ότι το πρόβλημα(μεγάλο εύρος τιμών) παραμένει ακόμη και μετά τον κατακερματισμό . Αυτό συνεπάγεται ότι η διαδικασία Random Binary hashing μετατρέπει τις εντάσεις των pixelsσε δυαδικές συμβολοσειρές , χωρίς όμως να προσθέτει στην εγγενή τυχαιότητα της ακατέργαστης απόκρισης . Συγκεκριμένα , η μέση τιμή απόστασης hammingγια την περίπτωση intraείναι 17.8 που σημαίνει ότι 6.9% των bitsαλλοιώνονται λόγω θορύβου ενώ στην περίπτωση intra, η μέση τιμή απόστασης hammingείναι 120.3 που σημαίνει ότι αλλοιώνεται το 46.9% των bits . Αυτή η απόκλιση από την ιδανική τυχαιότητα (50%) προκύπτει από το σωρευτικό αποτέλεσμα της γραμμικής συσχέτισης μεταξύ των εικόνων και της ύπαρξης σταθερών χωρικών χαρακτηριστικών , λόγω του φωτός του περιβάλλοντος κατά τη διενέργεια του πειράματος.

Ενίσχυση απροβλεπτότητας μέσω της χωρικής πολυπλοκότητας

Όπως είδαμε , τα αποτελέσματα των παραγόμενων αποκρίσεων παρουσιάζουν σημαντική προκατάληψη (δεν είναι αρκετά ασυσχέτιστες). Για αυτό το λόγο άλλες υλοποιήσεις οπτικών PUFαπέφευγαν των συνδυασμό pixelστο στοιχείο δημιουργίας προκλήσεων (SLM). Βέβαια , αν χρησιμοποιούνται μόνο πρωτόγονα pixelστότε ο αριθμός των πιθανών προκλήσεων κλιμακώνεται γραμμικά με τον αριθμό των pixelsκαι έτσι καθίσταται μη κατάλληλο για πραγματικές εφαρμογές παραγωγής κλειδιών. Παρακάτω βλέπουμε μια ακατέργαστη απόκριση , ένα μοτίβο κηλίδων , που παρουσιάζει ένα τεράστιο αριθμό χωρικών χαρακτηριστικών (φωτεινές-σκοτεινές κηλίδες).



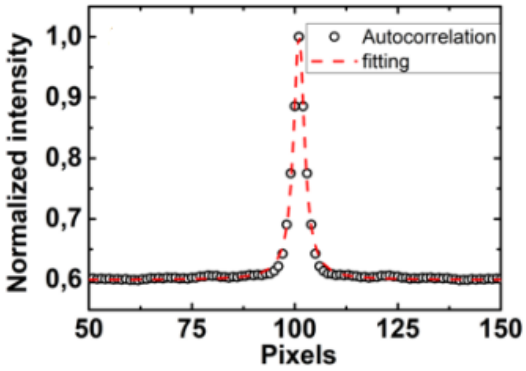
(MESARITAKIS, 2020)[8]

Εικόνα 73: Απεικόνιση μιας ακατέργαστης απόκρισης (μοτίβο κηλίδων)

Αν και κάθε εικόνα πιθανότατα έχει σημαντικά υψηλή εντροπία , μόνο ένα μέρος αυτής (256 bits) εξάγεται . Για την ποσοτικοποίηση της εντροπίας κάθε εικόνας και συνεπώς υπολογισμό του αριθμού των τυχαίων bitπου υπάρχουν σε κάθε απόκριση χρησιμοποιούμε την ακόλουθη εξίσωση:

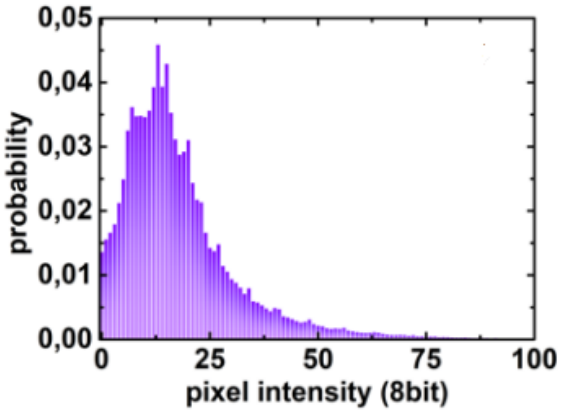
$$N = \frac{X*Y}{d}\sum_{i=1}^{256} I_i * log_2(I_i)$$ [8]

Όπου deίναι το μέσο μέγεθος κηλίδας , X και Yείναι τα κάθετα και οριζόντια pixelsστην εικόνα αντίστοιχα και I_iείναι η πιθανότητα για κάθε επίπεδο έντασης από 256 διαθέσιμες καταστάσεις . Στην εικόνα βλέπουμε την αποσυσχέτιση της εικόνας μετά την προσαρμογή υποθέτοντας κατανομή Cauchy.



Εικόνα 74: Διάγραμμα αποσυσχέτισης της εικόνας χρησιμοποιώντας κατανομή Cauchy (MESARITAKIS, 2020)[8]

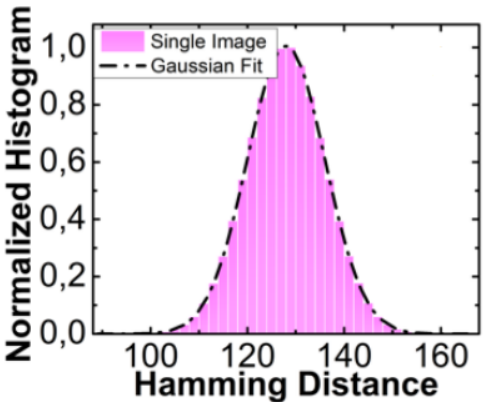
Το μέσο μέγεθος κηλίδας υπολογίστηκε στα d=3.2 pixelsπου ισούται με 1,6 φορές το κριτήριο του Nyquist .Στη συνέχεια , βλέπουμε το ιστόγραμμα έντασης για μια τυπική απόκριση ακολουθώντας συνάρτησηGamma.



Εικόνα 75 : Ιστόγραμμα πιθανότητας -έντασης μιας τυπικής απόκρισης (MESARITAKIS, 2020)[8]

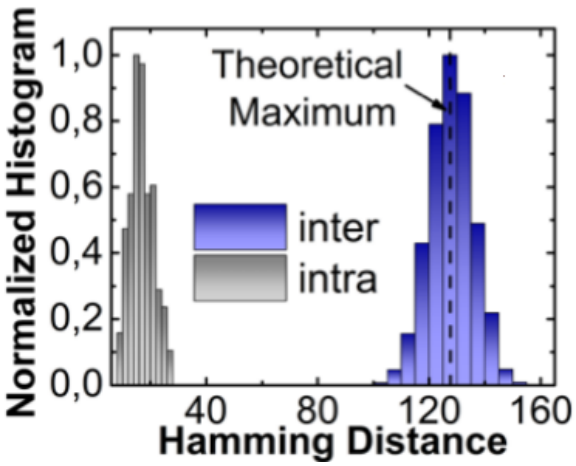
Μια τυπική απόκριση μπορεί να παράγει $2*10^6$ τυχαία bitsκαι επομένως μέχρι στιγμής σε κάθε ζευγάρι πρόκλησης-απόκρισης εξάγεται μόνο 0.012% της διαθέσιμης τυχαιότητας.

Διατηρείται το ίδιο τυχαίο Θ κατά τον κατακερματισμό και εφαρμόζεται η ίδια πρόκληση στο SLM, ενώ έχει αλλάξει το I_Sώστε να εξάγονται πολλές δυαδικές συμβολοσειρές ακόμη και από μία εικόνα . Έτσι , κατασκευάστηκαν 100 διαφορετικές δυαδικές συμβολοσειρές από μία μόνο απόκριση και στην εικόνα που ακολουθεί έχουν απεικονιστεί (το λογικό 1 για άσπρο και το λογικό 0 για μαύρο) . Οι αποστάσεις Hamming των δυαδικών συμβολοσειρών για αυτή την εικόνα φαίνονται στην εικόνα :



Εικόνα 76: Ιστόγραμμα αποστάσεων Hamming των δυαδικών συμβολοσειρών (MESARITAKIS, 2020)[8]

Η μέση τιμή είναι στο 50% (θεωρητικό όριο) ενώ το ιστόγραμμα ακολουθεί μία τέλεια Gaussian κατανομή . Άρα , προσαρμόζοντας τον μηχανισμό δημιουργίας προκλήσεων και υποθέτοντας ότι για κάθε συνδυασμό pixeltou LCDθα επιλεγεί ένα τυχαίο σύνολο 256 pixelsστο CCD, οι παραγόμενες αποκρίσεις θα πολλαπλασιαστούν από την εντροπία που υπάρχει σε κάθε εικόνα . Έτσι, η πρόκληση θα αποτελείται από ένα διάνυσμα από τα pixeltou LCDκαι από ένα διάνυσμα από τα pixeltou CCD ενώ η απόκριση θα παραμένει μια συμβολοσειρά μήκους 256 bits. Στην εικόνα , υπολογίστηκαν πάλι οι αποστάσεις Hamming για το σύνολο δεδομένων που υπολογίστηκαν και στην εικόνα πιο της προηγούμενης ενότητας αλλά χρησιμοποιώντας τη λογική που περιγράφηκε όπου η πρόκληση αποτελείται από 2 παράγοντες.



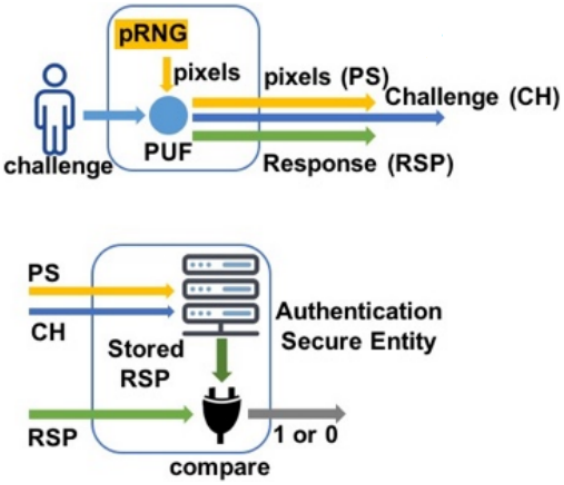
(MESARITAKIS, 2020)[8]

Εικόνα 77: Αποστάσεις Hamming για πρόκληση αποτελούμενη από 2 παραμέτρους

Αυτή η εναλλακτική τεχνική δεν επηρέασε καθόλου την απόσταση Hammingτου συνόλου δεδομένων intraλόγω του γεγονότος ότι ο θόρυβος είναι παρουσιάζεται εξίσου σε όλα τα pixelstou CCDανεξάρτητα από τη διαδικασία επιλογής . Αντιθέτως , η inter-distanceάλλαξε αρκετά , αυτός το μεγάλο εύρος τιμών της κατανομής (που θύμιζε μια ουρά στο γράφημα) εξαφανίστηκε , η μέση τιμή είναι στο ιδανικό 50% και η κατανομή ακολουθεί ένα Gaussianσχήμα. Έτσι , πλέον η έλλειψη επικάλυψης μεταξύ των 2 κατανομών σηματοδοτεί ότι η πιθανότητα ψευδώς θετικών ή ψευδώς αρνητικών μηδενίζεται.

Ωστόσο παρουσιάζονται 2 προβλήματα με αυτή τη λύση . Το πρώτο έγκειται στο ότι το φωτονικό PUFέχει στόχο να αντικαταστήσει τις συμβατικές ψευδό-τυχαίες γεννήτριες αλλά μέσω αυτής της προσέγγισης βασίζεται στην ύπαρξη και την ποιότητα τους ώστε να παρέχει ασφαλή λειτουργία (επιλογή pixels). Η εξάρτηση του PUFαπό την υποστήριξη ψευδό-τυχαίας γεννήτριας σημαίνει ότι το σύστημα είναι ευάλωτο σε επιθέσεις πλευρικού καναλιού , μειονέκτημα που συνήθως δε συναντάται στα οπτικά PUFs.

Το δεύτερο πρόβλημα προκύπτει στο σενάριο ελέγχου ταυτότητας της συσκευής . Σε αυτή την περίπτωση , ο χρήστης εφαρμόζει μια πρόκληση στο PUFώστε να πάρει μια δυαδική απόκριση RSPκαι τη μεταδίδει μαζί με την πρόκληση .



Εικόνα 78: Μετάδοση της πρόκλησης CH μαζί με την απόκριση RSP και το PS (MESARITAKIS, 2020)[8]

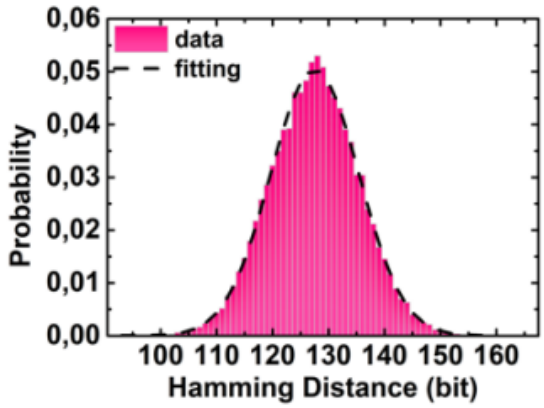
Οι αποκρίσεις αποθηκεύονται σε μια ασφαλή οντότητα του συστήματος, κατά τη διάρκεια της διαδικασίας εγγραφής η πρόκληση χρησιμοποιείται ώστε να εξαχθεί η απόκριση RSP' . Συγκρίνοντας τηνRSPμε την RSP' (RSP⊗RSP') επιτυγχάνεται η ταυτοποίηση . Σε αυτό το τροποποιημένο σενάριο που παρουσιάζεται , θα πρέπει επίσης να μεταδίδεται η επιλογή των pixel (PS) στην ασφαλή οντότητα . Το βάρος αυτής της προσέγγισης κλιμακώνεται με το μήκος του παραγόμενου τυχαίου αριθμού . Για παράδειγμα ένα κλειδί μήκους 256 bits, απαιτεί έξτρα 4096 bitsγια κάθε RSP(256 * 16bitγια τις συντεταγμένες του CCD).

Χωρική πολυπλοκότητα και κωδικοποίηση μέσης απόστασης

Ο στόχος είναι να διατηρηθεί η ενισχυμένη εντροπία κάθε εικόνας αλλά να εξαλειφθούν τα ελαττώματα που εισάγονται από την ψευδό-τυχαία γεννήτρια . Έτσι προτείνεται μια λύση ενός βελτιστοποιημένου σεναρίου δημιουργίας προκλήσεων .

Αντί το διάνυσμα επιλογής pixelsνα κατασκευάζεται τυχαία για κάθε πρόκληση , η δυαδική αναπαράσταση τροφοδοτείται στον κωδικοποιητή BCH(χρησιμοποιείται για τη διόρθωση σφαλμάτων). Οι κωδικές λέξεις κατασκευάζονται ώστε να παρουσιάζουν μέγιστη απόσταση Hamming . Το μήκος της πρόκλησης που υποστηρίζεται από κωδικοποίησης μέγιστης απόστασης μπορεί να επιλεγεί ώστε να είναι μεγαλύτερο από K*2^m , όπου K είναι το μήκος του τυχαίου αριθμού σε bitsκαι m≥ log_2(X*Y) με X και Y οι διαστάσεις τις εικόνας σε pixels. Δεδομένου ότι η δυαδική είσοδος στον BCHείναι χωρικές συντεταγμένες , στην πρόκληση θα επιλεγούν τα pixelπου εμφανίζουν τη μέγιστη χωρική απόσταση μεταξύ τους (λόγω του BCH) .Η επιλογή των pixelμπορεί να είναι προϋπολογισμένη και δημόσια , επομένως δεν υπάρχει ανάγκη μετάδοσης μιας μεγάλης πρόκλησης σε αντίθεση με το σενάριο που απεικονίζεται στην εικόνα πάνω. Αυτή η προσέγγιση επιπλέον , μπορεί να παρέχει έναν όχι τυχαίο τρόπο επιλογής των pixelγια την κατασκευή του διανύσματος και συνεπώς εξαφανίζει την ανάγκη για μια αλγοριθμική ψευδό-τυχαία γεννήτρια καθώς και τις ευπάθειες που αυτή εισάγει.

Έτσι , κάθε πρόκληση μετατρέπεται μέσω του BCH σε ένα σταθερό σύνολο συντεταγμένων τωνpixelπου χρησιμοποιούνται κατά τον κατακερματισμό . ΕΙΚΟΝΕΣ !!! Η απόσταση hammingγια την περίπτωση interφαίνεται στην εικόνα.

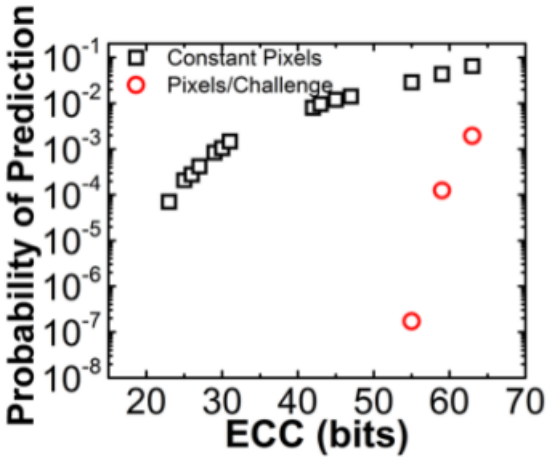


Εικόνα 79 : Αποστάσεις Hamming για την inter distance (MESARITAKIS, 2020)[8]

Όπως βλέπουμε η απόσταση Hammingείναι στο θεωρητικό μέγιστο (περίπου 128 bits) και δεν παρατηρούνται στατιστικές ανωμαλίες .Η περίπτωση της intraδεν χρειάζεται να απεικονιστεί καθώς όπως και πιο πάνω , η εναλλακτική επιλογή pixelστο CCDδεν επηρεάζει το επίπεδο θορύβου και συνεπώς δεν αλλοιώνονται καθόλου bits.

Στο επίπεδο της ασφάλειας , αντί να υπολογιστεί η πιθανότητα φυσικής κλωνοποίησης , εκτιμάται η πιθανότητα μιας διπλότυπης απόκρισης RSPγια διαφορετικές CH. Κάθε απόκριση RSPσυνοδεύεται από βοηθητικά δεδομένα εκτός του CHκαι του PSπου περιλαμβάνουν πλεονάζοντα bitsπου παράγονται ξανά μέσω του BCHώστε να προστατεύονται από αλλοιωμένα από το θόρυβο bits.Αυτό το βήμα είναι πολύ σημαντικό αν το σύστημα χρησιμοποιείται σαν ντετερμινιστική πηγή τυχαιότητας. Αυτό σημαίνει ότι ο χρήστης αντί να αποθηκεύει το κλειδί , το αναπαράγει κάθε φορά χρησιμοποιώντας το ίδιο CHστο ίδιο PUF. Συνεπώς , θα πρέπει η απόκριση RSPνα είναι χρονικά αμετάβλητη και άρα χρειάζεται να συμπεριλάβουμε ECC. Ο ECCμπορεί να μειώσει τις μεταβολές λόγω θορύβου αλλά και να επηρεάσει τις αλλαγές στην RSPπου προκύπτουν λόγω μεταβολής του CH. Η πιθανότητα πρόβλεψης υπολογίζεται συναρτήσει του αριθμού των ECC bits.

Στην εικόνα βλέπουμε την πιθανότητα δύο διαφορετικές προκλήσεις CHνα αντιστοιχούν στην ίδια απόκριση RSPσυναρτήσει των ECC bitsγια την τυπική διαδικασία κατακερματισμού με τετράγωνα . Με κύκλους βλέπουμε την ίδια πιθανότητα αλλά για το τροποποιημένο σενάριο που συνεπάγεται την αλλαγή των PSσε κάθε CH.



Εικόνα 81: Διάγραμμα πιθανότητας πρόβλεψης συναρτήσει του αριθμού των ECC bits (MESARITAKIS, 2020)[8]

Όπως παρατηρούμε , το τροποποιημένο σενάριο είναι σημαντικά ισχυρότερο . Συγκεκριμένα , για την τυπική επεξεργασία του PUF, αν συμπεριλάβουμε 55 ECC bitsη πιθανότητα πρόβλεψης είναι 10^{-2} ενώ για την προτεινόμενη τροποποιημένη προσέγγιση η πιθανότητα πρόβλεψης είναι 10^{-7}δηλαδή 5 τάξεις μεγέθους μικρότερη. Πέραν αυτού , για λιγότερα ECC bits η πιθανότητα πρόβλεψης για την τροποποιημένη προσέγγιση είναι μηδενική .

Αξιολόγηση τυχαιότητας δημιουργίας προκλήσεων με τη βοήθεια MDC

Τα αποτελέσματα που είδαμε δείχνουν ότι το οπτικό PUFπου βασίζεται σε κυματοδηγό πέραν του ότι είναι ανθεκτικό στην αντιγραφή μπορεί επίσης να χρησιμοποιηθεί σαν μια φωτονική ψευδό-τυχαία γεννήτρια αριθμών . Για να επιβεβαιωθεί αυτός ο ισχυρισμός , οι δυαδικές συμβολοσειρές που παρήγαγε το PUFδοκιμάστηκαν χρησιμοποιώντας τυχαίες τυπικές δοκιμές. Το πρώτο τεστ είναι το NISTπου αξιολογεί την ομοιότητα των στατιστικών ιδιοτήτων της γεννήτριας με μια πραγματικά τυχαία πηγή. Βασική προϋπόθεση για αυτό το τεστ είναι να εφαρμοσθεί σε ένα σύνολο δεδομένων μεγέθους τουλάχιστον 1 Gbitγια να πετύχουμε έναν παράγοντα σιγουριάς α=0.1 . Έτσι εκμεταλλευτήκαμε τη συνολική εντροπία ανά απόκριση . Από ένα αρχικό σύνολο 1536 εικόνων , κάθε απόκριση κατακερματίστηκε αρκετές φορές (αλλάζοντας σε κάθε περίπτωση τοPS) ώστε να εξαχθούν 4000 αποκρίσεις μήκους 256 bitsανά εικόνα .4000*256 ισούται με 1Mbitπου είναι μικρότερο από το μέγιστο των 2Mbittυχαίων bitsσε κάθε εικόνα που υπολογίστηκε πιο πάνω . Τα αποτελέσματα των 15 NIST τεστ φαίνονται στον πίνακα.

Table 1. NIST Test PUF Results

Test	p-Value	Success (%)
Block Frequency	0.7645	98.75
Cumulative Sums-1	0.4895	98.5
Entropy	0.6111	99%
FFT	0.3306	98.5
Mono-Bit	0.9512	98.75
Linear Complexity	0.7349	98.75
Longest Run	0.689	97.75
Non-Overlapping Templates-1	0.1372	97.75
Overlapping Templates	0.7498	98.25
Random Excursion Variable-1	0.3431	98.18
Random Excursions	0.1394	97.27
Rank	0.1969	99.75
Runs	0.2429	98.75
Serial	0.1473	98
Universal	0.0308	99.5

Πίνακας 4: Αποτελέσματα του NIST test (MESARITAKIS, 2020)[8]

Όπως βλέπουμε , το προτεινόμενο PUF γεννήτρια με κυματοδηγό περνά όλα τα τεστ διατηρώντας την τιμή p-Valuekαι έτσι οι παραγόμενες αποκρίσεις δεν μπορούν να διακριθούν στατιστικά από μια πραγματική τυχαία πηγή.

Στην ίδια λογική , το ίδιο σύνολο δεδομένων τροφοδοτήθηκε σε ένα σύνολο από τεστ που λέγεται DIEHARD. Το DIEHARDαξιολογεί την απόδοση της γεννήτριας ως τυχαία πηγή. Για λόγους σύγκρισης στο DIEHARDτροφοδοτήθηκε επίσης και ένα δεύτερο σύνολο δεδομένων που προέρχεται από μια πραγματική τυχαία γεννήτρια. Στον πίνακα βλέπουμε τα αποτελέσματα για 17 τεστ (p-values) για το προτεινόμενο PUFενώ για την πραγματική τυχαία γεννήτρια αν περνά ή αν δεν περνά το τεστ (pass/fail).

Table 2. DIEHARD(ER) PUF/TRNG Test Results

Test	p-Value (No.)	PUF	TRNG
Birthday Test	0.2351	pass	pass
Operm5	0.000005	weak	pass
Rank 32x32	0.9407	pass	pass
Rank 6x8	0.8511	pass	pass
Bitstream	0.6166 (20)	pass	weak
Opso	0.9291 (23)	pass	pass
Oqso	0.6205 (28)	pass	pass
Dna	0.5877 (31)	pass	pass
Count 1s str	0.3582	pass	pass
Count 1s byte	0.6851	pass	pass
Parking Lot	0.4982	pass	pass
2D Spheres	0.4488	pass	pass
3D Spheres	0.9504	pass	pass
Squeeze	0.267	pass	weak
Sums	0.0535	pass	pass
Runs	0.8361	pass	pass
Craps	0.368	pass	pass
	Dieharder		
Tsang gcd	0	fail	fail
Monobit	0.5442	pass	pass
Runs sts	0.9448	pass	weak
Serial*	0.1288 (31)	pass	pass

RGB bit dist.-1	0.0766 (12)	pass	pass
RGB min Dist.-1	0.0288 (5)	pass	weak
RGB perm.-1	0.1761 (4)	pass	pass
RGB lagged -2	- (32)	pass/fail	pass/fail
RGB Kstest	0.454	pass	pass
Byte distr.	0	fail	fail
DCT	0.9235	pass	pass
Filltree-1	0.0586 (2)	pass	weak
Filltree 2-1	0.000584	weak	fail
Monobit2	1	fail	fail

Πίνακας 5: Αποτελέσματα του test DIEHARD και DIEHARDER για το προτεινόμενο PUF και για την πραγματική τυχαία γεννήτρια αριθμών (TRNG) (MESARITAKIS, 2020)[8]

Τα αποτελέσματα που παρήγαγε το PUFπερνάνε όλα τα τεστ του DIEHARDενώ η πραγματική τυχαία γεννήτρια παρουσιάζει κάποια αδύναμα αποτελέσματα για πολλά τεστ τα οποία περνά οριακά . Το PUF έδωσε μόνο ένα αδύναμο αποτέλεσμα .Εφαρμόστηκαν επίσης 14 επιπλέον τεστ του DIEHARDER. Σε αυτά οι αποκρίσεις του οπτικού PUFαπέτυχαν σε 4 τεστ ενώ της πραγματικής τυχαίας γεννήτριας σε 5 τεστ και επιπλέον είχαν πολλά αδύναμα αποτελέσματα που οριακά πέρασαν. Αυτά τα στατιστικά επιβεβαιώνουν τη στατιστική ομοιότητα των παραγόμενων αποκρίσεων με πραγματικές τυχαίες γεννήτριες. Τέλος , θα πρέπει να εξεταστεί η ανθεκτικότητα των παραγόμενων δυαδικών συμβολοσειρών σε τεχνικές συμπίεσης δεδομένων . Ένας βασικός αλγόριθμος που χρησιμοποιείται για τη συμπίεση δεδομένων είναι ο context-weight-tree. Για τη συγκριτική αξιολόγηση χρησιμοποιήθηκαν τα δεδομένα του PUF , ένα κανονικό αρχείο κειμένου , ένα αρχείο που περιέχει μόνο λογικά 0 , δυαδικές συμβολοσειρές που παράχθηκαν από ψευδό-τυχαίο αλγόριθμο και την πηγή της πραγματικής τυχαίας γεννήτριας που χρησιμοποιήθηκε παραπάνω. Για τη σωστή σύγκριση όλα τα σύνολα δεδομένων είχαν το ίδιο μέγεθος.

Στον πίνακα βλέπουμε το ρυθμό συμπίεσης (Cr) για κάθε τεχνική σε bits/bytes.

Table 3. CTW Compression Results

Source	Cr
Zero Padding File	0.00586
CIA Fact book	1.44178
Ziggurat	8.00755
PUF	8.00752
TRNG	8.00754

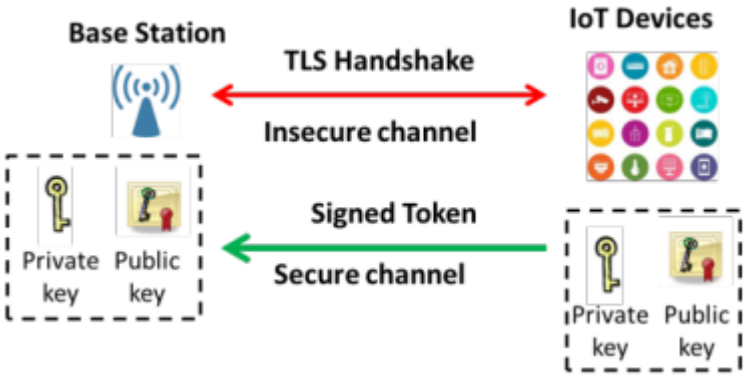
Πίνακας 6: Ρυθμός συμπίεσης για κάθε τεχνική (MESARITAKIS, 2020)[8]

Για παράδειγμα αν το Cr=8 σημαίνει ότι δεν έγινε καθόλου συμπίεση ενώ αν το Creίναι πολύ μικρότερο του 8σημαίνει ότι υπήρχε ένας σημαντικός πλεονασμός στα bytetου κάθε συνόλου δεδομένων. Προφανώς , το αρχείο που περιείχε μόνο μηδενικά είναι λογικό να παρουσιάζει την υψηλότερη συμπίεση αφού δεν έχει καθόλου εντροπία . Το αρχείο κειμένου στα αγγλικά παρουσίασε επίσης υψηλό επίπεδο συμπίεσης . Από την άλλη , ο αλγόριθμος Ziggurat, το PUFκαι η πραγματική τυχαία γεννήτρια έδωσαν σχεδόν ίδιο αποτέλεσμα (Cr=8bits/byte) που ξεκάθαρα σηματοδοτεί την υψηλή ανθεκτικότητα στη συμπίεση λόγω της υψηλής εντροπίας. Καταλήγουμε δηλαδή στο συμπέρασμα ότι από στατιστικής άποψης , το βελτιστοποιημένο PUFπαρέχει ίδια αποτελέσματα με μια πραγματική τυχαία γεννήτρια.

Αμοιβαίος έλεγχος ταυτότητας χρησιμοποιώντας φωτονικό PUFπηγή εμπιστοσύνης

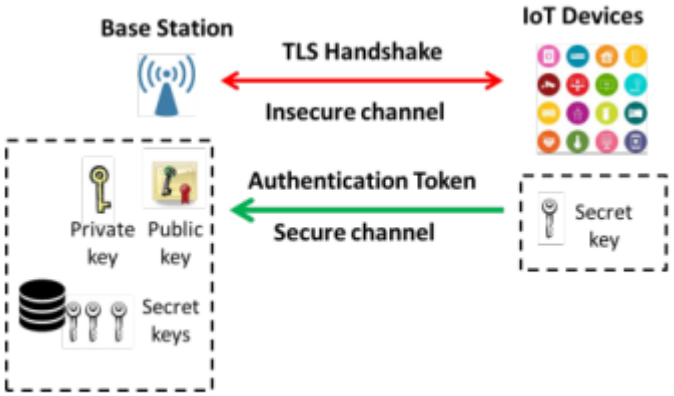
Ας δούμε τα πλεονεκτήματα του σχήματος που περιγράφηκε στο IoT. Εξετάζονται 2 σενάρια αμοιβαίου ελέγχου ταυτότητας όπου ένας σταθμός βάσης (BS) με πρόσβαση στο internetρυθμίζεται για τον έλεγχο ταυτότητας πολλών συσκευών και χρηστών . Ο σταθμός βάσης χρησιμεύει είτε ως ενδιάμεσο μεταξύ των αισθητήρων και μιας υποδομής cloudή είναι η κύρια πηγή υπολογισμού στην περίπτωση συσκευών αιχμής. Η πιο συνηθισμένη περίπτωση χρήσης είναι αυτή όπου οι συσκευές IoTπου χρησιμοποιούνται μπορούν να εκτελούν λειτουργίες δημοσίου κλειδιού και ότι υποστηρίζεται από τα πρωτόκολλα SSL/TLS 1.2 ή 1.3 . Ο έλεγχος ταυτότητας χωρίζεται σε 2 φάσεις . Στην πρώτη φάση , το πρωτόκολλο Handshaketου SSL/TLSχρησιμοποιείται για τον έλεγχο ταυτότητας του σταθμού βάσης. Ο σταθμός βάσης κατέχει ένα ζευγάρι δημοσίου/ιδιωτικού κλειδιού που χρησιμοποιείται για την απόδειξη της ταυτότητας του μέσω δημοσίου καναλιού . Όταν η πρώτη φάση εκτελεστεί επιτυχώς , δημιουργείται ένας ασφαλές κανάλι μεταξύ του σταθμού και της συσκευής. Στη δεύτερη φάση , η συσκευή ταυτοποιείται χρησιμοποιώντας το ασφαλές κανάλι και το πρωτόκολλο Recordtου SSL/TLS .Διακρίνονται 2 περιπτώσεις ανάλογα με τον τύπο των διαπιστευτηρίων που είναι διαθέσιμα , η περίπτωση του δημοσίου κλειδιού και η υβριδική περίπτωση .

Στην πρώτη περίπτωση , η συσκευή έχει επίσης ένα ζευγάρι δημοσίου/ιδιωτικού κλειδιού . Το δημόσιο κλειδί διανέμεται χρησιμοποιώντας ένα πιστοποιητικό X.509 και το ιδιωτικό κλειδί πρέπει να αποθηκεύεται στη συσκευή. Το πιστοποιητικό μπορεί να σταλεί είτε όταν η συσκευή προσπαθεί να συνδεθεί είτε να αποθηκευτεί στο σταθμό βάσης όταν η συσκευή καταχωρηθεί από τον ιδιοκτήτη της. Η συσκευή αποδεικνύει την ταυτότητα της υπογράφοντας ένα σύντομο μήνυμα με το ιδιωτικό κλειδί . Τέλος , ο σταθμός βάσης επαληθεύει την υπογραφή και την ταυτότητα με το δημόσιο κλειδί από το πιστοποιητικό όπως βλέπουμε στην εικόνα .



Εικόνα 82: Σχηματική απεικόνιση του σεναρίου ενός δημοσίου/ιδιωτικού κλειδιού (MESARITAKIS, 2020)[8]

Στο υβριδικό σενάριο , γίνεται κρυπτογράφηση συμμετρικού κλειδιού για τον έλεγχο ταυτότητας της συσκευής. Η λογική είναι η ίδια με τον έλεγχο ταυτότητας μέσω ενός κωδικού πρόσβασης όπου η συσκευή και ο σταθμός βάσης μοιράζονται το ίδιο μυστικό κλειδί. Όταν η συσκευή καταχωρήθηκε στο σταθμό βάσης , αυτό το μυστικό κλειδί αποθηκεύτηκε στην τοπική βάση δεδομένων του σταθμού βάσης. Το ίδιο μυστικό κλειδί αποθηκεύεται και στην συσκευή . Μετά τον έλεγχο ταυτότητας του σταθμού βάσης , το πρωτόκολλο Recordtou SSL/TLSπροστατεύει την επικοινωνία μεταξύ των 2 οντοτήτων . Με αυτό τον τρόπο , η συσκευή μπορεί με ασφάλεια να στείλει το μυστικό κλειδί μη κρυπτογραφημένο μέσω του ασφαλούς καναλιού για να αποδείξει την ταυτότητα του .



Εικόνα 83: Σχηματική απεικόνιση του υβριδικού σεναρίου (MESARITAKIS, 2020)[8]

Ο σταθμός και οι συσκευές IoTπρέπει να αποθηκεύουν και να προστατεύουν τα διαφορετικά μυστικά κλειδιά , ανάλογα με το σενάριο ελέγχου ταυτότητας . Το σενάριο αυτό φαίνεται στον πίνακα .

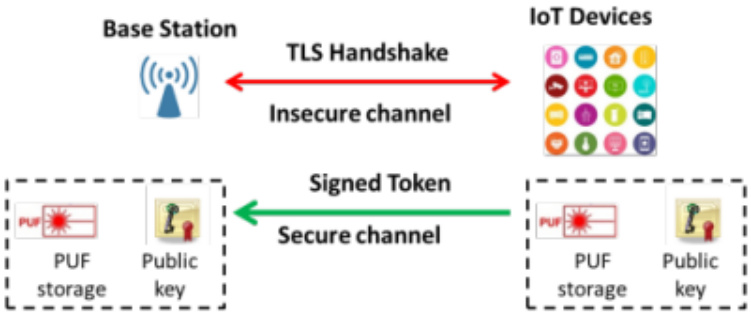
	Public key Scenario	Hybrid Scenario
Base Station	1Private key	1Private key
		N secret keys
IoT Device	1Private key	1secret key

Πίνακας 7: Απεικόνιση των αναγκαίων κλειδιών για κάθε σενάριο για το σταθμό βάσης και για τη συσκευή IoT (MESARITAKIS, 2020)[8]

Στην περίπτωση του δημοσίου κλειδιού , ο σταθμός βάσης και η συσκευή πρέπει να αποθηκεύουν μόνο το δικό του ιδιωτικό κλειδί . Στο υβριδικό σενάριο , ο σταθμός βάσης αποθηκεύει το δικό του ιδιωτικό κλειδί αλλά και όλα τα N μυστικά κλειδιά των καταχωρημένων συσκευών ενώ η συσκευή IoTαποθηκεύει το μυστικό κλειδί που μοιράζεται με το σταθμό βάσης . Πρέπει όλα αυτά τα κλειδιά να είναι ασφαλισμένα .

Σε αυτό το σημείο , αντί να χρησιμοποιηθεί ακριβό hardware, προτείνεται μια εναλλακτική λύση βασισμένη σε PUF . Η λογική βασίζεται στο ότι αντί να αποθηκεύονται τα κλειδιά , τα υπολογίζουμε εκείνη τη στιγμή σαν εξόδους του PUF .

Πιο συγκεκριμένα , όλα τα σχήματα δημοσίου κλειδιού έχουν μια αρχική φάση στην οποία υπολογίζεται το ζευγάρι ιδιωτικού/δημοσίου κλειδιού . Στις περισσότερες περιπτώσεις όπως στον αλγόριθμο ψηφιακής υπογραφής DSA, το ιδιωτικό κομμάτι του ζευγαριού κλειδιών είναι μια τυχαία επιλεγμένη τιμή Rκαι μετά το δημόσιο κομμάτι του κλειδιού υπολογίζεται ντετερμινιστικά από το ιδιωτικό κλειδί . Στη διαδικασία δημιουργίας ζευγαριών κλειδιών μπορεί εύκολα να ενσωματωθεί το PUF .Άρα αντί να χρησιμοποιείται απευθείας η τυχαία επιλεγμένη τιμή Rσαν ιδιωτικό κλειδί , η τιμή αυτή μπορεί πρώτα να φιλτραριστεί από το PUFκαι στη συνέχεια η έξοδος να χρησιμοποιηθεί ως ιδιωτικό κλειδί . Έτσι , κάθε φορά που χρειάζεται το ιδιωτικό κλειδί , το Rτροφοδοτείται στο PUFκαι το ιδιωτικό κλειδί παράγεται εκείνη τη στιγμή και δεν αποθηκεύεται ποτέ . Όπως βλέπουμε στην εικόνα , η εμπιστευτικότητα του PUFδεν χρειάζεται να είναι προστατευμένη.

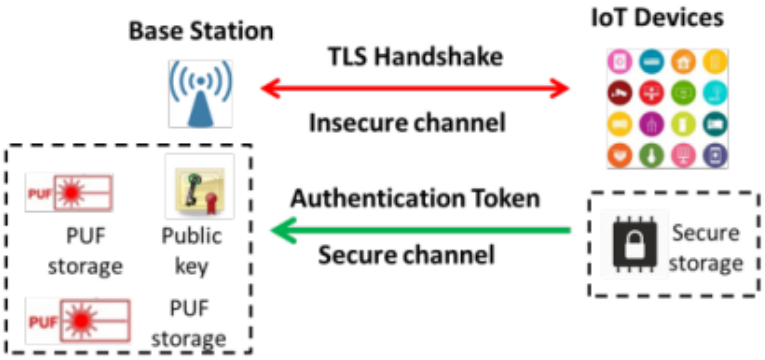


Εικόνα 84: Ενσωμάτωση του PUF στο σενάριο (MESARITAKIS, 2020)[8]

Ομοίως , στο συμμετρικό κλειδί , η ασφαλής αποθήκευση του κοινού μυστικού μπορεί να αντικατασταθεί από υπολογισμό εκείνη τη στιγμή του κλειδιού κάθε φορά που χρειάζεται

κλειδί . Το κλειδί φυσικά είναι η έξοδος του PUFκαι σαν είσοδος χρησιμοποιείται μια τυχαία τιμή Rκαι για άλλη μια φορά η εμπιστευτικότητα του PUFδεν χρειάζεται να είναι προστατευμένη.

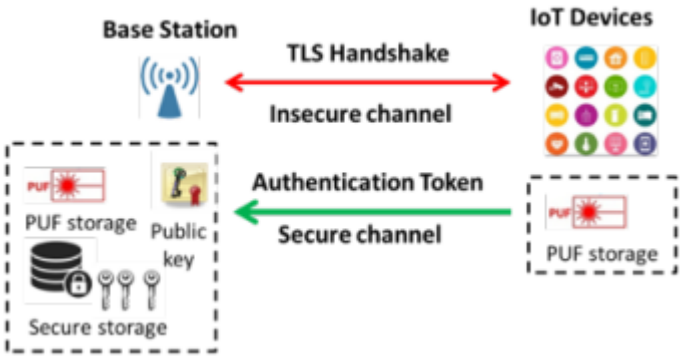
Ωστόσο , η ιδιότητα της μη κλωνοποιησιμότητας του PUFεπιφέρει έναν περιορισμό . Αυτός είναι το γεγονός ότι ο σταθμός βάσης και η συσκευή IoTδεν μπορούν και οι 2 να χρησιμοποιήσουν το ίδιο PUFγια να αποθηκεύσουν το κοινό κλειδί . Κάποια από τις 2 αυτές οντότητες πρέπει να χρησιμοποιήσει ασφαλές hardware .Επομένως το υβριδικό σενάριο ελέγχου ταυτότητας έχει 2 μεταβλητές. Στην πρώτη περίπτωση που βλέπουμε στην εικόνα , το PUFχρησιμοποιείται από το σταθμό βάσης και άρα κάθε συσκευή θα πρέπει να κατέχει ασφαλές hardwareμνήμης.



Εικόνα 85: Ενσωμάτωση του PUF στο υβριδικό σενάριο (MESARITAKIS, 2020)[8]

Σε αυτήν την περίπτωση , ο σταθμός βάσης πρέπει απλά να αποθηκεύσει απροστάτευτα τις τυχαίες τιμές Rπου αντιστοιχούν στην κάθε συσκευή.

Στη δεύτερη περίπτωση , το PUFχρησιμοποιείται από τις συσκευές IoTκαι ο σταθμός βάσης χρησιμοποιεί ασφαλές hardwareμνήμης για να αποθηκεύσει όλα τα κοινά κλειδιά .



Εικόνα 86: Αποθήκευση των κλειδιών στο σταθμό βάσης

(MESARITAKIS, 2020)[8]

Συνοπτικά , οι επιλογές σχεδίασης φαίνονται στον πίνακα .

	Public key Scenario	Hybrid Scenario	
Base Station	1 PUF	1 PUF	1 PUF
		1 PUF	N secHW
IoT Device	1 PUF	1secHW	1 PUF

Πίνακας 8 : Απεικόνιση των αναγκαίων PUF για κάθε σενάριο για το σταθμό βάσης και για τη συσκευή IoT [8]

Συμπεράσματα από την προτεινόμενη υλοποίηση με PUF

Ένα PUFπου βασίζεται σε οπτικό κυματοδηγό επεκτείνεται ώστε να δημιουργηθεί μια φωτονική μονάδα χαμηλού κόστους που μπορεί να χρησιμοποιηθεί ως μια αδύνατον να αντιγραφεί ασφαλής ντετερμινιστική ψευδό-τυχαία γεννήτρια με την ικανότητα να παράγει έναν εκθετικά μεγάλο αριθμό αποκρίσεων . Η γραμμικότητα της διαδικασίας οπτικής σκέδασης που προκύπτει όταν χρησιμοποιούνται συνδυασμοί από pixelsστην πρόκληση και προκαλεί υψηλά συσχετιζόμενες αποκρίσεις παρακάμπτεται με την επινόηση μιας νέας διαδικασίας επεξεργασίας των αποκρίσεων . Εκμεταλλευόμαστε το MDCώστε να επιλεγούν pixelsπου εμφανίζουν μέγιστη χωρική απόσταση μεταξύ τους και συνδέονται με την εφαρμοσμένη πρόκληση . Όλη αυτή η διαδικασία είναι υπολογιστικά ασφαλής , η πρόκληση μπορεί να προϋπολογιστεί και συνεπώς να είναι δημόσια . Οι δυαδικές αποκρίσεις που παράγονται αξιολογήθηκαν από μια σειρά τυπικών αξιολογήσεων τυχαιότητας όπως το DIEHARD , DIEHARDER , NISTκαι το CTW . Περνώντας όλα τα τεστ απέδειξαν ότι δεν διαφέρουν στατιστικά από μία πραγματική τυχαία γεννήτρια αριθμών . Τέλος , λόγω των πολλών πλεονεκτημάτων που παρουσιάστηκαν , κρίνεται ότι η προτεινόμενη υλοποίηση μειώνει την ανάγκη για υψηλού κόστους και επιρρεπείς σε επιθέσεις πλευρικών κλειδιών διαδικασίες αποθήκευσης κρυπτογραφικών κλειδιών σε συσκευές IoTκαι σταθμούς βάσης . Αντί για αυτό , επιτρέπει την κατά παραγγελία αναπαραγωγή κρυπτογραφικών κλειδιών .

Βιβλιογραφία

[1] Charidimos Chaintoutis1, 2. (2018). Optical PUFs as physical root of trust for. *IET*, p. 5.

[2] Charis Mesaritakis, D. D. (2022, November 15). Photonic Physical Unclonable Function Based. *JOURNAL OF LIGHTWAVE TECHNOLOGY*.

[3] Charis Mesaritakis, M. A. (2018, June 25). Physical Unclonable Function based. *Scientific Reports*, p. 12.

[4] Fabio Pavanello, I. O. (2021, September 7). Recent Advances in Photonic Physical Unclonable. *HAL open science*.

[5] Fahem Zerrouki, S. O. (2022, August 17). A Survey on Silicon PUFs. *Journal of Systems Architecture*, p. 21.

[6] Maes, R. (2013). *Physically Unclonable Functions Constructions , Properties and Applications.* Springer.

[7] Maes, R. (n.d.). *Towards Hardware-Intrinsic Security.*

[8] MESARITAKIS, C. (2020, February). Photonic Pseudo-Random Number Generator. p. 14.

[9] Ouchani, S. (2022, April). A survey on Silicon PUFs. *Journal of Systems Architecture*.

[10] P.Eder. (2023, February 12). Synthesis of a Semiconducting 2D Material for Novel Strong PUFs.

[11] Pappu, R. (2001). *Physical One-Way Functions. PhD Thesis.* Massachusetts Institute of Technology.

[12] Pappu, R. S. (2002, September 20). Physical one-way functions.

[13] Professor Helena Silva, P. A. (2019, March). Exploiting Phase Change Memory Nano-device Properties for Hardware Security Applications.

[14] Ulrich Rührmair, C. H. (2013). Optical PUFs Reloaded.