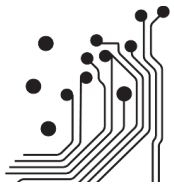


ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ. Ε.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Φυσικές μη κλωνοποιήσιμες συναρτήσεις για τον επακριβή προσδιορισμό συσκευών ασφαλείας

Αδαμοπούλου Αμαλία

Επιβλέπων καθηγητής: Παρασκευάς Κίτσος (Διδάκτωρ Ηλεκτρολόγος Μηχανικός και Τεχνολογίας Υπολογιστών)

ΠΑΤΡΑ
ΣΕΠΤΕΜΒΡΗΣ 2018

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Φυσικές μη κλωνοποιήσιμες συναρτήσεις για τον επακριβή προσδιορισμό συσκευών ασφαλείας

Αδαμοπούλου Αμαλία
Α.Μ. : 1314

Επιβλέπων καθηγητής: Παρασκευάς Κίτσος (Διδάκτωρ Ηλεκτρολόγος Μηχανικός και Τεχνολογίας Υπολογιστών)

ΠΕΡΙΛΗΨΗ

Τα PUFs (Physical Unclonable Functions), (στα ελληνικά:φυσικές μη κλωνοποιημένες συναρτήσεις), είναι ένας νέος και αναπτυσσόμενος κλάδος, όπου υλοποιείται στο υλικό των υπολογιστών, και έχει ως στόχο την αύξηση της σθεναρότητας σε συσκευές ασφαλείας.

Επίσης, είναι καλό να επισημάνουμε, πως η ανάπτυξη των ολοκληρωμένων κυκλωμάτων μας έχει δώσει την δυνατότητα να τα υλοποιούμε σε FPGA (Field Programmable Gate Arrays),CPLD(Complex Programmable Logic Devices) και σε ASIC(Application Specific Integrated Circuits), τα οποία είναι προγραμματιζόμενα ψηφιακά κυκλώματα, όπου αποτελούνται από πίνακες λογικών στοιχείων, τα οποία και αυτά με την σειρά τους συνδέονται μεταξύ τους με έναν προκαθορισμένο τρόπο. Έτσι θα μπορούσαμε να πούμε πως δημιουργούνται πολλοί ψηφιακοί σχεδιασμοί, οι οποίοι στοχεύουν σε οποιαδήποτε μέρη του hardware(υλικού).

Στην συγκεκριμένη εργασία θα αναλύσσουμε την χρησιμότητα των PUF's, το πως λειτουργεί καθένα από αυτά, πως λειτουργούν και που, και θα γίνει και μια σύγκριση των δύο για να έχουμε μια ορθή εικόνα των αποτελεσμάτων τους. Ύστερα γίνεται και μια ανάλυση αυτών σε κώδικα, για να αναλυθεί και η πολυπλοκότητα τους.

Έχει χρησιμοποιηθεί η γλώσσα VHDL(Very High Speed Integrated Circuits = ολοκληρωμένα κυκλώματα πολύ υψηλής ταχύτητας), η οποία είναι μια γλώσσα περιγραφής υλικού και με απλά λόγια περιγράφει την συμπεριφορά ενός ηλεκτρονικού κυκλώματος ή συστήματος, με βάση την οποία το σύστημα ή το κύκλωμα μπορεί να υλοποιηθεί.

Σκοπός της παρούσας πτυχιακής είναι η αναλυτική παρουσίαση της μεθόδου των φυσικών μη κλωνοποιημένων συναρτήσεων και του κλάδου τους. Οι φυσικές μη κλωνοποιημένες συναρτήσεις έρχονται να εξασφαλήσουν την ασφάλεια ορισμένων συσκευών, που συνεπάγεται με την ασφάλεια προσωπικών και απόρρητων δεδομένων. Πρόκειται για μια επιστήμη που βασίζεται στα μαθηματικά, σε αλγόριθμους κρυπτογράφησης και κωδικοποίηση και αποκωδικοποίηση των δεδομένων.

Στόχος είναι η εξήγηση, ανάπτυξη και ανάλυση δύο ήδη υπάρχων κρυπτογραφικών συστημάτων με βάση τις φυσικές μη κλωνοποιημένες συναρτήσεις, οι οποίες ζητούνται να ανταποκριθούν στις προσδοκίες ενός σωστά δομημένου και ασφαλούς σχεδιασμού. Επίσης, σημαντικό γνώρισμα ειναι η ασφάλεια που θέλουμε να παρέχεται μέσω των PUFs είναι πως ότι, σε κάθε γύρο χρησιμοποιείται ένα διαφορετικό κλειδί το οποίο παράγεται εκείνη τη στιγμή και δεν είναι αποθηκευμένο σε ένα σημείο, στο οποίο θα μπορούσε κάποιος να επέμβει, και έτσι κάνει το σύστημά μας εξαιρετικά δυνατό και ανθεκτικό απέναντι σε επιθέσεις όπως είναι η διαφορική κρυπτανάλυση.

Αυτό είναι και το κλειδί που κάνει τις συγκεκριμένες συναρτήσεις να ξεχωρίζουν.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ : Ασφάλεια υλικού (hardware)
ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ : puf, συνάρτηση, ολοκληρωμένα κυκλώματα, στιγμιότυπα

ABSTRACT

PUF' s is a new and growing industry where it is implemented in computer hardware and is aimed at increasing the vigor of security devices.

It is also good to note that the development of integrated circuits has enabled the implementation of Field Programmable Gate Arrays (FPGAs), Complex Programmable Logic Devices (CPLDs) and ASICs (Application Specific Integrated Circuits), which are programmable digital circuits, consisting of logic arrays, which in turn are connected in a predetermined manner. On that way, we could say how many digital designs are being created that target any piece of hardware.

In this paper we will analyze the usefulness of PUF's, how each of them works, how they work and how, and a comparison of the two of them, so we can make a good impression of their results. Then, an analysis of these in code is made to analyze their complexity.

VHDL (Very High Speed Integrated Circuits) has been used, which is a hardware description language, and simply describes the behavior of an electronic circuit or system on which the system or circuit can be used implemented.

The purpose of this diploma is to analyze the method of natural non-cloned functions and their branch. Physical non-cloned functions come to ensure the security of certain devices, which involves the security of personal and confidential data. It is a science based on mathematics, encryption algorithms, and encoding and decoding of data.

The aim is to explain, develop and analyze two existing cryptographic systems based on natural non-cloned functions, which are required to meet the expectations of a properly structured and secure design. Also, an important feature is the security we want to provide through PUFs is that each round uses a different key that is produced at that time and is not stored at a point where anyone could intervene, and so does our system is extremely powerful and resilient to attacks such as differential cryptanalysis.

SUBJECT AREA: Security Hardware
KEYWORDS: puf, function, integrated circuits, proposal

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1

ΠΡΟΛΟΓΟΣ

Το ανθρώπινο είδος προσπαθεί μέσα στα χρόνια όλο και περισσότερο να διασφαλίσει την ασφαλή επικοινωνία του σε οποιδήποτε μέσο χρησιμοποιεί και του επιτρέπει να μεταφέρει πληροφορίες είτε προσωπικές είτε δημόσιες. Η ανάγκη αυτή τους οδήγησε στην εύρεση τρόπων να μεταφέρουν με ασφάλεια πληροφορίες και μηνύματα, αποτρέποντας την παραποίηση ή υποκλοπή τους.

Σκοπός της εργασίας αυτής είναι η ανάλυση τεχνικών ασφαλείας στα PUF (Physical Unclonable Functions) συστήματα. Τα PUF συστήματα από το μόνο που μπορούμε να πούμε ότι αποτελούνται είναι από μια είσοδο, πολλές εξόδους και το αντίστοιχο ζευγάρι τους. Ένα PUF πρακτικά είναι μια συνάρτηση η οποία ορίζεται σε ένα φυσικό σύστημα και ουσιαστικά στην συνέχεια το ίδιο το φυσικό το σύστημα ορίζει τις εξόδους της. Υπάρχουν πολλά είδη PUF, και συνεχίσουν να αναπτύσσονται και να αναπαράγονται. Υπάρχουν ακόμα ιδέες που δεν έχουν ακόμα υλοποιηθεί καν, υπάρχουν απλά σαν εικασίες.

Πιο απλά, για να κατανοήσουμε πως λειτουργεί ένα PUF, σε ένα σύστημα το τελευταίο στάδιο της επικοινωνίας είναι η επιβεβαίωση της λήψης του. Αυτή η λήψη είναι ένα αρχείο οποιουδήποτε τύπου (εξαρτάται το σύστημα). Σε πολλές εφαρμογές λοιπόν αυτά τα αρχεία έρχονται σε επαφή με ανθρώπους που έχουν την δυνατότητα να τα μελετήσουν, να μελετήσουν την λειτουργία του συστήματος, με σκοπό να βρουν έναν τρόπο να να δημιουργήσουν έναν κλώνο του πιστοποιημένου αυτού πλέον αρχείου. Πράγμα το οποίο είναι κάτι που δεν το θέλουμε διότι το σύστημα θα το αντιμετωπίσει και αυτό το αρχείο ως έγκυρο (ενώ είναι ο κλώνος του), όπως το πρωτότυπο του. Με αυτό τον τρόπο αναιρείται όποιο πρωτόκολλο πιστοποίησης μπορούμε να σκεφτούμε.
Η λύση λοιπόν στο πρόβλημα αυτό είναι τα PUF's ή Physical Unclonable Functions.

Η εργασία αυτή έχει οργανωθεί σε κεφάλαια.

Στο πρώτο κεφάλαιο αναλύονται με απλά λόγια οι λόγοι που υπάρχουν και έχουν αναπτυχθεί τα PUF και γίνεται μια περίληψη εκ αυτών.

Στο δεύτερο κεφάλαιο αναλύονται οι όροι ενός PUF, τι είναι ένα PUF ο τρόπος που λειτουργεί, τα μέρη του. Επίσης αναλύονται όλα τα είδη του που μέχρι τώρα έχουν είτε αναφερθεί, είτε αναλυθεί από επιστήμονες ή ομάδες πανεπιστημίων.

Στο τρίτο κεφάλαιο γίνεται η ανάλυση των συστήματα που υλοποιούν τα PUF's, και τον σχεδιασμό των PUF's μέσα σε αυτά.

Στο τέταρτο κεφάλαιο αναλύονται οι βασικές αρχές της ασφάλειας ενός υπολογιστικού συστήματος, οι βασικές της κρυπτογραφίας δημόσιου και ιδιωτικού κλειδιού. Και στο τέλος του γίνεται μια σύγκριση των PUF με τα γενικότερα και πιο κοινά συστήματα ασφαλείας.

ΚΕΦΑΛΑΙΟ 2

PUFs-(Physical Unclonable Functions)

Για την ευκολότερη κατανόηση των φυσικών μη κλωνοποιήσιμων συναρτήσεων θα εξηγήσουμε πρώτα τι είναι μια συνάρτηση στον κόσμο των υπολογιστών.

Συνάρτηση:
Ο όρος συνάρτηση λοιπόν, όπου είναι επίσης γνωστός και ως διαδικασία ή υποπρόγραμμα, είναι μια σειρά εντολών που αποτελούν ένα υποπρόγραμμα, με σκοπό την υλοποίηση ενός ευρύτερου προγράμματος/αλγόριθμου σε γλώσσα μηχανής.
Η λειτουργία των συναρτήσεων γίνεται ως εξής : το εκτελούμενο πρόγραμμα φτάνει σε μια εντολή, η οποία ονομάζεται εντολή διακλάδωσης, και στην συνέχεια καλεί το υποπρόγραμμα/ συνάρτηση.
Αξίζει να σημειώσουμε πως οι συναρτήσεις αφορούν διαδικασίες στις οποίες οι εντολές διακλάδωσης στο τέλος του τρέχωντος υποπρογράμματος επιστρέφουν μια μεταβλητή ή μια δομή δεδομένων, για την χρήση τους στην συνέχεια του αρχικού προγράμματος/αλγόριθμου.

Φυσικές μη κλωνοποιήσιμες συναρτήσεις-PUFs:
Μια φυσική τυχαία συνάρτηση ή μια φυσική μη κλωνοποιήσιμη συνάρτηση (**PUF:physical unclonable function**) σαν μια γενική άποψη, είναι μια συνάρτηση/ακολουθία η οποία καθορίζει ένα σύνολο από εισόδους σε ένα σύνολο από εξόδους, βασισμένες σε ένα ατίθασο σύνθετο φυσικό σύστημα.
Πιο συγκεκριμένα ένα PUF (ή μια φυσική μη κλωνοποιήσιμη συνάστηση) δεν είναι από μαθηματικής μεριάς μια 'πραγματική ακολουθία', διότι μια είσοδος σε ένα puf μπορεί να παράγει πολλές εξόδους. Είναι καλύτερα να θεωρηθεί πως ένα puf είναι από **μηχανικής** μεριάς 'πραγματική ακολουθία', διότι είναι μια διαδικασία που <εκτελείται> ή <εκτελεί και ενεργεί>, κατά έναν συγκεκριμένο σύστημα.

Έτσι έχουμε ως αποτέλεσμα, η συνάρτηση (το PUF δηλαδή) να μπορεί να αξιολογηθεί μόνο με το φυσικό σύστημα, και να είναι μοναδικό για κάθε φυσική περίπτωση. Από την έρευνα που έχει υπάρξει η αξιολόγηση των PUF είναι εύκολη, αλλά η πρόβλεψη του δύσκολη, εώς πολύ δύσκολη.

Ένα PUF για να φτιαχτεί πρέπει να του δωθεί ένας χειρισμός, ένας τρόπος που θα δουλεύει(θα προσπαθήσουμε να βρούμε έναν).Δηλαδή, όταν λέμε ότι το PUF αναζητά έναν λειτουργικό χειρισμό, εννοούμε ότι όταν ζητείται να μαθευτεί μια συγκεκριμένη είσοδος ο χειρισμός παράγει μια καταμετρημένη έξοδο.

- Μια είσοδος (**input**) στον κόσμο των PUF ονομάζεται πρόκληση (**challenge**),

και μια έξοδος (**output**) ονομάζεται απάντηση (**response**).

- Μια εφαρμοσμένη είσοδος με την καταμετρημένη έξοδο της, αποκαλείται ζευγάρι εισόδου- εξόδου και αποτελεί την συμπεριφορά (**CRP**) του PUF. Καλύτερα θα λέγαμε πως η σχέση που έχει τεθεί ως ενεργή ανάμεσα στις εισόδους και τις εξόδους ενός συγκεκριμένου PUF ονομάζεται συμπεριφορά, (**CRP=Challenge Response Pair**).
- **Inter-distance** (μεταξύ-απόσταση), είναι η σημασία της απόστασης μεταξύ δύο PUF στιγμιοτύπων για μια συνηθισμένη είσοδο είναι η απόσταση μεταξύ δύο εξόδων τους, οι οποίες έχουν βγει εφαρμόζοντας την είσοδο από μια φορά και στα δύο PUF.

  ➔ Εκφράζει την μοναδικότητα.
- **Intra-distance** (ενδο-απόσταση), είναι η σημασία της απόστασης μεταξύ δύο εκτιμήσεων σε ένα στιγμιότυπο ενός μόνο PUF για μια συνηθισμένη είσοδο, είναι η απόσταση ανάμεσα σε δύο εξόδους, οι οποίες έχουν βγει εφαρμόζοντας την είσοδο δύο φορές σε ένα PUF.

  ➔ Η ίδια είσοδος που έχει απαντηθεί στο ίδιο PUF, δεν παράγει απαραίτητα την ίδια έξοδο, δίνοντας 'δύναμη' στην intra-distance μεταξύ των εξόδων του PUF.

  ➔ Εκφράζει τον μέσο θόρυβο τον απαντήσεων – εξόδων

  ➔ Αντικατοπτρίζει την αναπαραγωγισημότητα.
- **μ-inter**: Δείχνει το ποσοστό μοναδικότητας του PUF που έχει δημιουργηθεί, δηλαδή μετράει τον μέσο επιφανειακό όγκο δύο συστημάτων βασισμένων στις απαντήσεις-εξόδους των PUF.

  ➔ Όσο πιο μεγάλη είναι η τιμή του τόσο το καλύτερο.
- **μ-intra**: Δείχνει το ποσοστό μέσου θορύβου στις εξόδους του PUF, δηλαδή μετράει την μέση επαναληψιμότητα μιας συγκεκριμένης σε όγκο εξόδου. Θέλουμε να είναι όσο πιο μικρή γίνεται, εφόσον αποδίδει πολύ αληθοφανείς εξόδους των PUF.

  ➔ Ιδανική τιμή μ-intra = 0.

<u>Εν κατακλείδι, η πιο γενική έννοια που υπάρχει για τον ορισμό ενός PUF είναι:</u>

είναι μια φυσική οντότητα που είναι ενσαρκωμένη σε μια φυσική δομή που είναι εύκολη να αξιολογιθεί (/μετρηθεί-για την καλύτερη κατανόηση της έννοιας) αλλά δύσκολο να προβλεφθεί (υπάρχει μεγάλη τυχαιότητα στις εξόδους-απαντήσεις).

Μια ανεξάρτητη puf συσκευή πρέπει να είναι εύκολη για να υλοποιηθεί αλλά πρακτικά αδύνατη να υπάρξει διπλότυπο (κάποια pufs είναι κλωνοποίησημα όμως), ακόμα και αν κάποιος γνωρίζει την διαδικασία κατασκευής που αναπαράχθηκε. Από αυτή την οπτική γωνία είναι το ανάλογικό λογισμικό μιας συνάρτησης ενός-δρόμου(one-way function).

Σήμερα τα PUFs είναι συνήθως εφαρμοσμένα σε ενσωματωμένα συστήματα και σε εφαρμογές με ανάγκες για υψηλού επιπέδου ασφάλεια.

2.1 ΤΑ ΕΙΔΗ ΤΩΝ PUFS

Ψάχνοντας γενικότερα για τις φυσικές μη κλωνοποιήσιμες συναρτήσεις δυστηχώς δεν θα βρούμε πολλά λήμματα τα οποία μπορούν να καθορίσουν ακριβώς το πόσα ήδη μπορεί να υπάρξουν. Σύμφωνα λοιπόν με τα paper που έχω βρει και είναι διαθέσιμα θα προσπαθήσω να είμαι όσο πιο αντικειμενική γίνεται για αυτά (αν και κάποιες από τις προτάσεις που υπάρχουν δεν είναι και ιδιαίτερα κατατοπιστηκές). Οι κατηγορίες των PUF μέχρι στιγμής είναι χωρισμένες ως προς την κατασκευή τους και ως προς τον τρόπο λειτουργίας τους.

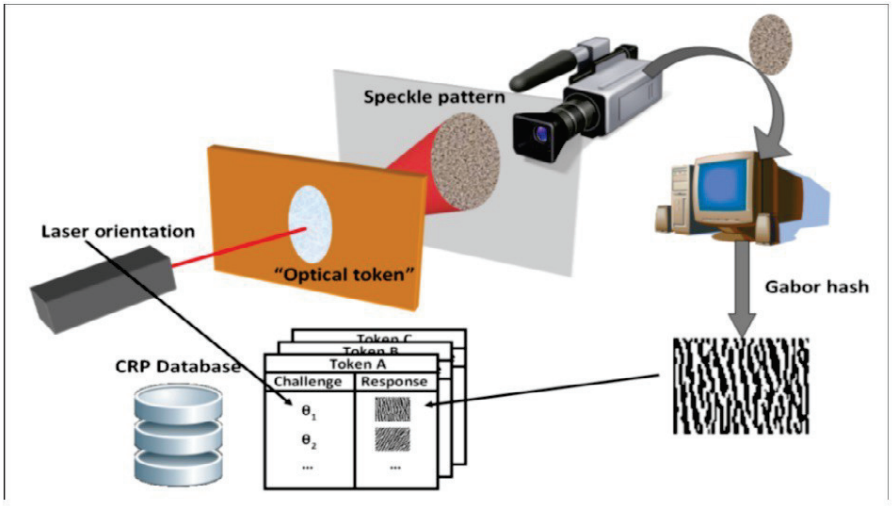
2.1.1 ΜΗ – ΗΛΕΚΤΡΟΝΙΚΑ PUFS (NON – ELECTRONIC PUFS)

Μη ηλεκτρονικά PUFs ονομάζουμε τα PUFs των οποίων η κατασκευή των ιδιοτήτων τους είναι εσωτερικά και φυσικά μη ηλεκτρονική. Αξίζει να σημειωθεί φυσικά, πως σε κάποιο σημείο θα χρησιμοποιηθεί κάποια ηλεκτρονική τεχνική για την επεξεργασία και την αποθήκευση των εξόδων των PUF με έναν αποτελεσματικό τρόπο. Το συμπέρασμα λοιπόν εδώ είναι, πως φαίνεται η μοναδικότητα των PUF λόγο των φυσικών ιδιοτήτων τους και της τυχαίας δομής τους.

2.1.1.1 ΟΠΤΙΚΑ PUFS (OPTICAL PUFS)

Μια πρώιμη έκδοση ενός μη κλωνοποιήσιμου συστήματος εξακρίβωσης βασισμένο σε τυχαία μοτίβα οπτικών αντανακλάσεων, της λεγόμενης Ετικέτας Αντανάκλασης Μορίων, προτάθηκες πολύ πριν την εισαγωγή των PUF. Είχαν χρησιμοποιηθεί για την εξακρίβωση των στρατηγικών όπλων για τον έλεγχο των εξοπλισμών συνθηκών.
Τα οπτικά PUF βασίζονται σε διαφανή μέσα όπως οι φυσικές
συναρτήσεις μιας κατεύθυνσης (POWF). Το βασικό στοιχείο του σχεδιασμού τους είναι ένα οπτικό token που περιέχει μια μικροδομή κατασκευασμένη από ανάμειξη μικροσκοπικών (500μm) σφαιρών διάθλασης γυαλιού σε μια μικρή (10×10×2.54mm) διαφανής εποξείδια πλάκα. Το token είναι εκπεμπόμεναο από ήλιον και νέον λέιζερ και η μέτρηση κυμάτων γίνεται ακανόνιστη όταν υπάρχουν πολλαπλές σκεδάσεις της δέσμης μαζί με σωματίδια διάθλασης.
Το μοτίβο στιγμάτων που προκύπτει είναι από μια CCD κάμερα για ψηφιακή επεξεργασία. Ως χαρακτηριστικό διαδικασίας εκχύλισης, λέμε ότι είναι, ο κατακερματισμός των στιγμάτων που υπάρχουν σε ένα μοτίβο. Το αποτέλεσμα είναι μια συμβολοσειρά από bits που εκπροσωπούν την κατακερματισμένη τιμή. Είναι σαφές και ήταν πειραματικά επαληθευμένο ακόμα και μετά από αλλαγές του λεπτού στο σχετικό προσανατολισμό της δέσμης του λέιζερ και του αποτελέσματος σε ένα τελείως διαφορετικό μοτίβο εξαγώμενων κατακερματισμών.
Η πραγματική PUF λειτουργικότητα είναι συμπληρωμένη από μία πρόκληση-είσοδο, την οποία περιγράφει ο ακριβής προσανατολισμός του laser και τα αποτελέσματα του κατακερματισμού τα οποία απορρέουν ένα μοτίβο στιγμάτων ως απάντηση.

Είναι προφανές ότι η χρήση του οπτικού PUF όπως περιγράφεται παραπάνω είναι μάλλον επίπονη, λόγω του μεγάλου setup που συνεπάγονται σε μια δέσμη λέιζερ και ένα ανιαρό μηχανικό σύστημα τοποθέτησης.



Εδώ φαίνεται η βασική δομή ενός οπτικού PUF.

2.1.1.2 PUF – ΧΑΡΤΙ (PAPER PUF)

Αυτό που αποκαλέιται PUF χαρτί στην πραγματικότητα είναι ένας αριθμός προτάσεων που φτιάχθηκαν σε επίπεδο βιβλιοθήκης που ουσιαστικά αποτελούνται από την σάρωση των μοναδικών και τυχαίων δομών των ινών ενός συνηθισμένου ή τροποποιημένου χαρτιού. Το PUF χαρτί είναι άμεσα συνδεδεμένο με το οπτικό PUF. Η αντανάκλαση μιας εστιασμένης δέσμης λέιζερ από μια ακανόνιστη δομή ίνας ενός εγγράφου χρησιμοποιείται σαν δακτυλικό αποτύπωμα του εγγράφου για να αποτραπεί η πλαστογράφηση του.
Επίσης έχει προταθεί μια μέθοδος η οποία διασυνδέει τα δεδομένα σχετικά με το εν λόγω έγγραφο με το χαρτί, χρησιμοποιώντας ένα συνδυασμό ψηφιακής υπογραφής των δεδομένων και του αποτυπώματος του χαρτιού, το οποίο είναι τυπωμένο στο έγγραφο.

2.1.1.3 CD PUFS

Σε ένα απλό CD παρατηρήθηκε πως το μήκος και τα κυλόματα που έχει, περιέχουν μια τυχαία απόκλιση από τα προβλεπόμενα μήκη λόγω πιθανών διακυμάνσεων κατά την διαδιακασία παρασκευής. Επιπλέον,αυτή η απόκλιση είναι αρκετά μεγάλη για να παρατηρηθεί από την παρακολούθηση του ηλεκτρικού σήματος από το φωτοανιχνευτή σε ένα κανονικό CD player. Αυτό δοκιμάστηκε για ένα μεγάλο αριθμό CD και θέσεων για το κάθε CD.

2.1.1.4 RF - DNA

Το RF-DNA (radio frequency) ονομάζεται ραδιοσυχνότητα. Είναι η κατασκευή ενός μικρού (25×50×3mm) φθηνού διακριτικού token παρόμοια με αυτή που χρησιμοποιείται στο οπτικό PUF, μόνο που εδώ υπάρχουν λεπτά καλώδια χαλκού με τυχαίο τρόπο σε ελαστικό στεγανοποιητικό πυρίτιο. Αντί της παρατήρησης της διάχυσης του φωτός, όπως γίνεται στα οπτικά PUFs παρατηρείται ο κοντινός τομέας σκέδασης ηλεκτρομαγνητικών κυμάτων από τα καλώδια χαλκού σε άλλα μήκη κύματος, ιδίως στα 5-6 GHz.
Η τυχαία διασπορά των αποτελεσμάτων μετριέται από ένα πρωτότυπο σκάνερ που αποτελείται από ένα δίκτυο κεραιών RF. Η εντροπία του περιεχομένου ενός μοναδικού token εκτιμάται ότι είναι τουλάχιστον 5000 bit.

2.1.1.5 ΜΑΓΝΗΤΙΚΑ PUFS (MAGNETIC PUFS)

Τα μαγνητικά PUF χρησιμοποιούν την εγγενή μοναδικότητα των ρευμάτων των σωματιδίων σε μαγνητικά μέσα, π.χ. Μαγνητική σάρωση καρτών. Χρησιμοποιούνται σε εμπορική εφαρμογή για την αποφυγή απάτης με πιστωτική κάρτα.
Δεν δίνονται περαιτέρω δημοσιμοποιημένες λεπτομέρειες.

2.1.1.6 ΑΚΟΥΣΤΙΚΑ PUFS (ACOUSTICAL PUFS)

Η ακουστική καθυστέρηση των γραμμών είναι τα συστατικά που
χρησιμοποιούνται για την καθυστέρηση των ηλεκτρικών σημάτων. Μετατρέπουν το εναλλασόμενο ηλεκτρικό σήμα σε μηχανικούς κραδασμούς και το αντίστροφο. Είναι φτιαγμένα από την παρατήρηση του φάσματος συχνοτήτων μιας γραμμής ακουστικής καθυστέρησης. Μια ακολουθία από bit εκχυλίζεται εκτελώντας ένα μέρος την ανάλυσης, και υπολογίζεται ότι μπορεί να υπάρξουν τουλάχιστον 160 bits εντροπίας. Μια τέτοια κατασκευή μπορεί να αποτελέσει την εξακρίβωση της, με ψευδή ποσοστό απόρριψης των 10-4 και ψευδή ποσοστό αποδοχής σε πιο 10^5.

2.1.2 ΑΝΑΛΟΓΙΚΑ ΗΛΕΚΤΡΟΝΙΚΑ PUFS (ANALOG ELECTRONIC PUFS)

Τα αναλογικά και ηλεκτρονικά PUFs, είναι εκείνα τα οποία αποτελούνται από μια αναλογική μέτρηση μιας ηλεκτρικής ή ηλεκτρονικής ποσότητας. Εδώ δεν υπάρχει η ανάγκη οι μετρήσεις να γίνουν με ξεπερασμένο τρόπο όπως στα μη ηλεκτρονικά PUFs, εδώ υπάρχει η ψηφιακή μέτρηση.

2.1.2.1 VT PUFs

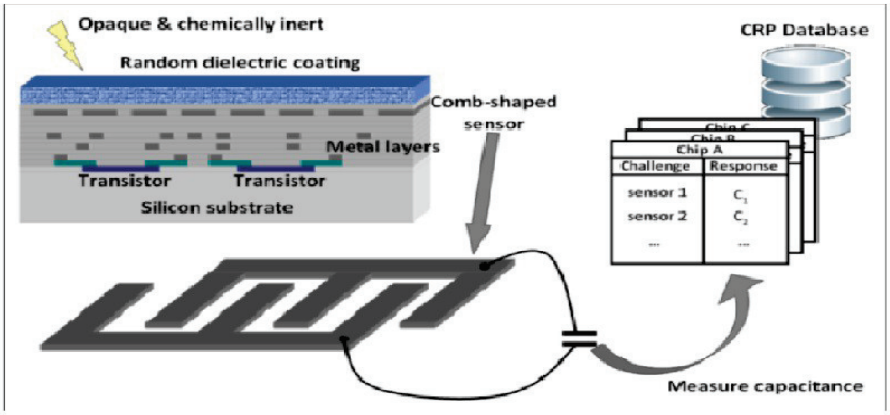
Η τεχνική εκχώρησης μιας μοναδικής εξακρίβωσης σε κάθε μενονωμένη περίπτωση από μια τακτική ολοκληρωμένου κυκλώματος, χωρίς την ανάγκη ειδικών βημάτων επεξεργασίας ή του προγραμματισμού μετά την παραγωγή, ονομάζεται ICID. Η λειτουργία είναι η εξής: ένας αριθμός από ίδια σχεδιασμένα τρανζίστορ, είναι καθορισμένα σε διευθυνσιοδοτημένες περιοχές.
Το διευθυνσιοδοτημένο τρανζίστορ απευθύνεται σε αντιστεκόμενο φορτίο και επειδή το αποτέλεσμα των κατασκευαστικών αποκλίσεων είναι στα όρια της τάσης (VT) αυτών των τρανζίστορ, το ρεύμα μέσα από αυτό το φορτίο θα είναι εν μέρει τυχαίο. Η τάση πάνω από το φορτίο είναι μετρημένη και μετατρέπεται σε μια ακολουθία από bit με έναν συγκριτή αυτόματου μηδενισμού.

2.1.2.2 ΔΥΝΑΜΙΚΑ ΚΑΤΑΝΕΜΜΗΜΕΝΑ PUFS (POWER DISTRIBUTION PUFS)

Αυτό το PUF είναι βασισμένο στην αντίσταση των διακυμάνσεων ισχύος της δύναμης του πλέγματος ενός chip. Οι πτώσεις της τάσης και οι ισοδύναμες αντιστάσεις στο σύστημα διανομής ρεύματος, μετρώνται χρησιμοποιώντας εξωτερικά μέσα και έχει παρατηρηθεί πως αυτές οι ηλεκτρικοί παράμετροι επηρεάζονται από τυχαίες κατασκευαστικές διαφορές.

2.1.2.3 PUFS ΣΕ ΣΤΡΩΜΑΤΑ (COATING PUFS)

Στα PUFs σε στρώματα έχουμε το ενδεχόμενο της τυχαιότητας των μετρήσεων χωριτηκότητας στους αισθητήρες του πιο πάνω στρώματος ενός ολοκληρωμένου κυκλώματος. Αντί να βασίζονται αποκλειστικά στα τυχαία γεγονότα των κατασκευαστικών διαφορών, τα τυχαία στοιχεία παρουσιάζονται από μια παθητική διηλεκτρική επίστρωση που ψεκάζεται απευθείας στην κορυφή των αισθητήρων. Επιπλέον, δεδομένου ότι η επικάλυψη είναι ματ και χημικά αδρανές, προσφέρει δυνατή προστασία από φυσικές επιθέσεις. Μια πειραματική αξιολόγηση της ασφαλείας, αποκαλείπτει πως τα PUFs με στρώματα είναι προφανής αλλοιώσεις, δηλ., μετά από μια επίθεση με FIB οι έξοδοι των PUF είναι αξιοσημείωτα αλλαγμένοι. Σε μια πιο θεωρητική αξιολόγηση του συγκεκριμένου είδους παρατηρήθηκες ότι το μέγεθος της εντροπίας είναι 6.6 bit ανά αισθητήρα.



Εδώ φαίνεται η βασική δομή ενός PUF σε στρώματα.

2.1.2.4 LC PUFS

Ένα LC PUF είναι κατασκευασμένο σαν μια μικρή γυάλινη πλάκα (≈1mm^2) με μια μεταλλική πλάκα σε κάθε πλευρά, σχηματίζοντας έτσι έναν πυκνωτή, σειριακά δεμένο με ένα μεταλλικό πηνίο στην πλάκα, το οποίο ενεργεί ως επαγωγικό εξάρτημα. Μαζί σχηματίζουν ένα παθητικό LC κύκλωμα το οποίο θα απορροφήσει ένα ποσό ενέργειας όταν τοποθετηθεί σε ένα RF πεδίο. Η συχνότητα σάρωσης αποκαλύπτει τις συχνότητες συντονισμού του κυκλώματος, το οποίο εξαρτάται από τις ακριβείς τιμές της χωρητικότητας και της επαγωγής του εξαρτήματος. Λόγω των κατασκευαστικών διακυμάνσεων, η απεικόνιση της κορυφής θα είναι ελαφρώς διαφορετική για τα ίδια κατασκευασμένα κυκλώματα. Αντίθετα από το RF DNA, η κατασκευή του LC PUF είναι εσωτερικά ένα παθητικό ηλεκτρικό κύκλωμα και όχι μια τυχαία διάταξη των χάλκινων καλωδίων. Από πειραματικά δεδομένα από 500 κυκλώματα φάνηκε η αναπαραγωγιμότητα της κορυφής στο 1MHz σε σταθερή θερμοκρασία και η εντροπία του περιεχομένου μεταξύ 9 και 11 bits ανά κύκλωμα.

2.2 ΕΝΔΟΓΕΝΗΣ/ΕΣΩΤΕΡΙΚΑ PUF (INSTRINSIC PUFS)

Τα ενδογενή ψηφιακά PUF, είναι εκείνα τα οποία είναι ενσωματωμένα σε ένα ολοκληρωμένο κύκλωμα (IC), και των οποίων οι βασικές δομικές μονάδες είναι συνηθισμένες και ξεπερασμένες για την επιλεγείσα κατασκευαστική τεχνολογία. Αυτό σημαίνει πως τα ενδογενή PUFs είναι εύκολο να κατασκευαστούν, επειδή δεν χρειάζονται ειδικά βήματα επεξεργασίας κατά την κατασκευή και επίσης δεν υπάρχει εξειδικευμένος ή εξωτερικός εξοπλισμός για την λειτουργία τους. Για αυτά τα PUFs, η ρύθμιση των μετρήσεων είναι συχνά ένα φυσικό τμήμα της κατασκευής των PUF και να είναι ενσωματωμένο σε ένα ολοκληρωμένο. Υπάρχουν δύο είδη φυσικών PUF, το ένα είναι με βάση την καθυστέρηση των μετρήσεων και το δεύτερο με βάση την διευθέτηση των στοιχείων της μνήμης.

Πιο συγκεκριμένα:
Όλα τα PUF ξεκινάνε από μια αναλογική μέτρηση τυχαίων φυσικών παραμέτρων, οι οποίοι αργότερα 'κβαντίζονται' και δεν μπορούν να χρησιμοποιηθούν ως 'αναγνωριστές' ολόκληρου του συστήματος. Ένα PUF για το ονομάσουμε ενδογενή χρειαζόμαστε δύο προυποθέσεις:

1. Τα PUF, συμπεριλαμβανομένου του εξοπλισμού μέτρησης, θα πρέπει να ενσωματωθούν πλήρως στη συσκευή.
Αυτό σημαίνει πως η συσκευή μπορεί να ρωτήσει και να διαβάσει το δικό της PUF, χωρίς την ανάγκη επιπλέον συσκεών ή διαδικασίων, όπως επίσης και χωρίς την ανάγκη οι είσοδοι και έξοδοι να 'αφήσουν' την συσκευή, να έχουν κάνει εξαγωγή. Συμπερασματικά θα μπορούσαμε να πούμε πως σε αυτή την περίπτωση η συσκευή λειτουργεί δυναμικά.

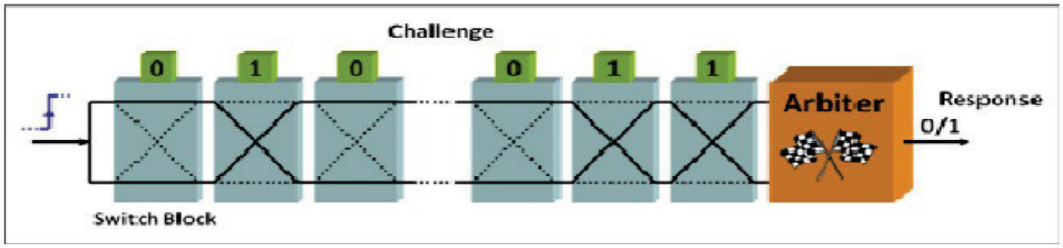
2. Η πλήρης κατασκευή των PUF θα πρέπει να αποτελείται από αρχέτυπα που είναι φυσικά διαθέσιμα για τη διαδικασία κατασκευής της συσκευής ενσωμάτωσης.
Η προυπόθεση αυτή σημαίνει ότι η πλήρης κατασκευή των PUF δεν έχει σχεδόν καμία επιβάρυνση, εκτός από τον χώρο που καταλαμβάνει το PUF, δηλ., δεν χρειάζονται επιπλέον κατασκευστικά στάδια ή στοιχεία.

Όπως παρατηρείται, λόγο του ότι εδώ δεν χρειάζονται επιπλέον στάδια, διαδικασίες κτλ., εδώ δεν ισχύουν τα PUF σε στρώματα ή τα οπτικά.
Το μεγάλο πλεονέκτημα ενός ενσωματωμένου PUF σε ένα ψηφιακό τσιπ είναι ότι οι έξοδοι του, μπορούν να χρησιμοποιηθούν άμεσα από άλλες εφαρμογές που τρέχουν στην ίδια συσκευή.

2.2.1 DELAY – BASED INSTRINSIC PUFS

2.2.1.1 PUF ΚΡΙΤΕΣ (ARBITER PUFS)

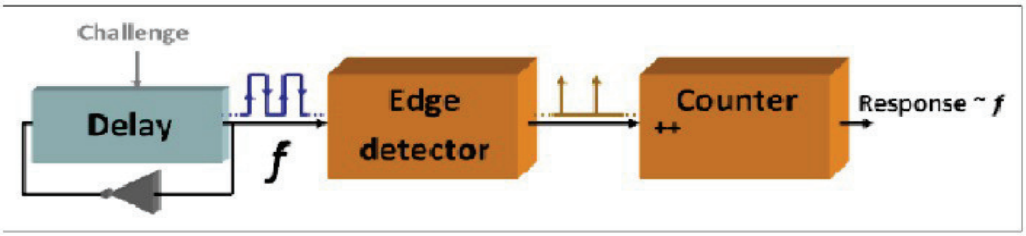
Η βασική ιδέα των PUF κριτών, είναι να εισαχθεί μια κατάσταση κούρσας σε δύο διαδρομές σε ένα τσιπ, και έτσι ο PUF κριτής να αποφασίσει ποιά από τις δύο διαδρομές θα κερδίσει. Εάν τα δύο αυτά μονοπάτια είναι συμμετρικά σχεδιασμένα, δηλ. με την ίδια καθυστέρηση προορισμού, τότε το αποτέλεσμα του αγώνα είναι αμετάβλητο εκ των προτέρων. Κατά την παραγωγή του τσιπ, οι κατασκευαστικές αποκλίσεις θα έχουν ως αποτέλεσμα να καθορίζουν την ακριβή καθυστέρηση κάθε διαδρομής για τις φυσικές παραμέτρους και να προκαλούν μια μικρή τυχαία αντιστάθμιση μεταξύ των δύο καθυστερήσεων. Αυτό οδηγεί σε μια τυχαία και, πιθανών βγαλμένη από την συσκευή, έκβαση του διαιτητή και επομένως εξηγεί την συμπεριφορά του PUF μιας τέτοιας συσκευής. Αν το σύνολο αντιστάθμισης είναι πολύ μικρό, ο χρόνος εγκατάστασης-αναμονής του κριτή θα παραβιαζόταν και η έξοδος του δεν θα εξαρτιόταν από την έκβαση αγώνα πια, αλλά από τον τυχαίο θόρυβο. Η από πάνω λειτουργία ονομάζεται metastability του διαιτητή και είσάγει θόρυβο στις εξόδους των PUF.
Ο αρχικός σχεδιασμός χρησιμοποιεί το μπλοκ εναλλαγής για την κατασκευή των δύο συμμετρικών μονοπατιών, και ένα μανταλωτή ή ένα flip-flop για την υλοποίηση του κυκλώματος κριτή. Τα μπλοκ εναλλαγής έχουν δύο εισόδους και δύο εξόδους και βασίζονται σε ένα παραμετροποιημένο bit, και είναι συνδεδεμένα είτε ευθεία είτε αντιστραμένα. Συνδέοντας έναν αριθμό από μπλοκ εναλλαγής σε σειρά δημιουργούμε δύο παραμετροποιημένες γραμμές καθυστέρησης οι οποίες τροφοδοτούνται από τον κριτή. Η ρύθμιση των μπλοκ εναλλαγής θα είναι η είσοδος του PUF και η έξοδος του κριτή θα είναι και έξοδος. Σημειώστε πως ο αριθμός των πιθανών εξόδων είναι ραγδαία αυξανόμενος στον αριθμό των μπλοκ εναλλαγής που μπορούν να χρησιμοποιηθούν.



Εδώ φαίνεται η βασική δομή ενός PUF κριτή.

2.2.1.2 ΔΑΧΤΥΛΙΔΙΑ ΤΑΛΑΝΤΩΤΕΣ PUFS (RING OSCILLATOR PUFS)

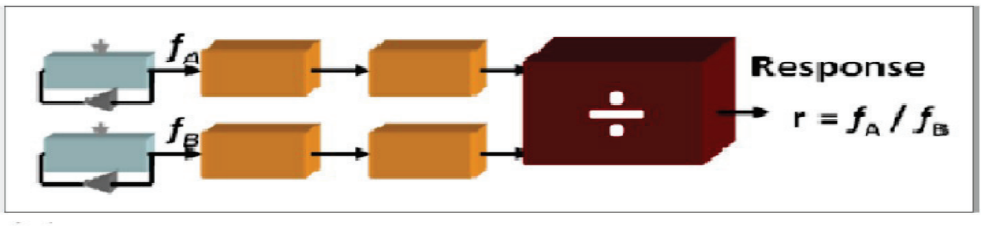
Τα PUF δαχτυλίδια ταλαντωτές μετρούν με διαφορετικό τρόπο τις τυχαίες αποκλίσεις των καθυστερήσεων που δημιουργούνται από κατασκευαστικές διαφορές. Η έξοδος μια ψηφιακής γραμμής καθυστέρησης αντιστρέφεται και τροφοδοτείται πίσω στην ίδια την είσοδο του, δημιουργώντας ένα ασύγχρονα ταλαντούμενο βρόχο, που ονομάζεται επίσης ταλαντωτής δακτυλίου. Είναι προφανές ότι η συχνότητα του ταλαντωτή αυτού προσδιορίζεται επακριβώς από την ακριβή καθυστέρηση της γραμμής καθυστέρησης. Η μέτρηση της συχνότητας είναι ισοδύναμη με τη μέτρηση της καθυστέρησης, και σύμφωνα με τυχαίες κατασκευαστικές διακυμάνσεις στην καθυστέρηση, η ακριβής συχνότητα θα είναι επίσης εν μέρει τυχαία και εξαρτώμενη από την συσκευή. Οι μετρήσεις την συχνότητας μπορεί να γίνουν σχετικά εύκολα χρησιμοποιώντας ψηφιακά εξαρτήματα : έναν ανιχνευτή ακμής όπου ανιχνεύει ανερχόμενες ακμές κατά την περιοδική ταλάντωση και έναν ψηφιακό μετρητή που μετράει τον αριθμό των ακμών κατά την διάρκεια μιας χρονικής περιόδου.
Η τιμή του μετρητή περιέχει όλες τις λεπτομέρειες του επιθυμητής μέτρου και θεωρείται η PUF απάντηση. Εάν η γραμμή καθυστέρησης μπορεί να παραμετροποιηθεί με βασικό σχεδιασμό PUF κριτή, η συγκεκριμένη ρύθμιση καθυστέρησης θεωρείται είσοδος/πρόκληση.



Εδώ φαίνεται η βασική δομή ενός PUF δακτυλίου ταλαντωτή.

Όπως είναι λογικό μερικές περιβαλλοντικές παράμετροι μπορούν να επηρεάσουν τις εξόδους των PUF. Στην περίπτωση των μετρήσεων καθυστέρησης σε ολοκληρωμένα κυκλώματα, η θερμοκρασία έκλειψης και η τάση τροφοδοσίας επηρεάζουν την ακριβή καθυστέρηση. Για τα PUF κριτές αυτό το αποτέλεσμα δεν ήταν τόσο μεγάλο εφόσον θα ασκούν εμμέσως μια διαφορετική μέτρηση, εξετάζοντα δύο παράλληλα

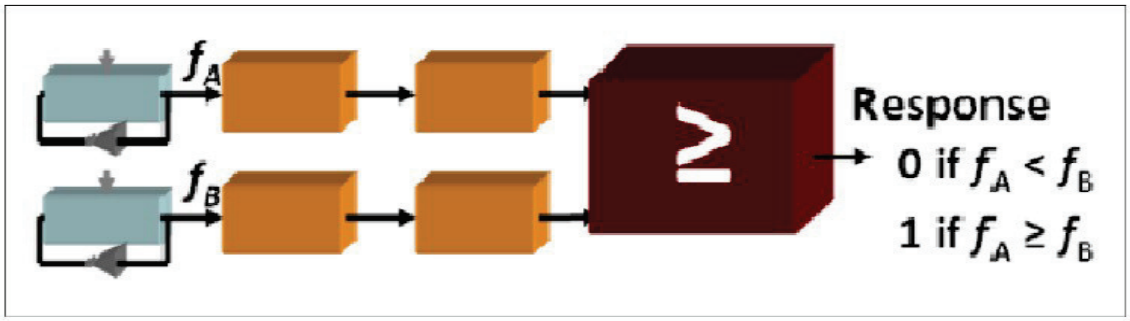
μονοπάτια καθυστέρησης ταυτόχρονα. Για το PUF δακτυλίδι ταλαντωτή, αυτά τα αποτελέσματα είναι πολύ μεγαλύτερα και κάποιο είδος αποζημίωσης είναι απαραίτητο. Η προτεινόμενη τεχνική αντιστάθμισης είναι να διαιρεθούν οι τιμές του μετρητή από δύο ταυτόχρονες ταλαντώσεις, το οποίο όλο αυτό οδηγεί σε πολύ



ισχυρές απαντήσεις/εξόδους.

PUF δακτυλίδι ταλαντωτής με διαίρεση αποζημίωσης.

Υπάρχει μια άλλη ιδέα δημιουργίας PUF δακτυλίων ταλαντωτών. Η βασική μέτρηση συχνότητας και η μέτρηση ανερχόμενων ακμών είναι το ίδιο, αλλά τώρα χρησιμοποιείται ένα πολύ απλό και σταθερό κύκλωμα καθυστέρησης. Ένας αριθμός από ταλαντωτές με την ίδια επιδιωκούμενη συχνότητα εφαρμόζονται παράλληλα. Η είσοδος/πρόκληση για το PUF επιλέγει ένα ζεύγος από ταλαντωτές και η έξοδος/απάντηση παράγεται συγκρίνοντας τις δύο υπάρχοντες τιμές του μετρητή. Αυτή είναι μια πολύ φτηνή και απλή προσέγγιση για τα συγκεκριμένα PUF.

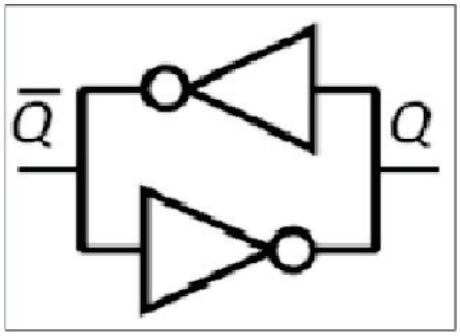


PUF δαχτυλίδι ταλαντωτής με σύγκριση διαίρεσης.

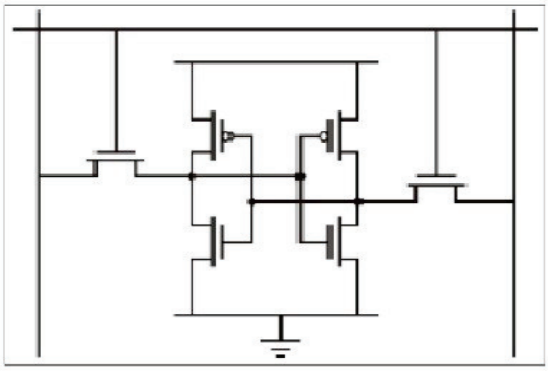
2.2.2 MEMORY-BASED INSTRINSIC PUFS

2.2.2.1 SRAM PUFS

SRAM (Static Random Access Memory) είναι η στατική μνήμη τυχαίας προσπέλασης και είναι ένας τύπος μνήμης που αποτελείται από κελιά όπου το καθένα είναι ικανό να αποθηκεύει έναν δυαδικό αριθμό. Ένα δυαδικό SRAM κελί είναι λογικά κατασκευασμένο με δύο διασταυρωμένα ζευγάρια μετατροπέων, που οδηγούν σε δύο σταθερές καταστάσεις. Στην κανονική τεχνολογία CMOS, αυτό το κύκλωμα υλοποιείται με 4 MOSFETs, και επιπλέον 2 MOSFETs χρησιμοποιούνται για την πρόσβαση ανάγνωσης / εγγραφής.



Logical circuit of an SRAM (PUF) cell.

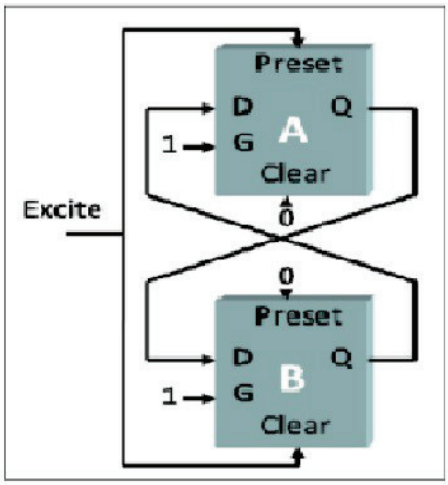


Electrical circuit of an SRAM (PUF) cell in standard CMOS technology.

Για λόγους απόδοσης, η φυσική αναντιστοιχία μεταξύ των δύο μισών του κυκλώματος (κάθε εφαρμογής ενός μετατροπέα) διατηρείται όσο το δυνατόν μικρότερη. Δεν είναι σαφές από τη λογική περιγραφή του κελιού σε ποια κατάσταση θα είναι αμέσως μετά την έναρξη λειτουργίας της μνήμης. Όταν η τάση τροφοδοσίας έρχεται, παρατηρείται ότι μερικά κελιά κατά προτίμηση αυτά που αποθηκεύουν 0, και άλλα κατά προτίμηση αποθηκεύουν 1, και άλλα δεν έχουν πραγματική προτίμηση, αλλά η κατανομή αυτών των τριών τύπων κυττάρων κατά την διάρκεια όλης την μνήμης είναι τυχαία.
Όπως αποδεικνύεται, η τυχαία φυσική αναντιστοιχία στο κελί, που προκαλείται από την κατασκευαστική μεταβλητότητα, καθορίζει την πιο δυναμική συμπεριφορά. Αναγκάζει ένα κελί να γίνει μηδέν ή ένα κατά την εκκίνηση ανάλογα με το πρόσημο της αναντιστοιχίας. Εάν η αναντιστοιχία είναι πολύ μικρή, η πιο δυνατή κατάσταση καθορίζεται από στοχαστικό θόρυβο στο κύκλωμα και θα είναι τυχαία χωρίς πραγματική προτίμηση.

2.2.2.2. ΠΕΤΑΛΟΥΔΕΣ PUFS (BUTTERFLY PUFS)

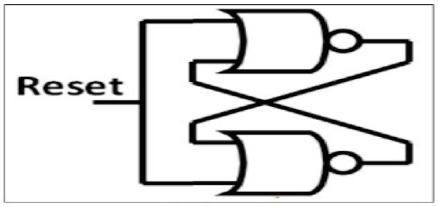
Ένα μειονέκτημα των SRAM PUFs είναι ότι τα κελιά SRAM έχουνε το πρόβλημα πως είναι δύσκολο να γίνει reset στο μηδέν αμέσως μετά την έναρξη της λειτουργίας ενός FPGA, και με αυτό τον τρόπο η τυχαιότητα χάνεται. Επίσης ένα ακόμα μειονέκτημα είναι πως όταν μια συσκευή είναι ενεργή, είναι απαραίτητη για να ενεργοποιήσει την παραγωγή εξόδων, το οποίο μπορεί να μην είναι πάντα εφικτό. Για την αντιμετώπιση των δύο αυτών μειονεκτημάτων, τα PUF πεταλούδες δημιουργήθηκαν. Η συμπεριφορά ενός SRAM κελιού μιμείται τη λογική ενός FPGA με την διασταύρωση δύο διαφανών μανταλωτών δεδομένων.
Σημειώνουμε πως ένα τέτοιο κύκλωμα επιτρέπει δύο λογικά σταθερές καταστάσεις. Ωστόσο, χρησιμοποιώντας την σαφή/προκαθορισμένη λειτουργία των μανταλωτών,μια ασταθής κατάσταση μπορεί να εισαχθεί μετά από την οποία το κύκλωμα συγκλίνει σε μια από τις δύο σταθερές καταστάσεις. Αυτό είναι συγκρίσιμο με την σύγκλιση για τα SRAM κελιά μετά την ενεργοποίηση, αλλά χωρίς την ανάγκη για μια πραγματική ενεργοποίηση συσκευής. Η προτιμώμενη κατάσταση σταθεροποίησης ενός PUF πεταλούδα κελιού καθορίζεται από την φυσική αναντιστοιχία ανάμεσα στους μανταλωτές και στην διασταύρωση της διασύνδεσης. Πρέπει να σημειωθεί πως λόγω των διακριτών επιλογών δρομολόγησης από ένα FPGA, είναι σημαντικό για την εφαρμογή του κελιού να γίνει με τέτοιο τρόπο ώστε η αναντιστοιχία του σχεδιασμού να είναι μικρή. Αυτή είναι μια απαραίτητη προυπόθεση αν κάποιος θέλει την τυχαία αναντιστοιχία που προκαλείται από κατασκευαστική μεταβλητότητα να έχουν οποιαδήποτε αποτελέσματα.



Schematical circuit of a butterfly PUF cell.

2.2.2.3 PUFS ΜΑΝΤΑΛΩΤΕΣ (LATCH PUFS)

Ο PUF μανταλωτής είναι ένα ολοκληρωμένο κύκλωμα τεχνικής αναγνώρισης και είναι παρόμοιο με ένα SRAM PUF ή ένα PUF πεταλούδα. Αντί για την διασταύρωση δύο μετατροπέων ή δύο μανταλωτών, διασταυρώνονται δύο πύλες NOR. Εισάγοντας ένα σήμα επαναφοράς, αυτός ο μανταλωτής γίνεται ασταθής και πάλι συγκλίνει σε μια σταθερή κατάσταση εξαρτόμενη στην εσωτερική αναντιστοιχία μεταξύ των ηλεκτρονικών εξαρτημάτων. Ισοδύναμα με τα SRAM PUFs και τα PUFs πεταλούδες ο από πάνω σχεδιασμός μπορεί να χρησιμοποιηθεί για την κατασκευή ενός PUF.



Logical circuit of a latch (PUF) cell.

2.2.2.4 FLIP – FLOP PUFS

Ισοδύναμα με τα SRAM PUFs, η πιο δυνατή συμπεριφορά των συνηθισμένων flip-flop μπορεί να μελετηθεί.

2.3 PUF ΠΡΟΤΑΣΕΙΣ/ΙΔΕΕΣ

Εδώ θα δούμε μερικές γενικεύσεις ή ακόμα και τρόπους λειτουργίας των PUF. Μερικές από αυτές είναι πραγματικές ιδέες για την δημιουργία PUF οι οποίες έχουν υλοποιηθεί αλλά η σκοπιμότητα τους δεν έχει βρεθεί ακόμα. Έχουνε βρεθεί από pappers.

2.3.1 POKS – ΦΥΣΙΚΑ ΜΠΕΡΔΕΜΕΝΑ ΚΛΕΙΔΙΑ

Τα POKs(Physically Obfuscated Keys) είναι φυσικά μπερδεμένα κλειδιά και η έννοια τους έχει γενικευτεί σε φυσικούς μπερδεμένους αλγορίθμους. Η βασική έννοια των κλειδιών αυτών, είναι ότι αποθηκεύονται μόνιμα με φυσικό τρόπο, γεγονός που καθιστά δύσκολο από έναν επιτηθέμενο να μάθει το κλειδί κάνοντας μια σχολαστική επίθεση. Επιπλέον, μια επεμβατική επίθεση στην συσκευή αποθηκεύει το κλειδί που θα πρέπει να καταστρέψει και να κάνει την περαιτέρω χρήση του αδύνατη, παρέχοντας έτσι το απαραβίαστο. Φαίνεται πως τα POKs και τα PUFs μοιάζουν πολύ, και αξίζει να σημειωθεί πως τα POKs μπορούν να κατασκευαστούν από (δηλωμένα ότι έχουν παραβιαστεί) PUFs.

2.3.2 CPUFS – ΕΛΕΓΧΟΜΕΝΑ PUFS

Στην πραγματικότητα ένα τέτοιο PUF είναι ένας τρόπος λειτουργίας για ένα PUF σε συνδιασμό με άλλους τρόπους κρυπτογραφίας.
Ένα PUF λέγεται ότι ελέγχεται εάν μόνο μπορεί να προσεγγιστεί από έναν αλγόριθμο, το οποίο είναι φυσικά δεμένο στον αλγόριθμο με αδιαχώριστο τρόπο. Προσπαθώντας να σπάσει ο σύνδεσμος ανάμεσα στο PUF και τον αλγόριθμο πρόσβασης πρέπει κατά προτίμηση να οδηγηθούμε στην καταστροφή του PUF. Είναι κάποια πλεονεκτήματα στην μετατροπή ενός PUF σε CPUF.

- Μια (κρυπτογραφημένη) συνάρτηση κατακερματισμού για να αναπαράγει τις εξόδους ενός PUF μπορεί να εμποδίσει διαλεγμένες-εισόδους επιθέσεις, δηλαδή, να φτιάξει τα μοντέλα των επιθέσεων του πιο δύσκολα. Ωστόσο, για PUF κριτές έχει δειχθεί ότι τα μοντέλα των επιθέσεων δουλεύουν το ίδιο καλά από τυχαία διαλεγμένες εισόδους.
- Ένας αλγόριθμος διόρθωσης σφαλμάτων που δρα στις μετρήσεις των PUF κάνει τις τελικές εξόδους πολύ πιο αληθοφανείς, μειόνωντας την πιθανότητα ενός bit-σφάλματος στην 'έξοδο σε εικονικό 0'.
- Μια κρυπτογραφημένη συνάρτηση κατακερματισμού εφαρμοσμένη στις εξόδους διορθωμένων σφαλμάτων, σπάει αποτελεσματικά τον σύνδεσμο ανάμεσα στις εξόδους και τις φυσικές λεπτομέρειες των μετρήσεων του PUF. Αυτό κάνει τα μοντέλα των επιθέσεων πολύ πιο δύσκολα.
- Η συνάρτηση κατακερματισμού παράγωντας τις εξόδους των PUF μπορεί να πάρει επιπλέον εισόδους, δηλαδή, να αφήνει να δωθούν στο PUF πολλαπλές 'προσωπικότητες'. Αυτό μπορεί να είναι επιθυμητό, όταν το PUF χρησιμοποιείται σε προσωπικές-ευαίσθητες εφαρμογές για την αποφυγή παρακολούθησης.

Είναι κατανοητό ότι μετατρέποντας ένα PUF σε CPUF αυξάνει κατά πολύ την ασφάλεια. Ένας αριθμός από πρωτόκολλα που χρησιμοποιούνε CPUFs είναι ήδη προτεινόμενα. Πρέπει να τονιστεί ότι η ενισχυμένη ασφάλεια ενός CPUF εξαρτάται από την φυσική συνδεσμολογία του PUF με τους αλγόριθμους πρόσβασης, οι οποίοι μπορεί να είναι πολύ αυθαίρετοι και μπορεί να είναι το αδύναμο σημείο των CPUFs.

2.3.3 RECONFIGURABLE PUFS (ΕΠΑΝΑΔΙΑΜΟΡΦΩΣΙΜΑ PUFS)

Τα επαναδιαμορφώσιμα PUFs ή rPUFs επεκτείνουν την συμπεριφορά CRP ενός PUF με μια πρόσθετη λειτουργία που ονομάζεται reconfiguration=επαναδιαμόρφωση. Αυτή η επαναδιαμόρφωση έχει ως αποτέλεσμα ότι η πλήρης συμπεριφορά CRP ενός PUF να είναι τυχαία και κατά προτίμηση να αλλάζει αμετάκλητα, και στο τέλος να αλλάζει σε ένα εντελώς νέο PUF. Υπάρχουν δύο πιθανές εφαρμογές επαναδιαμορφώσιμων PUF, των οποίων ο μηχανισμός επαναδιαμόρφωσης είναι πραγματικός και φυσικός σύμφωνα με την τυχαιότητα των PUF.

(1) Το πρώτο είναι μια επέκταση των οπτικών PUF όπου μια ισχυρή δέσμη λέιζερ λιώνει το οπτικό μέσο, προκαλώντας αναδιάταξη των οπτικών σκεδαστών, η οποία με την σειρά της προκαλεί μια τελείως τυχαία και καινούργια CRP συμπεριφορά.
(2) Η δεύτερη πρόταση τώρα, βασίζεται σε μια νέου τύπου στατική μνήμη η οποία καλείται μνήμη αλλαγής φάσης. Γράφοντας σε μια τέτοια μνήμη αποτελείται από φυσικώς μεταβαλλόμενη φάση ενός μικρού κελιού από φυσικό σε άμορφο ή κάπου στο ενδιάμεσο, και διαβάζεται μετρώντας την αντίσταση του κελιού. Δεδομένου ότι οι μετρήσεις αντίστασης είναι πιο ακριβής από την ακρίβεια της γραφής, οι ακριβείς μετρούμενες αντιστάσεις μπορούν να χρησιμοποιηθούν ως αποκρίσεις/έξοδοι, και ξαναγράφοντας τα κελιά θα αλλάξουν με έναν τυχαίο τρόπο.

Και οι δύο προτάσεις είναι μάλλον είναι λίγο 'μακριά' αυτή την στιγμή και παραμένουν σε μεγάλο βαθμό μη δοκιμασμένες.

Μια τρίτη επιλογή είναι μια λογική επέκταση ενός συνηθισμένου PUF. Φτιάχνοντας ένα μέρος μιας PUF εισόδου με ένα παρελθόν ασφαλειών, το PUF μπορεί να επαναδιαμορφωθεί χτυπώντας την ασφάλεια, το οποίο αυτό με βέλτιστο τρόπο οδηγεί σε μια εντελώς διαφορετική CRP συμπεριφορά για τα bit εισόδου που είναι ελεγχόμενα από τον χρήστη. Ωστόσο, η μη αναστρειψιμότητα μιας τέτοιας λογικής rPUF μπορεί να είναι αμφισβητήσιμη, δεδομένου ότι η CRP συμπεριφορά δεν έχει χαθεί, και απλά είναι μπλοκαρισμένη. Πιθανές εφαρμογές των rPUFs είναι το κλειδί διαγραφής του περιεχομένου (key-zeroization), η ασφαλής αποθήκευση σε μια μη αξιόπιστη μνήμη και η πρόληψη υποβάθμισης, π.χ. η συσκευή firmware.

2.3.4 ΠΟΣΟΤΙΚΑ ΑΝΑΓΝΩΣΙΜΑ PUFS (QUANTUM READOUT PUFS)

Τα ποσοτικά αναγνώσιμα PUFs παρουσιάζουν μια ποσοτική επέκταση στα συνηθισμένα PUFs. Αυτό το PUF προτείνεται για να αναγνωρίσει τις συνηθισμένες εισόδους και εξόδους του με ποσοτικές καταστάσεις. Λόγω των ιδιοτήτων των ποσοτικών καταστάσεων, ένας αντίπαλος δεν μπορεί να υποκλέψει τις εισόδους και τις εξόδους, χωρίς να τις αλλάζει. Αυτό οδηγεί στο πλεονέκτημα ότι ο μηχανισμός ανάγνωσης ενός PUF δεν χρειάζεται να είναι έμπιστο πια, το οποίο είναι η περίπτωση για τα περισσότερα μη ποσοτικά PUFs. Μέχρι τώρα, η σκοπιμότητα αυτής της πρότασης δεν είναι πρακτικά εξακριβωμένη. Τέλος, δεν είναι σαφές εάν υφίστανται στα ήδη υπάρχοντα PUFs εάν μπορούν εύκολα να επεκταθούν για να δεχτούν και να παράγουν ποσοτικές καταστάσεις ως εισόδους και εξόδους.

2.3.5 SIMPL ΣΥΣΤΗΜΑΤΑ ΚΑΙ PPUFS

Το SIMPL(SImulation Possible but Laborious) σημαίνει προσομοίωση που μπορεί να είναι δυνατή αλλά επίπονη και είναι για να χρησιμοποιούνται τα PUFs σαν ένα αλγόριθμο δημοσίου κλειδιού. Εδώ η αξιολόγηση του μοντέλου είναι κοπώδης και για να ανιχνευθεί χρειάζεται μεγάλο χρονικό διάστημα όπως επίσης και για το ίδιο το PUF.

2.4.ΑΠΟΤΕΛΕΣΜΑΤΑ ΚΑΙ ΣΥΜΠΕΡΑΣΜΑΤΑ ΑΠΟ PAPERS

Είναι σημαντικό ορισμένες προτάσεις, να συμφωνούν σε μια σειρά από τυποποιημένα μέτρα, τα οποία μπορούν να αξιολογήσουν σωστά τις πρακτικές και την ασφάλεια που σχετίζονται με τα χαρακτηριστικά των PUFs που είναι κατασκευασμένα με αντικειμενικό τρόπο. Έτσι λοιπόν, θα δούμε μια σειρά από μεταχειρισμένες έννοιες που θεωρούνται σημαντικές για την σύγκριση κάποιων διαφορετικών προτάσεων PUF.

- Το μέγεθος του δείγματος.
  Αξίζει να επισημάνουμε πως το μέγεθος του δείγματος που χρησιμοποιείται για την εκτίμηση των χαρακτηριστικών των PUFs είναι αρκετά σημαντικό. Πιο συγεκριμένα είναι ο αριθμός των διακριτών διατάξεων, ο αριθμός των διακριτών εισόδων, ο αριθμός των διακριτών μετρήσεων της κάθε εξόδου κτλ. Μέχρι τώρα στα περισσότερα έργα υπήρχε επιμέλεια στην χρησιμοποίηση των μεταχειρισμένων συσκευών και του μεγέθους του πληθυσμού του δείγματος που εξετάσθηκε. Ωστόσο, για κανένα από τις προτάσεις για PUF ,η στατιστική ανάλυση, δεν είχε επισημανθεί το επίπεδο εμπιστοσύνης για την εκτίμηση των χαρακτηριστικών. Για την περαιτέρω τυπική ανάλυση των PUFs, αυτό θα έχει όλο και μεγαλύτερη σημασία.

- Εντός και μεταξύ των απόστασης ιστογράμματα.
  Η σημασία και των δύο εντός και μεταξύ απόστασης ως μέτρο για αντίστοιχα τη μοναδικότητα και το θόρυβο που υπάρχει σε μια PUF μέτρηση έχει επισημανθεί πολλές φορές νωρίτερα. Ευτυχώς, τα δύο αυτά μέτρα είναι σχεδόν πάντα υπό την προϋπόθεση της υπάρχουσας βιβλιοθήκης, κάνοντας τουλάχιστον μερικώς αντικειμενική σύγκριση μεταξύ των πρόωρων προτάσεων. Ωστόσο, μια σειρά από παρατηρήσεις είναι απαραίτητο να γίνουν.

  Πρώτον, αυτά τα ιστογράμματα συχνά θεωρούνται ότι είναι περίπου Gaussian και συνοψίζονται από τον μέσο όρο τους και πολλές φορές από την τυπική απόκλιση τους. Το Gaussian είναι μια προσέγγιση με στατιστική δομή. Επιπλέον, συνιστάται ιδιαίτερα να αναφέρονται πάντα και τα δύο και δεδομένου πως αυτό επιτρέπει να υπολογίσει τουλάχιστον την βέλτιστη FAR και FRR για τις εφαρμογές αναγνώρισης του συστήματος.
  Δεύτερον, αν και η μεταξύ απόσταση δίνει μια καλή αίσθηση της μοναδικότητας μια εξόδου, δεν μπορεί να χρησιμοποιηθεί για την εκτίμηση της παρούσας και πραγματικά ανεξάρτητης εντροπίας. Μερικά PUFs, π.χ., το PUF κριτής, το οποίο έχει αρκετά μεγάλη μεταξύ απόσταση υποφέρει από προβλεψιμότητα μεταξύ των εξόδων του.

- Εκτιμήσεις εντροπίας.

Για να ξεπεραστεί αυτό το τελευταίο πρόβλημα, μια σειρά από έργα προτινώμενων PUFs παρέχει μια εκτίμηση της πραγματικής εντροπίας που υπάρχει σε ένα μεγάλο αιρθμό από PUF εξόδους. Οι δύο μέθοδοι που χρησιμοποιούνται για να κάνουν αυτό τον έλεγχο συμπίεσης των συναρτήσεων των εξόδων, συνήθως χρησιμοποιούν την μέθοδο στάθμισης πλαισίου-δέντρου και τρέχουν συγκεκριμένα τυχαία τεστ όπως το Diehard τεστ και το NIST τεστ. Παρατηρούμε ότι λόγω του περιορισμένου μήκους των διαθέσιμων εξόδων, και οι δύο μέθοδοι γενικά προσφέρουν μόνο ένα χαμηλό επίπεδο αυτοπεποίηθησης κατά την έκβαση τους. Ειδικότερα, για τα τεστ τυχαιότητας, τα οποία είναι στην πραγματικότητα σχεδιασμένα να τεστάρουν την φαινομενική τυχαιότητα στην έξοδο των ψευδοτυχαίων αριθμών των γεννητριών, δεν είναι σαφές κατά πόσο η έκδοση των τεστ είναι σημαντική για τα PUFs. Τέλος, επισημαίνουμε ότι και οι δύο μέθοδοι υπολογίζουν μόνο την ανεξάρτητη εντροπία μέσα σε ένα ενιαίο PUF, δηλαδή πόση αβεβαιότητα μπορεί να έχει ένα αντίπαλος για την έκβαση μιας αόρατης απάντησης, ακόμα και αν έχουν μάθει όλες τις υπόλοιπες απαντήσεις από αυτό το PUF.
Ωστόσο, για να είναι ένα PUF ασφαλές, πρέπει επίσης να είναι απρόβλεπτο εφόσον του έχουν δοθεί εξόδοι από άλλα PUFs. Η τελευταία αυτή έννοια δεν αξιολογείται από τις εξεταζόμενες εκτιμήσεις της εντροπίας.

- Επιδράσεις περιβάλλοντος.
  Οι PUF εξόδοι υπόκεινται σε ανεπιθύμητες φυσικές επιδράσεις από το άμεσο περιβάλλον τους. Για ένα PUF να χρησιμοποιηθεί σε πρακτική εφαρμογή, έχει ως αποτέλεσμα να πρέπει να είναι αυστηρά ποσοτικό προκειμένου να αποφευχθούν απρόβλεπτες βλάβες. Για τα εσωτερικά PUFs στα ολοκληρωμένα κυκλώματα, θα πρέπει τουλάχιστον να μελετηθεί η συχνότητα της μειωμένης θερμοκρασία και η τάση τροφοδοσίας για της εξόδους των PUF.

- Απόδοση της CRP και της προβλεψιμότητας.
  Για όλα τα προτεινόμενα εσωτερικά PUFs, ο αριθμός των απρόβλεπτων CRPs περιορίζεται σε ένα πολυωνυμικό ποσό του μεγέθους των PUF. Για να εκτιμηθεί η χρησιμότητα ενός συγκεκριμένου PUF σε ορισμένες εφαρμογές, είναι σημαντικό να γνωρίζουμε πόσα απρόβλεπτης απόκρισης bits μπορεί κανείς να αποκτήσει με βέλτιστο τρόπο από ένα PUF ενός δεδομένου μεγέθους. Αυτό απαιτεί περαιτέρω μελέτη της προβλεψιμότητας των PUF εξόδων.

- Κόστος υλοποίησης και αποδοτικότητας.
  Είναι προφανές ότι, προκειμένου να υπάρχει οποιαδήποτε πρακτική χρήση, PUFs και εφαρμογές βασισμένες στα PUFs πρέπει να είναι από μεριάς κόστους όσο το δυνατόν πιο αποδοτικές. Μετρώντας την υλοποίηση και το κόστος λειτουργίας όσον αφορά το μέγεθος, την ταχύτητα και την κατανάλωση ενέργειας είναι μια άσκηση η οποία πρέπει να γίνεται για κάθε εφαρμογή

υλικού και δεν περιορίζεται σε PUFs.

- Παραποιημένες αποδείξεις.
  Αξίζει να επισημανθεί ότι ο κάθε ισχυρισμός ή παραδοχή σχετικά με την ένδειξη παραβίασης μιας συγκεκριμένης κατασκευής PUF έχει νόημα μόνο αν συνοδεύεται από μια πειραματική επαλήθευση. Μια λεπτομερής περιγραφή του εκτελείται στα πειράματα των παραποιημέων αποδείξεων, και τα προκείμενα αποτελέσματα στην συμπεριφορά CRP των PUF είναι ανεκτίμητα στην περίπτωση αυτή. Τέτοια πρακτικά αποτελέσματα ισχύουν μόνο για τα οπτικά και τα επικαλυμένα PUF.

ΚΕΦΑΛΑΙΟ 3

ΣΧΕΔΙΑΣΜΟΣ ΟΛΟΚΛΗΡΩΜΕΝΩΝ ΚΥΚΛΩΜΑΤΩΝ

Ο πραγματικός σχεδιασμός του μικροεπεξεργαστή γίνεται πρώτα σε λογικό επίπεδο. Ο επεξεργαστής ορίζεται όσον αφορά την επιθυμητή λειτουργία του, με τι εντολές που θα είναι καθορισμένος να λειτουργεί και πως τα δεδομένα θα μετακινούνται μεταξύ των λογικών μερών του. Αυτή η υψηλού επιπέδου σχεδίαση ξεκινάει από ένα θεμελιώδες επίπεδο και προχωράει σε πιο λεπτομερή, όπου τα διάφορα αρχιτεκτονικά χαρακτηριστικά του chip καθορίζονται με μεγάλη λεπτομέρεια, όπως το πως οι εντολές θα αποκωδικοποιούνται και πως οι μονάδες ελέγχου θα λειτουργούν. Πρόκειται για μια πολύ συντομή περιγραφή της διαδικασίας σχεδιασμού, που απαιτεί εκατοντάδες ή ακόμα και χιλιάδες μηχανικούς και παίρνει μήνες ή και χρόνια, κάτι το οποίο εξαρτάται από το πόσο εξελιγμένη είναι η σχεδίαση του νέου επεξεργαστή, καθώς και πόσα από τα χαρακτηριστικά είναι δανεισμένα από τις προηγούμενες σχεδιάσεις.

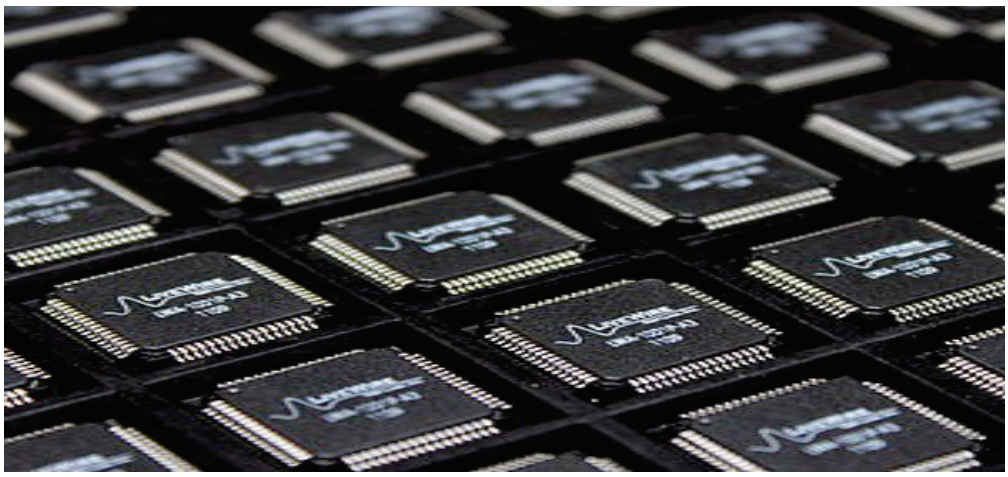
Καθώς ο επεξεργαστής έχει πλήρως καθοριστεί με αυτό τον τρόπο, σχεδιάζεται φυσικώς. Τα πραγματικά απαραίτητα transistors για την υλοποίηση του σχεδιασμού καθορίζονται και ένα φυσικός χάρτης δημιουργείται, ο οποίος δείχνει πως το chip πρέπει να κατασκευαστεί. Στην πραγματικότητα, δεν υπάρχει μόνο μια σχεδίαση, που σχεδιάζεται κατά αυτό τον τρόπο μια φορά. Πρόκειται για μια επαναληπτική διαδικασία με αλλαγές που γίνονται συνεχώς στο σχεδιασμό, εξαιτίας των λαθών, των βελτιώσεων, των θεμάτων αγοράς ή των αρχών της κατασκευής.

3.1 ΕΝΣΩΜΑΤΩΜΕΝΑ ΣΥΣΤΗΜΑΤΑ

Ένα ενσωματωμένο σύστημα είναι ένα υπολογιστικό σύστημα ειδικού σκοπού, σχεδιασμένο έτσι ώστε να εκτελεί μια ή και περισσότερες συναρτήσεις, συνήθως σε σταθερές πραγματικού χρόνου. Είναι συνήθως ενσωματωμένο σαν ένα μέρος μιας ολοκληρωμένης συσκευής, περιλαμβάνοντας hardware καθώς και μηχανικά μέρη. Σε αντίθεση, ένα υπολογιστικό σύστημα γενικού σκοπού, όπως ένας προσωπικός υπολογιστής, ανάλογα με τον προγραμματισμό που του έχει γίνει, μπορεί να κάνει πολλά διαφορετικά καθήκοντα. Τα ενσωματωμένα συστήματα ελέγχουν πολλές από τις κοινές καθημερινές συσκευές που χρησιμοποιούμε σήμερα. Από τη στιγμή που ένα σύστημα είναι προσανατολισμένο σε συγκεκριμένα καθήκοντα, οι μηχανικοί σχεδίασης μπορούν να το βελτιστοποιήσουν, μειώνοντας το μέγεθος και το κόστος του.
Το hardware(υλικό) των ενσωματωμένων συστημάτων είναι συνήθως διαφορετικό από το hardware ενός κλασικού συστήματος. Τους ενσωματωμένους επεξεργαστές μπορούμε να τους χωρίσουμε σε 2 μεγάλες κατηγορίες : Στους μικροεπεξεργαστές (μP) και στους μικροελεγχτές (μC), οι οποίοι έχουν πολλά περισσότερα περιφερειακά στο chip, μειώνοντας έτσι το κόστος και το μέγεθος.

3.1.1. ASIC

Το ASIC (application-specific integrated circuit) είναι επεξεργαστής υπολογιστών που εκτελεί έναν συγκεκριμένο στόχο αντί της εκτέλεσης γενικών υπολογισμών. Εκεί όπου η ΚΜΕ ενός υπολογιστή είναι ένα ολοκληρωμένο κύκλωμα που χειρίζεται ένα πλήθος γενικών στόχων επεξεργασίας, τα ASICs προσαρμόζονται και εκτελούν μόνο έναν συγκεκριμέο τύπο επεξεργασίας. Για παράδειγμα, ένα τσίπ το οποίο είναι σχεδιασμένο να τρέχει σε ένα ψηφιακό καταγραφέα φωνής ή σε ένα υψηλής απόδοσης παραγωγό νομισμάτων (bitcoins) είναι ένα ASIC.
Τα ASICs είναι σε θέση να εκτελέσουν τις εφαρμογές σε μια γρήγορη ταχύτητα και χρησιμοποιούνται συνήθως σε μια ποικιλία των ηλεκτρονικών συσκευών. Ωστόσο , ένα από τα σημαντικότερα μειονεκτήματα ενός ASIC είναι ότι δεν μπορούν να επαναπρογραμματιστούν για χρήση σε άλλη εφαρμογή. Για παράδειγμα, ο επεξεργαστής σε ένα κινητό τηλέφωνο δεν μπορεί να προγραμματιστεί για επαναχρησιμοποίηση ως ένα μόνιτορ καρδιακού ρυθμού.
Υπολογιστικές συσκευές γενικής χρήσης , που αναφέρονται επίσης ως μικροεπεξεργαστές , βρίσκονται στο άλλο άκρο του φάσματος. Μικροεπεξεργαστές μπορούν να προγραμματιστούν από το λογισμικό και είναι σε θέση να εκτελέσει ένα ευρύ φάσμα καθηκόντων και των εφαρμογών . Ωστόσο , η ευελιξία αυτή μπορεί να έρθει εις βάρος της ταχύτητας. Δεδομένου ότι οι μικροεπεξεργαστές έχουν σχεδιαστεί για να εκτελέσουν ένα ευρύ φάσμα εφαρμογών , μπορούν συχνά με πολύ καλύτερες επιδόσεις από τα ASICs στην ταχύτητα να το κάνουν.



Ένα ολοκληρωμένο κύκλωμα για συγκεκριμένες εφαρμογές (ASIC) είναι συμπαγώς συσκευασμένο ηλεκτρονικό κύκλωμα που προορίζεται για την απλοποίηση του συνολικού σχεδιασμού του κυκλώματος. Σε ορισμένες περιπτώσεις, εμποδίζει επίσης την αντίστροφη μηχανική ενός υπάρχοντος προϊόντος. Για παράδειγμα, πολλά προϊόντα χρησιμοποιούν ένα μόνο τσιπ ειδικού σκοπού για τον έλεγχο του προϊόντος. Σχεδόν όλες οι συσκευές, όπως υπολογιστές, κινητά τηλέφωνα, και άλλες ψηφιακές συσκευές θα χρησιμοποιούν τουλάχιστον ένα ASIC. Αυτό το κύκλωμα διαφέρει σημαντικά από ένα γενικού σκοπού ολοκληρωμένο κύκλωμα (IC).

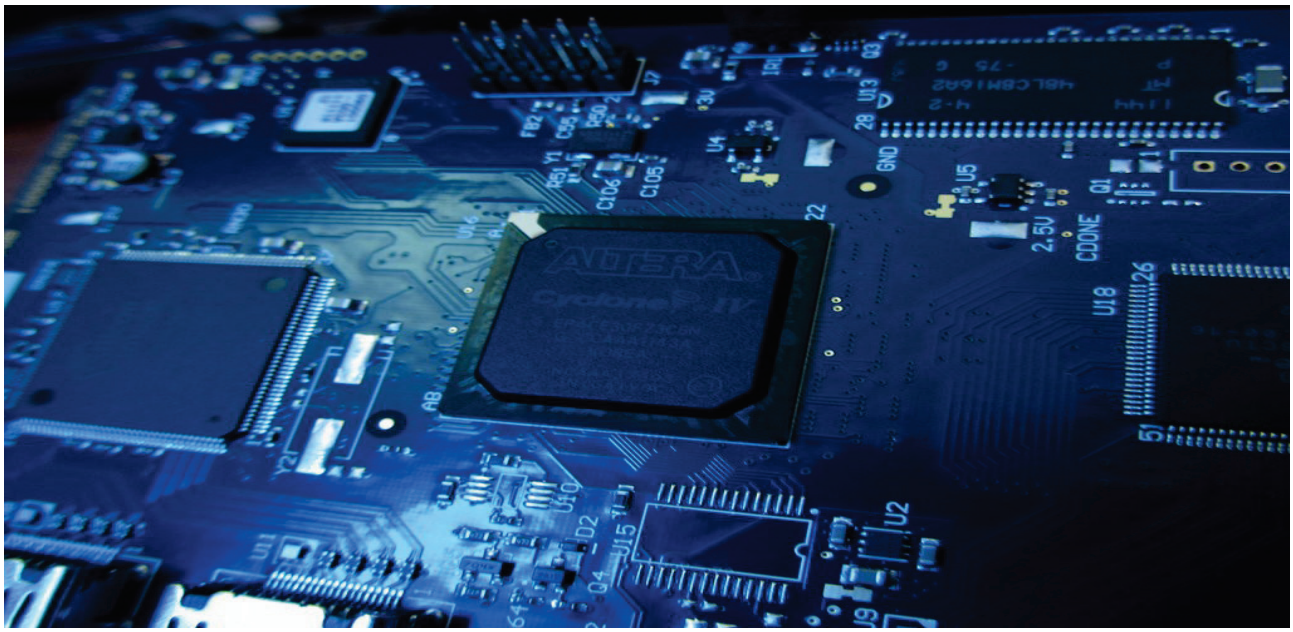
Επίσης γνωστό ως μικροτσίπ, το IC εισήχθη για πρώτη φορά για την ελαχιστοποίηση του αριθμού εξαρτημάτων σε ένα κύκλωμα της πλακέτας. Αν για το κύκλωμα χρησιμοποιείται μια ντουζίνα τρανζίστορ με δύο ντουζίνες τρανζίστορ και δύο ντουζίνες αντιστάσεις και πυκνωτές, το IC χρησιμποιείται για να αντικαταστήσει τα περισσότερα από αυτά τα μέρη. Το αποτέλεσμα είναι ένα ορισμένο ποσό σμίκρυνσης το οποίο έχει γίνει το πρώτο από μια σειρά από συνεχώς αυξανόμενη πυκνότητα των συστατικών σε ένα IC. Οι σύγχρονοι μικροεπεξεργαστές για παράδειγμα, περιλαμβάνουν πάνω από ένα εκατομμύριο τρανζίστορ σε ένα χώρο μικρότερο από μια τετραγωνική ίντσα.
Το ολοκληρωμένο κύκλωμα συγκεκριμένης εφαρμογής χρησιμοποιείται συχνά σε πολύπλοκες εφαρμογές κυκλώματος. Για παράδειγμα, στον προσωπικό υπολογιστή με μια απλή κάρτα προσαρμογέα γραφικών, μπορεί να μην είναι δυνατόν να εγκαταστήσετε με επιτυχία ένα παιχνίδι υψηλής έντασης γραφικών. Το πρόγραμμα εγκατάστασης του παιχνιδιού μπορεί να αναμένει μια συμβατή κάρτα γραφικών επιταχυντή (GAC), η οποία περιέχει ένα ASIC που είναι σε θέση να εφαρμόσει υψηλού επιπέδου γραφικές εντολές, και ένας συνηθισμένος προσαρμογέας γραφικών δεν θα μπορούσε να ερμηνεύσει. Ένα ASIC μπορεί να είναι σε θέση να αντλήσει συνήθη σχήματα ταυτόχρονα σε διαφορετικές τοποθεσίες στην οθόνη. Αυτή η λειτουργία είναι απαραίτητη για να δημιουργήσει εικόνες αρκετά γρήγορα για να δούμε σε πραγματικό χρόνο.
Στις επικοινωνίες δεδομένων, η συγκεκριμένη εφαρμογή ολοκληρωμένων

κυκλωμάτων μπορεί να χρησιμοποιηθεί σε υπολογιστές, διανομείς, διακόπτες και δρομολογητές. Η κάρτα διασύνδεσης δικτύου (NIC) χρησιμοποιεί ένα προσαρμοσμένο τσιπ, ένα ASIC που χειρίζεται τα στοιχεία και φυσική σύνδεση απαιτήσεις στρώμα του τοπικού δικτύου. Η ASIC στην NIC είναι υπεύθυνη για τη φυσική συμπεριφορά του NIC. Για παράδειγμα, ένας προσαρμογέας Ethernet θα έχει μια συγκεκριμένη εφαρμογή ολοκλωρωμένων κυκλωμάτων που θα είναι σε θέση να χειριστούν εργασίες όπως ανίχνευση πακέτων σύγκρουσης και αναμετάδοση, όπως απαιτείται. Αν το NIC είναι ένας τύπος token-δακτυλίου, το ASIC περιμένει τότε τη λήψη ενός πακέτου σημαία γνωστό ως ένδειξη προτού επιχειρείσει να μεταδώσει στο δίκτυο.
Τα υψηλότερης πυκνότητας τσιπ ημιαγωγών συχνά προτιμούνται στην κατασκευή ηλεκτρονικών. Αυτό έχει ως αποτέλεσμα νεότερα προϊόντα με τσιπ γενικής χρήσης και ολοκληρωμένα κυκλώματα για συγκεκριμένες εφαρμογές με χαμηλότερα μέρη μετράνε και μικρότερα μεγέθη ή ίχνη. Εάν τα τμήματα γενικού σκοπού του κυκλώματος μπορεί να ενσωματωθούν σε ένα μικρότερο πακέτο, το αποτέλεσμα είναι συνήθως ένα ολοκληρωμένο κύκλωμα συγκεκριμένης εφαρμογής.
Πιο επιστημονικά, ένα ολοκληρωμένο συγκεκριμένων εφαρμογών όταν συνεργάζεται με έναν μικροεπεξεργαστή, μια είσοδο και έναν επισημοποιημένο σταθμό, παρέχει λειτουργίες συγχρονισμού, την παραλαβή δεδομένων εισόδου και αποθήκευσης για την διαβίβαση προς τον μικροεπεξεργαστή και αποθήκευση για την παραλαβή, ενεργώντας βάσει πληροφοριών που έλαβε από τον μικροεπεξεργαστή.
Οι διάφορες λειτουργίες που μπορεί να επιτευχθούν από το κύκλωμα, διενεργούνται από το κύκλωμα κατόπιν εντολής από τον μικροεπεξεργαστής χρησιμοποιώντας ένα μονό σειριακό μονοπάτι δεδομένων.

3.1.2. FPGA

Το FPGA ή Field Programmable Gate Array ή "συστοιχία επιτόπια προγραμματιζόμενων πυλών" είναι τύπος ολοκληρωμένου κυκλώματος ικανό να επαναπροσδιορίζει την εσωτερική του δομή ανάλογα με τις ανάγκες του σχεδιαστή, Εξου και ο όρος "προγραμματιζόμενων πυλών". Η τροποποίηση του FPGA γίνεται με περιγραφικές γλώσσες (Hardware Description Languages-HDL), όπως VHDL, Verilog, Handle-C κ.ο.κ. Τα FPGAs μπορούν να χρησιμοποιηθούν στην υλοποίηση οποιουδήποτε λογικού κυκλώματος όπως καταχωρητές, απαριθμητές ακόμη και μικρών επεξεργαστών, αντικαθιστώντας πολλά από τα ήδη υπάρχοντα ολοκληρωμένα, αυξάνοντας αντίστοιχα τις επιδόσεις και μειώνοντας το κόστος. Η σημαντικότερη καινοτομία που εισήγαγαν είναι η ικανότητα επαναπροσδιορισμού του εσωτερικού τους κάτι που φάνταζε αδύνατο πριν την εμφάνιση τους. Αυτό το χαρακτηριστικό τα έκανε να επικρατήσουν έναντι των ASIC (application-specific integrated circuit ή ολοκληρωμένα κυκλώματα για συγκεκριμένη εφαρμογή), προσφέροντας πλεονεκτήματα για πολλές εφαρμογές.
Μια FPGA είναι μια συσκευή ημιαγωγών και αποτελείται από πολλά blocks προγραμματιζόμενης λογικής, καθώς και από τις διασυνδέσεις μεταξύ τους. Αυτά τα

λογικά blocks μπορούν να προγραμματιστούν για να εκτελέσουν τις λογικές πράξεις AND και XOR καθώς και ποιο περίπλοκους συνδυασμούς των πράξεων αυτών. Στις περισσότερες FPGAs κάποια από αυτά τα blocks υποκαθιστούν στοιχεία μνήμης, δηλαδή απλά flip – flops ή ποιο σύνθετα blocks μνήμης. Δεν προσφέρονται για τον σχεδιασμό πολύ πολύπλοκων κυκλωμάτων, αλλά σε αντιπαράθεση με αυτό μας προσφέρουν το πλεονέκτημα του επαναπρογραμματισμού από την αρχή. Υπάρχουν δύο τρόποι για να τις προγραμματίσουμε: είτε με τη βοήθεια κυκλωματικών σχεδιαγραμμάτων, είτε μέσω HDL που είναι μια περιγραφική γλώσσα προγραμματισμού για FPGAs και συνίσταται για μεγαλύτερα και πολυπλοκότερα projects. Μετατρέποντας είτε τα σχεδιαγράμματα είτε τον κώδικα της HDL σε εκτελέσιμα κυκλώματα χρειαζόμαστε είτε ένα σειριακό interface τύπου JTAG, Είτε τη βοήθεια εξωτερικής μνήμης τύπου EEPROM.



Τα FPGAs περιέχουν ομάδες από λογικές πύλες διασυνδεδεμένες μεταξύ τους ώστε να φέρνουν εις πέρας μια συγκεκριμένη λειτουργία. Αυτές οι ομάδες ονομάζονται "Λογικά μπλοκ" και δεν μπορούμε να επέμβουμε στην δομή τους. Μέσω κάποιων ιεραρχικών κανόνων και δυνατών συνδέσεων τα "Λογικά μπλοκ" συνδέονται μεταξύ τους (επαναπροσδιορίζονται) και φέρνουν εις πέρας το επιθυμητό αποτέλεσμα είτε αυτό είναι απλές λογικές πύλες ή πολύπλοκες λογικές συναρτήσεις. Τα περισσότερα FPGAs περιέχουν μέσα στα λογικά μπλοκ και στοιχεία από μνήμες, τα οποία είτε είναι μερικά Flip-Flops ή συστάδες από κύτταρα μνήμης (DRAM, SRAM). Εκτός από τις ψηφιακές λειτουργίες, μερικές FPGAs έχουν και αναλογικά χαρακτηριστικά. Ένα από αυτά είναι η ομαδοποίηση των ακροδεκτών ανάλογα με τις δυνατότητες τους τόσο σε ικανότητα οδήγησης απαιτητικών στοιχείων από πλευράς ισχύος, όσο και από πλευράς ταχύτητας. Ένα ακόμη χαρακτηριστικό τους το οποίο είναι δημιούργημα της εξελιγμένης μικροηλεκτρονικής είναι η ενσωμάτωση σε αυτά διαφορικών ενισχυτών, μετατροπέων σήματος από αναλογικό σε ψηφιακό και το

αντίστροφο και τέλος ακόμη και PLL (Phase Locked-Loop). Τέτοια χαρακτηριστικά ξενίζουν τους σχεδιαστές οι οποίοι είχαν να κάνουν με αμιγώς ψηφιακά ή αναλογικά ολοκληρωμένα, αλλά ταυτόχρονα χαράσσουν το μέλλον και τους εφοδιάζουν με δυνατότητες που απογειώνουν την παραγωγικότητα τους χωρίς αντίκτυπο στην ποιότητα του τελικού προϊόντος.

Σε θέματα που αφορούν την ασφάλεια, τα FPGAs έχουν τόσο πλεονεκτήματα όσο και μειονεκτήματα σε σχέση με τους ανταγωνιστές τους όπως τα ολοκληρωμένα τα οποία σχεδιάστηκαν και υλοποιήθηκαν για συγκεκριμένο σκοπό και τους μικροεπεξεργαστές. Εύκολα μπορούμε να καταλάβουμε ότι είναι αδύνατον να αλλάξουμε την εσωτερική δομή ενός ολοκληρωμένου ή ενός μικροεπεξεργαστή. Ωστόσο αυτή η σταθερότητα δεν υπάρχει στα FPGAs και κατά την διάρκεια του προγραμματισμού του FPGA και μετά ο κώδικας μπορεί να είναι εκτεθειμένος. Ως λύση σε αυτό το πρόβλημα, ορισμένα FPGAs υποστηρίζουν κρυπτογράφηση.

Εφαρμογές:

Τα FPGAs συναντώνται σε πληθώρα εφαρμογών όπως ψηφιακή επεξεργασία σήματος, ψηφιακό ραδιόφωνο, αεροδιαστημική και αμυντική τεχνολογία, ιατρική απεικόνιση, υπολογιστική όραση, αναγνώριση ομιλίας, κρυπτογραφία, εξομοίωση πειραματικών μονάδων υπολογιστών, ραδιοαστρονομία, ανίχνευση μετάλλων και σε πολλές άλλες γοργά αναπτυσσόμενες εφαρμογές. Τα FPGAs υλοποιήθηκαν και παρουσιάστηκαν στην αγορά σαν τον κυριότερο ανταγωνιστή των CPLDs, με δυνατότητες πολύ μεγαλύτερες από αυτές των προκατόχων τους τόσο σε ταχύτητα όσο και σε μέγεθος ίσως και μικρότερο από αυτό των CPLDs. Ποιο συγκεκριμένα μετά την εισαγωγή κυκλωμάτων πολλαπλασιαστών στην αρχιτεκτονική των FPGA στα τέλη της δεκαετίας του '90, εφαρμογές όπου παραδοσιακά κυριαρχούσαν τα DSPs άρχισαν να υλοποιούνται από FPGAs. 24 Συγκεκριμένα τα FPGAs βρίσκουν εφαρμογές στην επεξεργασία αλγορίθμων οι οποίοι κάνουν χρήση της παράλληλης επεξεργασίας που προσφέρει η αρχιτεκτονική τους. Ένα τέτοιο πεδίο εφαρμογής είναι η αποκρυπτογράφηση, η βίαιη προσπάθεια εύρεσης του κλειδιού ή του αλγορίθμου που υλοποιεί την κρυπτογράφηση. Ο εγγενής παραλληλισμός των λογικών πόρων σε ένα FPGA επιτρέπει σημαντική υπολογιστική απόδοση ακόμα και σε χαμηλές τιμές MHz. Η ευελιξία του FPGA επιτρέπει την επίτευξη ακόμα υψηλότερων επιδόσεων, όμως η ανάπτυξη των FPGAs σε υπολογιστές υψηλών επιδόσεων περιορίζεται σήμερα από την πολυπλοκότητά τους, σε σύγκριση με τα συμβατικά λογισμικά και τη συνεχώς αυξανόμενη βελτίωση των εργαλείων σχεδιασμού. Αν και το κόστος δημιουργίας των FPGAs είναι αρκετά μεγάλο παρόλα αυτά δαπανώνται αρκετοί πόροι από τις εταιρείες για την ανάπτυξή τους. Ο λόγος είναι η υψηλή δυναμική των επιδόσεών τους σε πολλές εφαρμογές.

Σχεδιασμός και προγραμματισμός:

Για να προγραμματίσουμε το FPGA, κάνουμε χρήση μιας γλώσσας περιγραφής υλικού (HDL) ή σχηματικό. Το έντυπο της HDL είναι πιο κατάλληλο για την εργασία με μεγάλες δομές, διότι είναι δυνατό να προσδιοριστούν ακριβώς αριθμητικά, αντί να κατασκευάσει κάθε κομμάτι με το χέρι. Ωστόσο, η σχηματική είσοδος μπορεί να επιτρέψει την ευκολότερη απεικόνιση ενός σχεδίου ή υποδείγματος.

Στη συνέχεια, χρησιμοποιώντας ένα ηλεκτρονικό αυτόματο εργαλείο σχεδιασμού, μια εικονική διασύνδεση δημιουργείται. Η netlist μπορεί στη συνέχεια να τοποθετηθεί στην πραγματική αρχιτεκτονική FPGA χρησιμοποιώντας μια διαδικασία που ονομάζεται placeand-route , που συνήθως εκτελούνται από τις διαδρομές και λογισμικό της εταιρείας FPGA.

Ο χρήστης θα επικυρώσει το σχέδιο, τον τόπο και τα αποτελέσματα διαδρομής μέσω της ανάλυσης χρονισμού, προσομοίωση, και άλλες επαληθεύσεις. Μόλις η διαδικασία σχεδιασμού ολοκληρωθεί, το δυαδικό αρχείο δημιουργείται (χρησιμοποιώντας ιδιόκτητο λογισμικό της εταιρείας του FPGA) και χρησιμοποιείται για να ρυθμίσουμε το FPGA. Πηγαίνοντας από το σχηματικό / HDL αρχείο προέλευσης σε πραγματική διαμόρφωση: Τα πηγαία αρχεία τροφοδοτούνται σε μια σουίτα λογισμικού από το FPGA / CPLD που μέσα από διάφορα στάδια, θα παράγει ένα αρχείο. Αυτό το αρχείο στη συνέχεια μεταφέρεται στο FPGA / CPLD μέσω μιας σειριακής θύρας (JTAG) ή σε εξωτερική μνήμη της συσκευής όπως ένα EEPROM .

Οι πιο συχνές HDLs είναι η VHDL και η Verilog, αν και σε μια προσπάθεια να μειωθεί η πολυπλοκότητα του σχεδιασμού σε HDLs, οι οποίες έχουν σχέση με το αντίστοιχο των γλωσσών συναρμολόγησης , έγιναν κινήσεις για να αυξηθεί το επίπεδο αφαίρεσης μέσω της εισαγωγής εναλλακτικών γλωσσών .

Για να απλοποιηθεί ο σχεδιασμός των πολύπλοκων συστημάτων σε FPGAs, υπάρχουν βιβλιοθήκες προκαθορισμένων λειτουργιών και κυκλώματα που έχουν δοκιμαστεί και βελτιστοποιηθεί ώστε να επιταχυνθεί η διαδικασία σχεδιασμού. Αυτά τα προκαθορισμένα κυκλώματα ονομάζονται κοινώς IP πυρήνες , και είναι διαθέσιμα από FPGA προμηθευτές και τρίτους προμηθευτές IP (σπάνια ελεύθερο, και τυπικά, που διατίθεται βάσει αποκλειστικής άδειας).

Άλλα προκαθορισμένα κυκλώματα είναι διαθέσιμα από τις αναπτυξιακές κοινότητες, όπως η OpenCores (τυπικά, που διατίθεται βάσει ελεύθερου και ανοικτού κώδικα αδειών, όπως η GPL , BSD ή παρόμοιες άδειες), και από άλλες πηγές. Σε ένα τυπικό σχέδιο ροής, η ανάπτυξη εφαρμογών για FPGA θα προσομοιώνουν το σχεδιασμό σε πολλαπλά στάδια σε όλη τη διαδικασία σχεδιασμού.

3.2 ΣΧΕΔΙΑΣΜΟΣ ΤΩΝ PUF

Μετά από την εκτεταμένη επισκόπηση της μεγάλης ποικιλίας των PUF προτάσεων γίνεται σαφές πως η έννοια της φυσικής μη κλωνοποιήσιμης συνάρτησης θα είναι δύσκολο να οριστεί σε μια μόνο πρόταση. Προηγούμενες απόπειρες επεξήγησης ενός PUF είναι συχνά πολύ περιορισμένες, με κάποιες εξαιρέσεις βέβαια, ή πολύ ευρεία, συμπεραλαμβανομένων και άλλων πραγμάτων εκτός από PUFs, και κατά κύριο λόγο ad-hoc, δίνοντας δηλαδή έτσι μια άτυπη περιγραφή της δοθήσας ποιότητας της προτεινόμενης κατασκευής. Επιπλέον σε πολλές από αυτές τις προσπάθειες περιλαμβάνονται λεπτομέρειες οι οποίες δεν έχουν καν επικυρωθεί απλά μόλις υποτεθεί.

3.2.1 ΠΕΡΙΓΡΑΦΗ

Εδώ θα απαριθμηθούν οι σημαντικότερες ατομικές ιδιότητες που έχουν επιλεγεί από διάφορες απόπειρες να δωθεί ορισμός και/ή να αναγνωριστεί στις PUF προτάσεις. Αν και δεν έχουν επισημοποιηθεί πλήρως οι ιδιότητες που συζητήθηκαν, δίνεται μια υπόδειξη προς μια ενδεχόμενη επισημοποίηση και προσπαθώντας να γίνουν όσο πιο σαφής γίνεται οι περιγραφές για την αποφυγή η ασάφεια στις μελλοντικές εργασίες.
Για την απλοποίηση της περιγραφής των ατομικών ιδιοτήτων, ξεκινάμε από μια πολύ βασική ταξινόμηση για ένα PUF ως μια φυσική διαδικασία εισόδου-εξόδου.
Σημείωση ότι αυτό ήδη αναθέτει δύο ιδιότητες στα PUFs, δηλαδή, *ένα στιγμιότυπο ενός PUF δεν μπορεί απλά να είναι μια αφηρημένη έννοια, αλλά είναι πάντα (ενσωματωμένο σε) μια φυσική οντότητα, και ένα PUF είναι μια διαδικασία (όχι αυστηρά μια συνάρτηση) με κάποιο λειτουργικότητα εισόδου-εξόδου*.

Δεδομένου ότι αυτές οι ιδιότητες είναι θεμελιώδεις και είναι σαφές από την κατασκευή για κάθε PUF πρόταση μέχρι τώρα, δεν χρειάζεται περαιτέρω ανάλυση.
Για λόγους συντομίας, χρησιμοποιείται ο συμβολισμός $\Pi : X \rightarrow Y : \Pi(x) = y$ για να υποδηλώσει τη λειτουργικότητα της εισόδου-εξόδου του Π PUF.

Ξεκινάμε καταγράφοντας τις επτά πιο τακτικές ιδιότητες που εμφανίζονται από πολλαπλές απόπειρες PUF ορισμών και δίνουν μια σύντομη αλλά ακριβής περιγραφή του τι εννοούμε με τον όρο τους.
Σημειώνουμε πως δεν είναι τυπικές ιδιότητες, αλλά μια υπόδειξη προς μια πιο επίσημη περιγραφή όπου δίνεται.

1. Αξιολογίσημο: με δοσμένο το Π και το x, είναι εύκολο να αξιολογηθεί το y=Π(x)
2. Μοναδικότητα: Π(x) περιέχει κάποιες πληροφορίες σχετικά με την ταυτότητα της φυσικής οντότητας ενσωματώνοντας το Π.
3. Επαναληψιμότητα: y=Π(x) είναι αναπαραγωγίσιμη μέχρι ένα μικρό σφάλμα.
4. Μη κλωνοποιήσιμη: δοσμένο Π, είναι δύσκολο να κατασκευαστεί μια διαδικασία με Γ διάφορο του Π έτσι ώστε $\forall x \in X : \Gamma(x) \approx \Pi(x)$ μέχρι ένα μικρό σφάλμα.
5. Απρόβλεπτο: με δοσμένο μόνο ένα σετ $Q = \{(xi, yi = \Pi(xi))\}$, είναι δύσκολο να προβλεφθεί $Yc \approx \Pi(Xc)$ μέχρι ένα μικρό σφάλμα, για Xc μια τυχαία είσοδος που $(xc, \cdot) \in Q$.
6. Μονόδρομος: δίνεται μόνο Y και Π, είναι δύσκολο να βρεθεί το x έτσι ώστε Π(x)=y.
7. Εμφανής παραβίαση: τροποποιώντας την φυσική οντότητα του ενσωματομένου Π μετατρέπεται Π->Π' έτσι ώστε μς υψηλή πιθανότητα $\exists x \in X : \Pi(x)$ διάφορο Π0(x), όχι ακόμα και μέχρι ένα μικρό λάθος.

Με περισσότερες λεπτομέρειες:

1. Το πότε ή όχι ένα PUF είναι αξιολογίσημο μπορεί να ερμηνευθεί σε ευρεία έννοια. Από θεωρητική σκοπιά, εύκολα μπορεί να σημαίνει ότι θέλουμε η αξιολόγηση να είναι εφικτή στα πλαίσια πολιονυμικού χρόνου και προσπάθειας. Από πρακτική σκοπιά, σημαίνει ότι θέλουμε η αξιολόγηση για την πρόκληση να είναι όσο το δυνατόν μικρότερη επιβάρυνση, π.χ. σε κλειστό χρονοδιάγραμμα, περιοχή, δύναμη και ενέργεια περιορισμένη σε ολοκληρομένο. Σημειώνουμε πως αν ένα PUF είναι αξιολογίσημο τότε μπορεί κάποιος να αρχίσει αμέσως να το φτιάχνει. Επίσης εάν η επιβάρυνση της αξιολόγησης είναι πρακτικά εφικτή εξαρτάται και από την εφαρμογή.

2. Σχετικά με την μοναδικότητα, μπορεί να εξακολουθεί να υπάρχει κάποια ασάφεια σχετικά με την έννοια της πληροφορίας και της ταυτότητας. Εάν αναλογιστούμε έναν καλά ορισμένο αριθμό ή σετ από PUF στιγμιοτύπων, οι πληροφορίες που περιέχονται σε μια έξοδο PUF Π(x) αναφέρεται στο μέρος το οποίο μπορεί να φτιάξει βασισμένο στην έξοδο/απάντηση. Διαδοχικές εξόδοι επιτρέπουν για μικρότερα και μικρότερα μέρη του πλυθησμού, μέχρι ένα μέρος με μια μοναδική έξοδο PUF να παραμείνει, και στην οποία περίπτωση το εξεταζόμενο σύνολο από CRPs να αναγνωρίζει το PUF από την μοναδικότητα του μέσα στον πλυθησμό. Αν βασιστούμε στο μέγεθος και τα χαρακτηριστικά μιας PUF εξόδου, μια τέτοια μοναδική αναγνώριση μπορεί να είναι εφικτή μπορεί και όχι. Ένα πιθανό μέτρο της μοναδικότητας, η οποία παρέχεται από πειραματικά αποτελέσματα μεταξύ αποστάσεων ενός ιστογράμματος, συνοψίζεται από τη μέση αξία μinter.

3. Στην επαναληψιμότητα, οι έξοδοι σε διαφορετικές αξιολογήσεις της ίδιας εισόδου x στο ίδιο PUF Π πρέπει να είναι κοντά στην μετρική απόσταση. Για πειραματικά

αποτελέσματα, αυτό μετράται από το intra-distance ιστόγραμμα και συνοψίζεται στην μέση αξία μintra. Η αναπαραγωγισιμότητα είναι η ιδιότητα που διακρίνει τα PUFs από τις αληθινές γεννήτριες τυχαίων αριθμών (TRNGs).

4. Από το ίδιο το όνομα του η μη κλωνοποίηση είναι ο κύριος πυρήνας ενός PUF.
Η παρεχόμενη περιγραφή είναι σχετικά προφανής, ωστόσο υπάρχουν αρκετές λεπτομέρειες που πρέπει να ληφθούν υπόψη. Αρχικά, σημειώστε ότι ο κλώνος Γ περιγράφεται ως μια διαδικασία, όχι απαραίτητα φυσική, δεδομένου ότι υπάρχει διάκριση ανάμεσα στην φυσική και μαθηματική κλωνοποίηση. Αν είναι δύσκολο να καταλήξουμε σε μια φυσική οντότητα που περιέχει ένα άλλο PUF ΠΓ 6 = Π6 έτσι ώστε ∀x: ΠΓ (x) ≈ Π (χ), λέμε ότι είναι φυσικά μη κλωνοποιήσιμη.
Σημειώνουμε ότι η δυσκολία της παραγωγής ενός φυσικού κλώνου ισχύει και για τον κατασκευαστή του αρχικού PUF Π και για αυτό τον λόγο ονομάζεται αντίσταση του κατασκευαστή. Είναι δύσκολο να καταλήξουμε σε μια περίληψη της διαδικασίας fΓ έτσι ώστε ∀x: fΓ (x) ≈ Π (χ), λέγοντας ότι το Π είναι μαθηματικά μη κλωνοποιήσιμο.
Σημειώνουμε ακόμα, ότι η φυσική και μαθηματική μη κλωνοποιησιμότητα είναι διαφορετικές θεμελιώδης ιδιότητες, από τότε που η κατασκευή μπορεί εύκολα να κλωνοποιήσει φυσικά και όχι μαθηματικά ή το αντίστροφο. Προκειμένου να είναι πραγματικά μη κλωνοποίσημα, το Π χρειάζεται να είναι και φυσικά και μαθηματικά μη κλωνοποιήσιμο. Και πάλι η δυσκολία της κλωνοποίησης μπορεί να υπολογιστεί και από θεωρητική και από πρακτική άποψη.
Πρακτικά η κλωνοποίηση μπορεί να είναι δύσκολη ή και ανέφικτη. Αποδεικνύοντας την θεωρητική μη κλωνοποιησιμότητα από την άλλη πλευρά είναι πολύ δύσκολο επίσης. Τα μόνα γνωστά συστήματα που μπορεί να αποδειχτεί ότι είναι θεωρητικά μη κλωνοποιήσιμα είναι βασισμένα σε κβαντική φυσική.

5. Το απρόβλεπτο είναι στην πραγματικότητα μια χαλαρή μορφή της μη κλωνοποιησιμότητας. Αν κάποιος μπορεί να προβλέψει σωστά το αποτέλεσμα ενός PUF για μια τυχαία είσοδο, μόνο παρατηρώντας ένα σύνολο από CRPs, είναι εύκολο να φτιάξει έναν μαθηματικό κλώνο αν έχει πρόσβαση σε όλο το PUF. Ως εκ τούτου, η προβλεψιμότητα προϋποθέτει τη μαθηματική κλωνοποίηση και απλή κλωνοποίηση.

6. Ο μονόδρομος είναι μια κλασσική ιδιότητα προερχόμενη από την κρυπτογραφία. Περιγράφονται ως φυσικές παραλλαγές των μονόδρομων συναρτήσεων.

7. Μια εμφανής παραβίαση είναι όταν αντιλαμβανόμαστε μόνιμες αλλαγές για την ακεραιότητα μια φυσικής οντότητας. Διακρίνουμε ανάμεσα από τις αποδείξεις παραβίασης κάποια συστημάτα, δηλαδή,συστήματα στα οποία η αλλοίωση δεν αφήνει κάποια χρήσιμη πληροφορία και απαραβίαστο σύστημα, δηλ., συστήματα στα οποία η αλλοίωση μπορεί να είναι εφικτή αλλά αφήνει ανεξίτηλα στοιχεία. Καλούμε ένα PUF απαραβίαστο αν η αλλοίωση με φυσικό τρόπο ενσωματώνει το PUF με υψηλές πιθανότητες αλλαγής της συμπεριφοράς του.

3.2.2. ΕΛΕΓΧΟΣ ΑΤΟΜΙΚΩΝ ΙΔΙΟΤΗΤΩΝ

Εδώ θα δούμε προτάσεις PUF ενάντια στις επτά ιδιότητες που είναι αναγνωρισμένες ήδη. Οι προτάσεις που είναι παρακάτω είναι προτεινόμενα φυσικά PUF για τα οποία συγκεκριμένες κατασκευαστικές λεπτομέρειες είναι διαθέσιμες, και επίσης δύο καλά μελετημένα μη φυσικά PUFs.

Για να καταλήξουμε σε κάποια λογικά συμπεράσματα, πρέπει να συγκριθούν κάποιες προτάσεις PUF με κάποιες προτάσεις οι οποίες δεν είναι γνωστές. Ελέγχεται σύμφωνα με τις τρείς ακόλουθες προτάσεις, οι οποίες περιγράφονται σε ένα εισόδου-εξόδου στυλ για εύκολη σύγκριση των PUF:

- Τριών αριθμών τυχαία γεννήτρια. Η μια είσοδος είναι το αίτημα για τον τυχαίο αριθμό. Η έξοδος είναι ένας τυχαίος αριθμός που εξάγεται από μια σχολαστικά φυσική διαδικασία.
- Ένα πολύ απλό RFID πρωτόκολλο αναγνώρισης. Η είσοδος είναι το αίτημα για την αναγνώριση. Η έξοδος είναι μια αναγνωριστική ακολουθία η οποία ήταν δύσκολα προγραμματισμένη στην συσκευή από τον κατασκευαστή.
- Ένα σύστημα δημοσίου κλειδιού υπογραφής. Η είσοδος είναι ένα μήνυμα ακολουθία. Η απάντηση είναι μια υπογραφή σε αυτό το μήνυμα δημιουργημένη χρησιμοποιώντας ένα δημόσιο κλειδί το οποίο ήταν δύσκολα προγραμματισμένο από τον κατασκευαστή της συσκευής.

Tip: Σημειώνουμε πάλι πως υπάρχει ρητή διάκριση ανάμεσα στην φυσική και μαθηματική μη κλωνοποιησιμότητα από τότε που θεωρούνται διαφορετικές έννοιες.

3.2.2.1 ΛΙΓΟΤΕΡΟ ΚΟΙΝΑ ΣΥΝΟΛΑ ΑΠΟ PUF ΠΡΟΤΑΣΕΙΣ

Οι βασικότερες ιδιότητες των PUF είναι η αξιολόγηση και η μοναδικότητα, οι οποίες ισχύουν για όλες τις περιπτώσεις των PUF που έχουν αναφερθεί μέχρι στιγμής οπουδήποτε. Αυτό σημαίνει πως αυτές οι δύο ιδιότητες είναι οι ποιο απαραίτητες για ένα PUF, αλλά δεν είναι επαρκής, δεδομένου ότι επιτρέπουν προγραμματισμένους αναγνωριστές, υπογραφές δημοσίου κλειδιού και TRNGs. Μια τρίτη απαραίτητη ιδιότητα είναι η αναπαραγωγισιμότητα, αποκλείει τα TRNGs. Τέλος, η βασικότερη από όλες τις ιδιότητες της φυσικής μη κλωνοποίησης διακρίνει τις PUF προτάσεις από τις περιπτώσεις αναφοράς βασισμένες πάνω στον δύσκολο προγραμματιζόμενο μοναδικό αναγνωριστικό ή κλειδί.
Παρατηρώντας περισσότερο τις ιδιότητες των PUF και τα αποτέλεσματα τους φένεται πως η μαθηματική μη κλωνοποιησιμότητα είναι ανέφικτη για τα περισσότερα γυμνά PUF, δηλ. για τα PUF τα οποία διαβάζονται εύκολα. Για την βελτίωση της μαθηματικής μη κλωνοποιησιμότητας αυτά τα PUF μπορούν να μετατραπούν σε Controlled PUFs.
Ο μονόδρομος φαίνετε να είναι μια καλή ιδιότητα διότι κανένα PUF δεν είναι στην πραγματικότητα μονόδρομος. Ακόμα και για τα optical PUFs, τα οποία είναι εισαγμένα ως φυσικές ενός δρόμου συναρτήσεις, αυτή η ιδιότητα είναι ασαφής. Τέλος, αν και ευρέως πιστεύεται ότι είναι ένα από τα κύρια πλεονεκτήματα της τεχνολογίας PUF, η εμφανής παραβίαση είναι μόνο πειραματικά εξακριβομένη για τα μη φυσικά και επικαλυμένα PUFs.

3.2.2.2 ΠΡΟΒΛΕΨΙΜΟΤΗΤΑ ΕΝΑΝΤΙΑ ΤΟΥ ΜΕΓΕΘΟΥΣ ΕΦΑΡΜΟΓΗΣ

Γενικότερα, από τα στοιχεία που έχουμε στα χέρια μας μέχρι στιγμής, είναι σαφές ότι κάποια συγκεκριμένα PUFs υποφέρουν από προβλεψιμότητα κατά τις επιθέσεις δημιουργίας ενός συστήματος, μετά από έναν σχετικά μικρό αριθμό από CRPs που έχουν παρατηρηθεί. Ποιο συγκεκριμένα αυτή η περίπτωση αφορά τα βασισμένα στην καθυστέρηση PUFs όπως τα PUF κριτές, αν και τα περισσότερα PUF τα οποία είναι βασισμένα στην μνήμη θεωρούνται εύλογα ότι αντέχουν τις επιθέσεις δημιουργίας συστήματος, δεδομένου ότι οι εξόδοι τους βασίζονται σε ανεξάρτητα τυχαία στοιχεία.

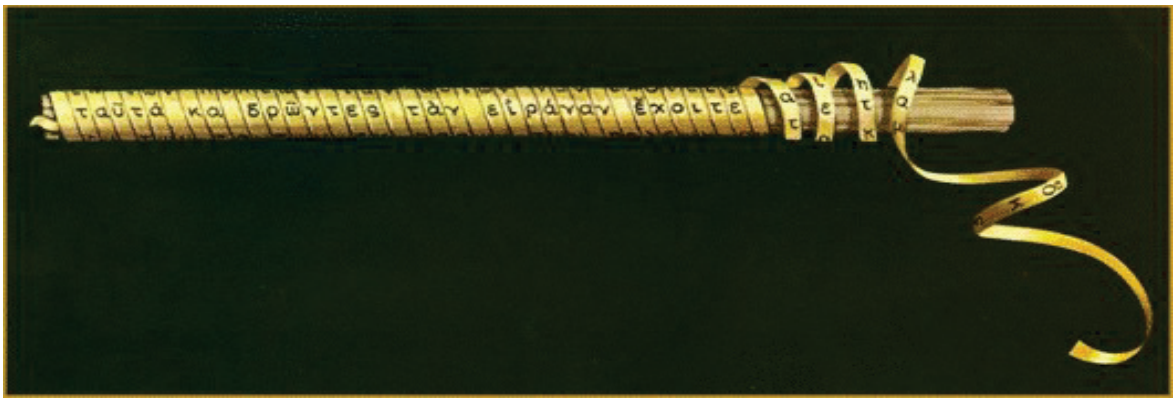
Από την άλλη μεριά, όλα τα PUFs που είναι βασισμένα στην μνήμη, όπως επίσης και εκείνα τα PUFs όπως π.χ. δαχτυλίδια ταλαντωτές PUFs, χρησιμοποιούνται από ένα άλλο μειονέκτημα. Το μέγεθος εφαρμογής τους αυξάνεται εκθετικά ανάλογα με το επιθυμητό μήκος των εισόδων τους. Με άλλα λόγια για αυτά τα PUFs ο αριθμός των πιθανών ικανοτήτων των CRPs κλιμακώνεται γραμμικά ανάλογα με το μέγεθος τους, ενώ για τον PUF κριτή αυτές οι ικανότητες κλιμακώνονται εκθετικά. Αυτό σημαίνει ότι για τους δύο τύπους των ψηφιακών εγγενών PUFs, ο αριθμός των απρόβλεπτων CRPs είναι περιορισμένος σε μια ποσότητα η οποία είναι πολυονυμική στο μέγεθος των PUFs. Για τα PUF τα οποία είναι παρεμφερές με τα PUF κριτές, ο περιορισμός αυτός οφείλεται στις επιθέσεις δημιουργίας συστήματος, ενώ για τα PUFs που είναι βασισμένα στην μνήμη οφείλεται λόγω του περιορισμένου αριθμού των διαθέσιμων CRPs.

Αυτή είναι μια παράξενη παρατήρηση, δεδομένου ότι δεν είναι σαφές κατά πόσον αυτό είναι ένα σημάδι ενός υποκείμενου φυσικού ορίου στον αριθμό των απρόβλεπτων CRPs, που μπορεί να ληφθεί για οποιοδήποτε εσωτερικό/εγγενή PUF, ή αν αυτό είναι απλώς ένα αποτέλεσμα των συγκεκριμένων κατασκευών PUF που έχουν προταθεί μέχρι στιγμής. Επιπλέον, περιορίζει τα πιθανά σενάρια εφαρμογής, δεδομένου ότι αποτελεί αναπόσπαστο PUF με ένα υπερ-γραμμικό ή ακόμα και ένα εκθετικό ποσό των απρόβλεπτων CRPs που θα μπορούσε να οδηγήσει σε ισχυρότερες υποθέσεις ασφαλείας.

Από φυσική άποψη, θα μπορούσε κανείς να πει ότι επειδή το ποσό της εντροπίας (θερμοδυναμική) σε ένα φυσικό σύστημα είναι το καλύτερο πολυονυμικό στο μέγεθος του συστήματος, ο αριθμός των πραγματικά ανεξαρτήτων CRPs για ένα μοναδικό PUF δεν μπορεί ποτέ να γίνει εκθετικός στο μέγεθος του PUF. Ωστόσο, για πολλές εφαρμογές κρυπτογράφησης στοχεύουμε για υπολογιστικά και όχι τέλεια μέτρα ασφαλείας, δηλαδή ακόμα και αν η πραγματική περιεκτικότητα εντροπίας περιορίζεται, θα μπορούσε ακόμα να υπάρχει ένας μεγάλος αριθμός από υπολογιστικά απρόβλεπτα CRPs. Με άλλα λόγια η δημιουργία ενός συστήματος θα μπορούσε να είναι δυνατή στην θεωρία αλλά σχεδόν μη εκτελέσιμη στην πράξη. Δεν συνιστάται περαιτέρω ανάλυση και από θεωρητική και από πρακτική άποψη.

ΚΕΦΑΛΑΙΟ 4

ΑΣΦΑΛΕΙΑ



Γενικότερα, η ασφάλεια στους υπολογιστές σχετίζεται με ένα πλήθος γνωστικών αντικειμένων, θεωριών και τεχνολογιών που σκοπό έχουν, την πρόβλεψη, ανίχνευση, και την αντιμετώπιση μη εξουσιοδοτημένων πράξεων, οι οποίες σχετίζονται με τις ενέργειες υπολογιστικών συστημάτων.
Ο ρόλος του Η/Υ κατά την εκτέλεση των μη εξουσιοδοτημένων πράξεων συνήθως είναι διπλός:

1. Αποτελεί βασικό εργαλείο (αλλά όχι πάντα αποκλειστικό) για την τέλεση τους
2. Ο ίδιος ο Η/Υ (και συγκεκριμένα τα δεδομένα ή/και οι πληροφορίες που περιέχονται ή δημιουργούνται σε αυτόν) αποτελεί στόχο των πράξεων αυτών.

Οι μη εξουσιοδοτημένες πράξεις, ανάλογα με τις συνέπειες τους μπορούν να αποτελούν ή όχι ένα Ηλεκτρονικό Έγκλημα (e-crime, computer crime). Οι [Forester and Morrison, 1994] ορίζουν το Ηλεκτρονικό Έγκλημα ως:
«Μία εγκληματική πράξη κατά την τέλεση της οποίας ο Η/Υ αποτελεί το βασικό εργαλείο».

Η Ασφάλεια Υπολογιστών χρησιμοποιεί (χωρίς να περιορίζεται από) τη γνώση που πηγάζει από τη μελέτη αρκετών γνωστικών χώρων, όχι απαραίτητα αλληλοσυσχετιζόμενων, όπως Πληροφορική, Κρυπτογραφία και Κοινωνικές Επιστήμες. Συγκεκριμένα:

- **Πληροφορική Ανάπτυξη λογισμικού**
  Η γνώση βασικών τεχνικών προγραμματισμού κρίνεται απαραίτητη για την αντιμετώπιση των «εχθρών» του συστήματος (hackers, crackers κ.λ.π) οι οποίοι παράγουν κακόβουλο κώδικα με σκοπό τη μη εξουσιοδοτημένη πρόσβαση στους πόρους του συστήματος ή εκμεταλλεύονται λάθη στον κώδικα των εφαρμογών του χρήστη-συστήματος. Διαχείριση Δικτύων-Internet & Τεχνολογίες Υλικού. Η κατανόηση των ηλεκτρονικών διατάξεων, των

δικτυακών υποδομών, καθώς και των υπηρεσιών που τις χρησιμοποιούν (λογισμικό δικτύου, δικτυακές εφαρμογές και υπηρεσίες Internet, αρχιτεκτονικές πρωτόκολλων, κ.λ.π) είναι σημαντική για την διεκπερέωση τους.

- **Κρυπτογραφία**
  Η επιστήμη που ασχολείται με την προστασία της εμπιστευτικότητας, της αυθεντικότητας και της ακεραιότητας των δεδομένων και πληροφοριών κατά την αποθήκευση ή/και μεταφορά τους μεταξύ υπολογιστικών διατάξεων. Η κρυπτογραφία χρησιμοποιεί (χωρίς να περιορίζεται από) στοιχεία θεωρίας πληροφοριών (Information theory), μαθηματικά μοντέλα και στοιχεία θεωρίας γραμμικής άλγεβρας (linear algebra), θεωρίας αριθμών (number theory) κ.α., για το σχεδιασμό τεχνικών προστασίας των δεδομένων.
- **Κοινωνικές Επιστήμες Διοίκηση Ανθρώπινων Πόρων & Ψυχολογία.**
  Η ασφάλεια αξιοποιεί βασικές γνώσεις της θεωρίας της ψυχολογίας (π.χ. προφίλ επιτιθέμενου & αμυνόμενου).
- **Δίκαιο και Ηθική του Κυβερνοχώρου**
  Η νομοθεσία αποτελεί ίσως το σημαντικότερο μη τεχνικό (non-technical) μέσο για την πρόληψη επιθέσεων στην ασφάλεια Η/Υ. Ωστόσο, ζητήματα όπως η ανωνυμία των χρηστών, η ελευθερία έκφρασης και η προστασία των πνευματικών δικαιωμάτων σχετίζονται σε μεγάλο βαθμό και με την αποκαλούμενη ως Ηθική του Κυβερνοχώρου (Cyber Ethics).
- **Ιστορία**
  Η μελέτη των γεγονότων (στα στρατιωτικά και διπλωματικά μέτωπα) κατά τους Α' και Β' Παγκόσμιους πολέμους (κώδικες, επιθέσεις σε συστήματα κρυπτογράφησης επικοινωνιών) καθώς και η γνώση που απορρέει από τη μελέτη περιπτώσεων παραβίασης συστημάτων Η/Υ και επικοινωνιών από τα μέσα της δεκαετίας του 1980 και μετά (δημιουργία και εξάπλωση κακόβουλου λογισμικού

Εμείς πιο συγκεκριμένα θα ασχοληθούμε με την κρυπτογραφία και θα μπορούσαμε να πούμε και ένα παρακλάδι της, την ασφάλεια του υλικού υπολογιστικών συστημάτων. Κατά την γνώμη μου όμως, χρόνο με τον χρόνο αυτό το παρακλάδι έχει αρχίσει και γίνεται "κατά κάποιο τρόπο" βέβαια, ανεξάρτητος και σε λίγα χρόνια θα αποτελεί έναν κλάδο μόνο του.

4.1. ΚΡΥΠΤΟΓΡΑΦΙΑ

Η Κρυπτογραφία είναι ο επιστημονικός κλάδος που ασχολείται με την μελέτη, ανάπτυξη και χρήση τεχνικών με σκοπό την ασφαλή επικοινωνία μεταξύ συνομιλητών, ενώ ταυτόχρονα υπάρχουν τρίτοι ενδιαφερόμενοι («αντίπαλοι» - adversaries) για τα περιεχόμενα αυτής της επικοινωνίας, οι οποίοι πρέπει να αποκλειστούν από το να αποκτήσουν αυτά τα περιεχόμενα. Πρακτικά, ασχολείται με την δημιουργία και ανάλυση αλγορίθμων και πρωτοκόλλων τα οποία υπερνικούν την επιρροή των «αντιπάλων» και τα οποία έχουν στόχο την παροχή διαφόρων εννοιών του κλάδου της ασφάλειας της πληροφορίας, όπως η εμπιστευτικότητα, η ακεραιότητα των δεδομένων, η πιστοποίηση και η μη-απάρνηση. Η μοντέρνα κρυπτογραφία έχει στενή σχέση με τους κλάδους των μαθηματικών, της επιστήμης των υπολογιστών και της ηλεκτρολογίας (electrical engineering).

Βασικές έννοιες αυτού του κλάδου είναι (το γνωστό φυσικά CIA):

- Εμπιστευτικότητα (Confidentiality), κατά την οποία εξασφαλίζεται ότι περιορισμένες και σαφώς καθορισμένες οντότητες μπορούν να έχουν πρόσβαση σε ένα σύνολο πληροφοριών, και καμία άλλη.
- Πιστοποίηση (Authentication), είναι η διαδικασία κατά την οποία εξασφαλίζεται η αληθινή ταυτότητα ή κάποια άλλη ιδιότητα μίας οντότητας.
- Ακεραιότητα Δεδομένων (Data Integrity), κατά την οποία εξασφαλίζεται ότι το υπό εξέταση σύνολο δεδομένων δεν έχει παραποιηθεί από μη εξουσιοδοτημένες οντότητες, και ότι κάθε παραποίηση τους θα γίνει αντιληπτή.
- Μη απάρνηση(Non-repudiation), Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της

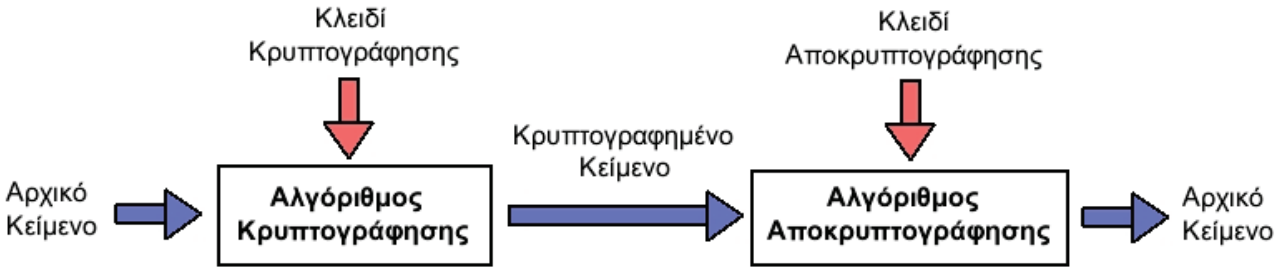
Χρήσιμοι ορισμοί:

- Κρυπτογράφηση (encryption), ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με τη χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη.
- Η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα ονομάζεται αποκρυπτογράφηση (decryption).
- Κρυπτογραφικός αλγόριθμος (cipher), είναι η μέθοδος μετασχηματισμού δεδομένων σε μία μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος πολύπλοκη μαθηματική συνάρτηση.
- Αρχικό κείμενο (plaintext), είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.
- Κλειδί (key), είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στη συνάρτηση κρυπτογράφησης.

- Κρυπτογραφημένο κείμενο (ciphertext), είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.
- Κρυπτανάλυση (cryptanalysis), είναι μία επιστήμη που ασχολείται με το "σπάσιμο" κάποιας κρυπτογραφικής τεχνικής ούτως ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί.

4.1.1. ΚΡΥΠΤΟΓΡΑΦΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ

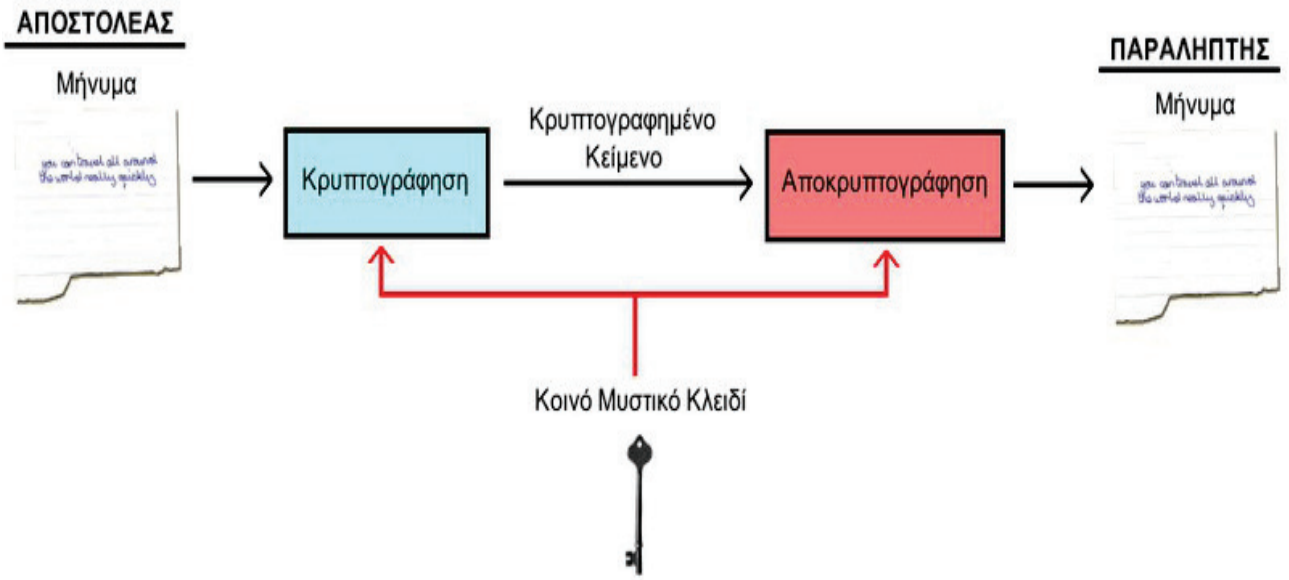
Οι κρυπτογραφικοί αλγόριθμοι, είναι αλγόριθμοι οι οποίοι παρέχουν κάποια/ες από τις βασικές έννοιες της κρυπτογραφίας. Αποτελούν την βάση κάθε ασφαλούς συστήματος και για αυτό θα πρέπει να δίνεται ιδιαίτερη προσοχή στην αποτελεσματικότητα τους, τόσο στον σχεδιασμό, όσο και στην υλοποίηση και την διασύνδεση τους με άλλους αλγορίθμους, πρωτόκολλα και συστήματα. Υπάρχουν διαφόρων ειδών κρυπτογραφικοί αλγόριθμοι, όπως αλγόριθμοι που παρέχουν κρυπτογράφηση δεδομένων (encryption), κατακερματισμού(hash) τους, απόκρυψης του γεγονότος ότι υπάρχουν εμπιστευτικά δεδομένα (plausible deniability, deniable encryption) και στεγανογραφίας (steganography), δηλαδή απόκρυψης και ενσωμάτωσης των σημαντικών δεδομένων σε άλλα, ασήμαντα και άσχετα.



4.1.1.1 ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Η κρυπτογράφηση είναι ένας μετασχηματισμός ενός συνόλου δεδομένων σε ένα άλλο, με στόχο την ασφάλιση αυτών των δεδομένων από την πρόσβαση τρίτων σε αυτά, δηλαδή με στόχο την παροχή εμπιστευτικότητας. Το αρχικά δεδομένα ονομάζονται καθαρό κείμενο (plaintext) ενώ τα δεδομένα που προκύπτουν μετά από την κρυπτογράφηση καλούνται κρυπτογραφημένο κείμενο (ciphertext). Ο ανάποδος μετασχηματισμός, ονομάζεται αποκρυπτογράφηση. Η μοντέρνα κρυπτογραφία χρησιμοποιεί κλειδιά (cryptographic keys) για την απόκρυπτογράφηση. Τα κλειδιά είναι ένας τρόπος παραμετροποίησης του αλγόριθμου κρυπτογράφησης και είναι απαραίτητα για να μπορεί να αποκρυπτογραφηθεί το μήνυμα. Με αυτόν τον τρόπο, η ασφάλεια των δεδομένων δεν εξαρτάται από το πόσο καλά κρατήθηκε κρυφός ο αλγόριθμος, και ακόμη, δεν υπάρχει ανάγκη εύρεσης καινούριου αλγορίθμου, όταν ο

ήδη χρησιμοποιούμενος γίνει γνωστός από τρίτους, και αρκεί μόνο η προστασία των κλειδιών. Υπάρχουν δύο βασικά είδη κρυπτογράφησης, η συμμετρική (symmetric encryption) και η ασύμμετρη (public key encryption). Στην συμμετρική κρυπτογράφηση, χρησιμοποιείται ένα κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Ο αποστολέας κρυπτογραφεί με 11 την χρήση του κλειδιού, το οποίο και παρέχει με κάποιον ασφαλή τρόπο στους επιθυμητούς παραλήπτες, οι οποίοι με την σειρά τους το χρησιμοποιούν για να αποκρυπτογραφήσουν.
Στην συμμετρική κρυπτογράφηση υπάρχουν δύο κατηγορίες αλγορίθμων, οι αλγόριθμοι δέσμης (block ciphers) και οι αλγόριθμοι ροής (stream ciphers). Οι αλγόριθμοι της πρώτης κατηγορίας αποκρυπτογραφούν το μήνυμα σε ισομεγέθη κομμάτια (blocks) ενώ της δεύτερης bit προς bit ή byte προς byte. Έτσι οι πρώτοι μπορούν να εφαρμοστούν όταν έχουμε όλα τα δεδομένα διαθέσιμα εκ' των προτέρων, ενώ οι δεύτεροι χρησιμοποιούνται όταν τα δεδομένα πρέπει να κρυπτογραφηθούν την στιγμή που παράγονται (on-the-fly).



Για τους αλγόριθμους δέσμης ορίζονται τρόποι λειτουργίας (operation modes), οι οποίοι περιγράφουν τον τρόπο της επαναλαμβανόμενης εφαρμογής ενός block αλγορίθμου σε δεδομένα εισόδου μεγαλύτερα από το μέγεθος του block. Όταν η είσοδος δεν είναι ακέραιο πολλαπλάσιο του μεγέθους του block που ορίζει ο αλγόριθμος, τότε πρέπει να χρησιμοποιηθεί «γέμισμα» της εισόδου (padding), ώστε να φτάσει στο κατάλληλο μέγεθος, και έπειτα το επεκταμένο κείμενο δίνεται ως είσοδος στον αλγόριθμο. Ο τρόπος και τα περιεχόμενα της διαδικασίας του «γεμίσματος» δίνονται συνήθως στην προδιαγραφή (specification) του αλγορίθμου.

Πλεονεκτήματα:

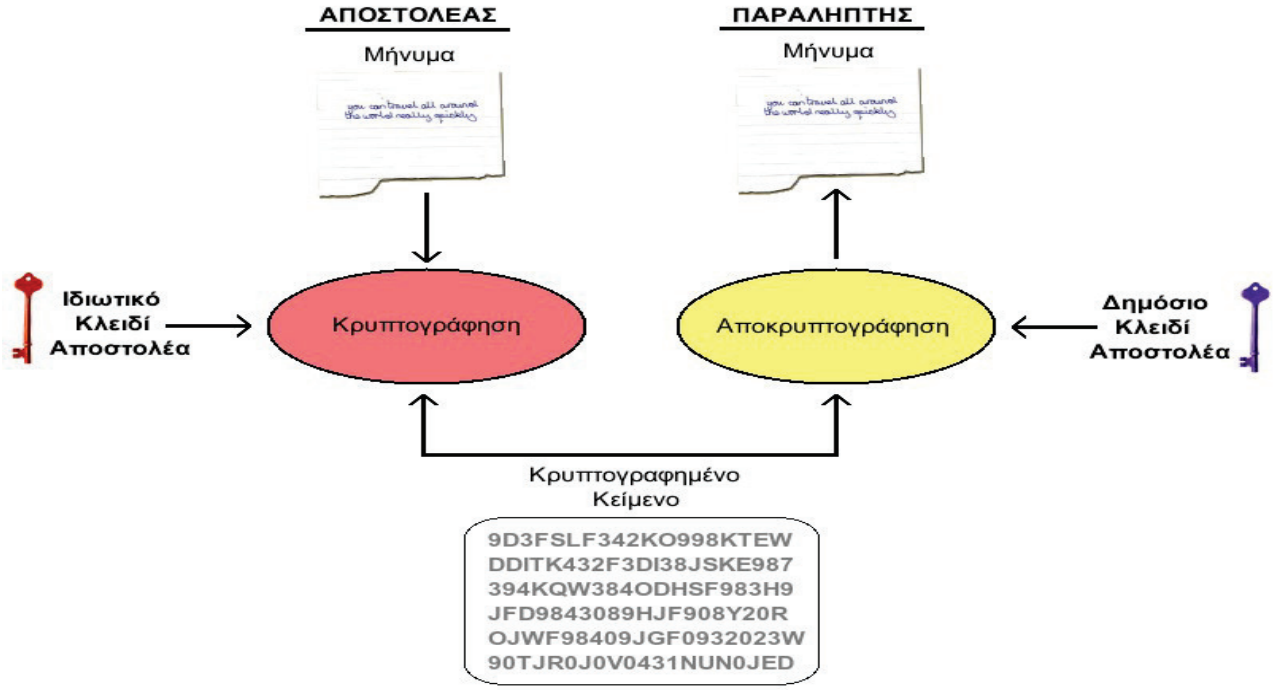
1) Πολύ γρήγορη κρυπτογράφηση.
2) Μέγεθος κλειδιών μικρό (συσκευές περιορισμένων πόρων).
3) Δημιουργία γεννητριών τυχαίων αριθμών και συναρτήσεων κατακερματισμού.
4) Συνδυασμοί τους παράγουν ισχυρότερους αλγορίθμους.
5) Είναι αρκετά δοκιμασμένα στην πράξη.

Μειονεκτήματα:

1) Απαιτείται ασφαλής δίαυλος επικοινωνίας για την ανταλλαγή κλειδιών.
2) Πολλά κλειδιά (n(n-1)/2).
3) Ύπαρξη άνευ όρων έμπιστου TTP (διαχείριση κλειδιών).
4) Συχνή αλλαγή κλειδιών.
5) Ψηφιακές υπογραφές απαιτούν μεγάλα κλειδιά ή την ύπαρξη TTP.

4.1.1.2 ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Στην ασύμμετρη κρυπτογράφηση(asymmetric cryptography, public-key cryptography), χρησιμοποιούνται δύο κλειδιά από κάθε οντότητα, ένα δημόσιο (public key) και ένα ιδιωτικό (private key). Το δημόσιο κλειδί διατίθεται σε οποιονδήποτε ενώ το ιδιωτικό πρέπει να κρατηθεί κρυφό. Αυτά τα κλειδιά έχουν την ιδιότητα να μπορούν να αποκρυπτογραφήσουν ότι έχει κρυπτογραφηθεί με το άλλο κλειδί, αμοιβαία.Ακόμη, έχουν την ιδιότητα ότι δεδομένου του δημόσιου κλειδιού, είναι πρακτικά αδύνατο να βρεθεί το ιδιωτικό. Οι ασύμμετροι αλγόριθμοι έχουν δύο βασικούς τρόπους χρήσης. Ο ένας παρέχει εμπιστευτικότητα ενώ ο άλλος πιστοποίηση. Όταν μια οντότητα θέλει να χρησιμοποιήσει εμπιστευτικότητα με μια άλλη, χρησιμοποιεί το δημόσιο κλειδί της δεύτερης για την κρυπτογράφηση των δεδομένων. Οπότε, η μόνη οντότητα που μπορεί να έχει πρόσβαση στο καθαρό κείμενο είναι αυτή που κατέχει το αντίστοιχο ιδιωτικό κλειδί, δηλαδή η δεύτερη (ιδανικά).



Για την επίτευξη πιστοποίησης, ο δημιουργός ή αποστολέας της πληροφορίας, χρησιμοποιεί το ιδιωτικό του κλειδί στα δεδομένα, και παράγει μία έξοδο, η οποία ονομάζεται υπογραφή (signature), η οποία είναι πολύ δύσκολο να πλαστογραφηθεί.

Όταν τα δεδομένα φτάσουν σε κάποιον παραλήπτη, αυτός μπορεί να ελέγξει την υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα.
Οι ασύμμετροι αλγόριθμοι χρησιμοποιούνται εφαρμογές όπως ψηφιακά πιστοποιητικά, σε πρωτόκολλα ασφαλούς ανταλλαγής κλειδιών (πχ Diffie-Hellman) στο πρωτόκολλο TLS(Transport Layer Security) κ.α.

Πλεονεκτήματα:

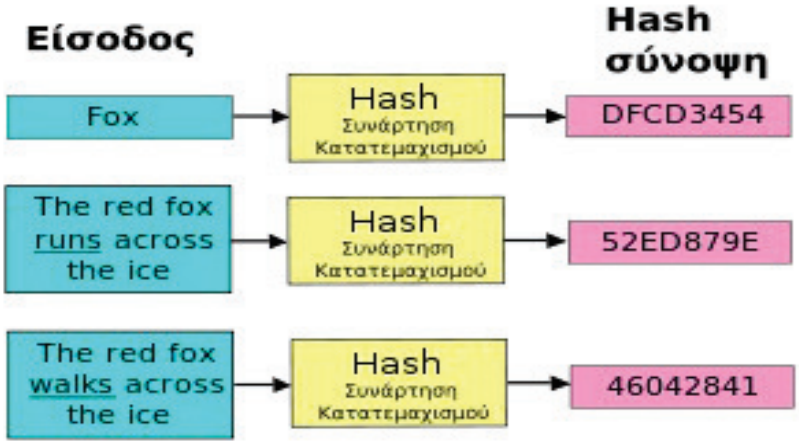
1) Δεν απαιτείται ασφαλής δίαυλος επικοινωνίας.
2) Τα κλειδιά δεν αλλάζουν συχνά.
3) Αλγόριθμοι ψηφιακών υπογραφών πολύ πιο αποδοτικοί.
4) Πλήθος κλειδιών σε δίκτυο n χρηστών μικρός.
5) Για τη διαχείριση των κλειδιών απαιτείται ένα λειτουργικά έμπιστο TTP(Trusted Third Party).

Μειονεκτήματα:

1) Ταχύτητα κρυπτογράφησης – αποκρυπτογράφησης πιο αργή.
2) Κλειδιά σχετικά μεγάλα.
3) Δεν έχουν δοκιμαστεί στην πράξη όσο τα συμμετρικά.
4) Βασίζονται σε προβλήματα θεωρίας αριθμών, των οποίων η δυσκολία δεν έχει αποδειχθεί θεωρητικά.

4.1.1.3 ΑΛΓΟΡΙΘΜΟΙ ΚΑΤΑΚΕΡΜΑΤΙΣΜΟΥ

Αλγόριθμος κατακερματισμού (hash algorithm) είναι ένας ντετερμινιστικός αλγόριθμος ο οποίος αντιστοιχεί δεδομένα μεταβλητού μεγέθους σε δεδομένα προκαθορισμένου μεγέθους (hash, digest). Λόγω του περιορισμένου αριθμού πιθανών εξόδων σε σχέση με τον απεριόριστο αριθμό πιθανών εισόδων, οι αλγόριθμοι κατακερματισμού έχουν συγκρούσεις (collisions), δηλαδή υπάρχουν παραπάνω από μία είσοδοι που παράγουν την ίδια έξοδο.



Στην κρυπτογραφία χρησιμοποιούνται οι κρυπτογραφικοί αλγόριθμοι

κατακερματισμού (cryptographic hash functions). Οι αλγόριθμοι αυτού του είδους έχουν επιπρόσθετες απαιτήσεις:

- Δυσκολία εύρεσης μιας εισόδου που παράγει συγκεκριμένη έξοδο
- Δυσκολία αλλαγής της εισόδου, με την έξοδο να παραμένει ίδια
- Δυσκολία εύρεσης δύο εισόδων που να παράγουν την ίδια έξοδο

Όσο μεγαλύτερος είναι ο βαθμός των παραπάνω δυσκολιών, τόσο πιο ασφαλής είναι ο αλγόριθμος. Οι κρυπτογραφικοί αλγόριθμοι κατακερματισμού χρησιμοποιούνται κυρίως για πιστοποίηση και ακεραιότητα των δεδομένων. Γνωστά παραδείγματα είναι οι MD5, RIPEMD και SHA.

4.1.1.4 ΚΑΤΑΚΕΡΜΑΤΙΣΜΟΣ ΜΕ ΚΛΕΙΔΙ

Για την διασφάλιση ακεραιότητας και πιστοποίησης, χρησιμοποιούνται συχνά οι κώδικες πιστοποίησης μηνυμάτων (Message Authentication Code – MAC). Οι MAC είναι ένα μικρό κομμάτι πληροφορίας, το οποίο στέλνεται μαζί με το μήνυμα που θέλουμε να προστατέψουμε, ώστε να ελεγχθεί κατά την παραλαβή του. Για την παραγωγή MAC, χρησιμοποιούνται πολύ συχνά κρυπτογραφικοί αλγόριθμοι κατακερματισμού σε συνδυασμό με ένα κλειδί (Hashed-based MAC – HMAC), το οποίο είναι στην κατοχή μόνο των δύο άκρων της επικοινωνίας. Οποιοσδήποτε κρυπτογραφικός αλγόριθμος κατακερματισμού, όπως οι SHA-1 και MD5, μπορεί να χρησιμοποιηθεί για τον υπολογισμό ενός HMAC, και ο προκύπτων αλγόριθμος ονομάζεται HMAC-MD5 και HMAC-SHA-1 αντίστοιχα.

4.1.1.5 ΓΕΝΝΗΤΡΙΕΣ ΨΕΥΔΟΤΥΧΑΙΩΝ ΑΡΙΘΜΩΝ

Οι γεννήτριες παραγωγής ψευδοτυχαίων αριθμών (Random Number Generator – RNG) είναι αλγόριθμοι που παράγουν ακολουθίες αριθμών, οι οποίες φαίνονται να είναι τυχαίες. Στην πραγματικότητα οι ακολουθίες δεν είναι τυχαίες αλλά προκύπτουν πρότυπα και επαναλήψεις των ακολουθιών. Συνήθως αυτοί οι αλγόριθμοι δέχονται και μια ακόμη είσοδο που ονομάζεται «σπόρος» (seed), και αποτελεί μια παραμετροποίηση των ακολουθιών εξόδου της γεννήτριας. Οι RNG χρησιμοποιούνται στην κρυπτογραφία, όταν χρειάζεται τυχαιότητα για να εξασφαλιστεί ή να ενισχυθεί η ασφάλεια ενός συστήματος. Παραδείγματα είναι η δημιουργία κρυπτογραφικών κλειδιών, διανυσμάτων αρχικοποίησης κ.α.

4.1.2 ΔΙΑΧΕΙΡΗΣΗ ΚΛΕΙΔΙΩΝ (KEY MANAGEMENT)

Η διαχείριση κλειδιών περιλαμβάνει την δημιουργία, τον διαμοιρασμό-ανταλλαγή τους, την αποθήκευση τους και την αντικατάσταση τους. Η διαχείριση των κλειδιών είναι μία κρίσιμη διαδικασία για την ασφάλεια του συστήματος, και στην πράξη η πιο δύσκολη στην εφαρμογή της, αφού περιλαμβάνει θέματα πολιτικών (policies) και διαφόρων άλλων εξωτερικών παραγόντων.

Πριν ξεκινήσει μια ασφαλής επικοινωνία, οι οντότητες θα πρέπει πρώτα να ορίσουν τις παραμέτρους της επικοινωνίας αυτής. Κάποιες φορές απαιτείται η ανταλλαγή κλειδιών. Στην περίπτωση της ασύμμετρης κρυπτογραφίας, διανέμεται το δημόσιο κλειδί ελεύθερα. Στην επικοινωνία με συμμετρική κρυπτογράφηση όμως, χρειάζεται να διανεμηθούν τα κρυφά κλειδιά. Επειδή η γνώση ενός κρυφού κλειδιού εκθέτει την ασφάλεια της επικοινωνίας, αυτά τα κλειδιά θα πρέπει να διανεμηθούν μέσω ενός ασφαλούς καναλιού επικοινωνίας. Για αυτό τον λόγο έχουν αναπτυχθεί διάφορα πρωτόκολλα ασφαλούς ανταλλαγής κλειδιών, με πιο γνωστό την ανταλλαγή Diffie-Hellman.
Τα κλειδιά πρέπει να έχουν κύκλο ζωής, δηλαδή να αντικαθιστούνται περιοδικά. Αυτό γιατί μπορεί να υπάρξει διαρροή των κλειδιών είτε να είναι αποτέλεσμα κρυπτανάλυσης. Η περιοδική αντικατάσταση τους, ελαχιστοποιεί το μέγεθος των επιπτώσεων, αφού ακόμα και να γίνει γνωστό ένα κλειδί, δεν αρκεί για να αποκρυπτογραφηθεί ολόκληρη η επικοινωνία. Επιπρόσθετα, βάζει ακόμα έναν βαθμό δυσκολίας στους κακόβουλους χρήστες του καναλιού, αφού περιορίζει το μέγεθος της κίνησης που κρυπτογραφήθηκε με το ίδιο κλειδί, μειώνοντας έτσι τα διαθέσιμα δεδομένα για κρυπτανάλυση.

Δ***ημιουργία κλειδιού:*** Ένα κλειδί πρέπει να ανθίσταται σε επιθέσεις λεξικού (dictionary attack). Ένα «ισχυρό» κλειδί αποτελείται από μια «τυχαία» συμβολοσειρά bit, που δημιουργείται από μια αυτοματοποιημένη διαδικασία (γεννήτορας) παραγωγής ψευδο-τυχαίων αριθμών (pseudo-randomness generator). Κάθε bit ενός κλειδιού πρέπει να είναι εξίσου πιθανό.

Μήκος κλειδιού: Ο μόνος τρόπος να παραβιαστεί ένας "ισχυρός" κρυπτογραφικός αλγόριθμος, είναι η αποκαλούμενη και ως επίθεση ωμής βίας (btute-force). Σε αυτήν την επίθεση, ο Mallory δοκιμάζει όλα τα πιθανά κλειδιά ώστε να βρει κάποιο που ταιριάζει με το κλειδί που χρησιμοποιήθηκε κατά την κρυπτογράφηση. Για να εξαπολύσει αυτού του είδους την επίθεση, ο κρυπταναλυτής πρέπει πρώτα να υποκλέψει ένα κρυπτογράφημα Η πολυπλοκότητα της επίθεσης υπολογίζεται ως εξής. Εαν το κλειδί έχει μήκος 8 bits, τότε υπάρχουν 28 , ή 256 πιθανά κλειδιά. Επομένως, θα χρειαστούν 256 προσπάθειες προκειμένου να βρεθεί το σωστό κλειδί, με πιθανότητα 50% να βρεθεί το κλειδί μετά τις μισές προσπάθειες. Οι χρόνοι μπορούν να συντομευθούν με κατανεμημένη επεξεργασία. Αν το κλειδί έχει μήκος 128 bit, τότε ο κρυπταναλυτής θα πρέπει να δοκιμάσει κατά μέσο όρο 2127 κλειδιά, πριν βρει το σωστό. Η επίθεση αυτή είναι πρακτικώς αδύνατη.

Σημείωση: Σε έναν συμμετρικό αλγόριθμο, το ελάχιστα αποδεκτό μήκος κλειδιού είναι 128 bit. Σε έναν αλγόριθμο δημόσιου κλειδιού, το ελάχιστα αποδεκτό μήκος κλειδιού είναι 1024 bit.

Ανταλλαγή κλειδιού: Σε μεγάλα ιδίως δίκτυα, ο τρόπος με τον οποίο τα

κλειδιά μεταφέρονται ή τίθενται υπό διαπραγμάτευση μεταξύ των χρηστών, πρέπει να είναι ασφαλής. Έχουν προταθεί πολλά πρωτόκολλα ανταλλαγής κλειδιών (π.χ Diffie Hellman), η επιλογή ενός εκ των οποίων πρέπει να γίνεται με μεγάλη προσοχή.

Αποθήκευση: Ένα μυστικό (ιδιωτικό) κλειδί πρέπει να φυλάσσεται σε ασφαλές σημείο. Για παράδειγμα, η φύλαξη του σε φορητό αποθηκευτικό μέσο ή στο σκληρό δίσκο ενός Η/Υ θα πρέπει να συνεπικουρείται από μηχανισμούς ταυτοποίησης χρήστη (κωδικός πρόσβασης ή/και βιομετρικά συστήματα). Το πλέον ενδεδειγμένο από τη σκοπιά της ασφάλειας σημείο φύλαξης ενός κλειδιού είναι μια έξυπνη κάρτα (smart card): η πρόσβαση στο κλειδί ελέγχεται με τη χρήση κωδικού PIN ή/και με βιομετρικά αποτυπώματα. Η κάρτα μπορεί επίσης να φέρει το ψηφιακό πιστοποιητικό του κλειδιού και να εκτελεί το λογισμικό κρυπτογράφησης-αποκρυπτογράφησης καθώς και ψηφιακής υπογραφής για λογαριασμό του κατόχου της. Σε μια τέτοια περίπτωση η κάρτα μπορεί να χρησιμοποιηθεί σε οποιοδήποτε τερματικό διαθέτει αναγνώστη έξυπνων καρτών. 88 Έξυπνες Κάρτες

Ανανέωση - Ανάκληση κλειδιού:
Όσο αυξάνεται το μέγεθος και ο αριθμός των επικοινωνιών που προστατεύονται από ένα κρυπτογραφικό κλειδί, τόσο αυξάνεται ο κίνδυνος κρυπτανάλυσης του κλειδιού. Επομένως ένα κλειδί θα πρέπει να έχει συγκεκριμένη διάρκεια ζωής. Ανά τακτά χρονικά διαστήματα, ένα κλειδί θα πρέπει να ανανεώνεται (key update). Σε συμμετρικά συστήματα, ένα κλειδί επιβάλλεται να αλλάζει κάθε φορά που ολοκληρώνεται η επικοινωνία (session). Σε συστήματα δημόσιου κλειδιού, ένα κλειδί πρέπει να ανανεώνεται-ανακαλείται όταν εκπνεύσει η περίοδος ισχύος που αναγράφεται στο ψηφιακό πιστοποιητικό, ή σε περίπτωση κλοπής του.

4.2. ΑΣΦΑΛΕΙΑ ΥΛΙΚΟΥ

Η ασφάλεια υλικού έχει να κάνει με την δημιουργία συστημάτων και το να παραμείνουν αξιόπιστα απέναντι στην παραχάραξη, τα σφάλματα και τα λάθη. Ως μέσο πειθαρχίας εστιάζει στα εργαλεία, τις διαδικασίες και τις μεθόδους που χρειάζονται για τον σχεδιασμό, την εφαρμογή και τον πλήρη έλεγχο των συστημάτων, και επίσης προσαρμόζει τα υπάρχοντα συστήματα στο εξελισσόμενο περιβάλλον.
Η ασφαλεία του υλικού απαιτεί διεπιστημονική εξειδίκευση, η οποία κυμαίνετε από την κρυπτογραφία και την ασφάλεια του υπολογιστή μέσω υλικού, εώς τις τυπικές μεθόδους στην γνώση της οικονομίας, τους νόμους και οργανισμούς. Οι δεξιότητες ενός μηχανικού συστήματος, από την ανάλυση των επιχειρηματικών διαδικασιών μέσω της τεχνολογίας λογισμικού για την αξιολόγηση και τον έλεγχο, είναι επίσης σημαντικές, αλλά όχι επαρκείς, δεδομένου ότι ασχολείται μόνο με τα λάθη και τα σφάλματα.
Πολλά συστήματα ασφαλείας έχουν σημαντικές απαιτήσεις διασφάλισης. Η αποτυχία τους μπορεί να φέρει σε κίνδυνο την ανθρώπινη ζωή ή το περιβάλλον (όπως με τα συστήματα ελέγχου πυρηνικής ασφαλείας), να κάνουν σοβαρή ζημιά σε μεγάλες οικονομικές υποδομές (συστήματα τραπεζών και ATMs), να υπονομεύσουν την βιοσιμότητα του συνόμου των επιχειρησιακών τομέων (pay-TV) και τέλος να διευκολήνουν την εγκληματικότητα (συστήματα συναγερμού και αυτοκινήτων). Ακόμα και η αντίληψη ότι ένα σύστημα είναι πιο ευάλωτο από ότι είναι στην πραγματικότητα (πληρώνοντας με πιστωτική στο διαδίκτυο) μπορεί να υποστηρίξει σημαντικά την οικονομική ανάπτυξη.
Οι απαιτήσεις ασφαλείας διαφέρουν σημαντικά από το ένα σύστημα στο άλλο. Κάποιος μπορεί να χρειάζεται κάποιον συνδιασμό ελέγχου ταυτότητας χρήστη, ακεραιότητα των συναλλαγών και υπευθυνότητα, ανοχή σε σφάλματα, απόρρητο για τα μηνύματα του και μυστικότητα. Πολλά συστήματα αποτυγχάνουν διότι οι σχεδιαστές τους προστατεύουν τα λάθος πράγματα, ή προστατεύουν τα σωστά πράγματα με λάθος τρόπο.
Εξασφαλίζοντας προστασία λοιπόν, εξαρτάται από διαφορετικούς τύπους διαδικασιών. Πρέπει κάποιος να σκεφτεί τι είναι αυτό το οποίο χρειάζεται προστασία και πως μπορεί να το προστατεύσει. Επίσης, πρέπει να διασφαλίσει πως οι άνθρωποι που θα επιβλέπουν το σύστημα και θα το συντηρούν θα έχουν τα κατάλληλα κίνητρα.

Γενικό πλαίσιο σωστής ασφαλείας:

Η καλή ασφάλεια απαιτεί τέσσερα πράγματα:

- ***Πολιτική*:** τι πρέπει να επιτευχθεί.
- ***Μηχανισμός*:** οι αλγόριθμοι κρυπτογράφησης, οι έλεγχοι πρόσβασης, το υλικό για την αντίσταση παραβίασης συστήματος και άλλων μηχανημάτων που θα συγκεντρωθούν για την εφαρμογή της πολιτικής.
- ***Διαβεβαίωση*:** πόση εμπιστοσύνη μπορεί να υπάρχει σε κάθε συγκεκριμένο

μηχανισμό.

- ***Κίνητρο*:** το κίνητρο που οι άνθρωποι θέλουν να διαφυλάξουν και να διατηρήσουν το σύστημα και το κίνητρο που οι επιτιθέμενοι προσπαθούν να νικήσουν την πολιτική.

Πολλοί από τους όρους που χρησιμοποιούνται στην ασφάλεια είναι απλοί, αλλά πολλές φορές είναι παραπλανητικοί, αμφιλεγόμενοι με αποτέλεσμα να σε μπερδεύουν.
Το πρώτο πράγμα που πρέπει να διευκρινιστεί είναι τι εννοούμε με τον όρο σύστημα. Στην πράξη αυτό μπορεί να σημαίνει:

- ένα προιόν ή συστατικό, όπως ένα πρωτόκολλο κρυπτογράφησης ή μια έξυπνη κάρτα (smartcard) ή το υλικό του υπολογιστή
- μια συλλογή από τα από πάνω συν ένα λειτουργικό σύστημα, κάποιες επικοινωνίες και άλλα πράγματα που μπορούν να αποτελέσουν την υποδομή ενός οργανισμού
- τα παραπάνω πάλι συν κάποιες επιπλέον εφαρμογές οποιασδήποτε δομής και αντικειμένου
- τα παραπάνω συν το προσωπικό
- τα παραπάνω συν κάποιο εσωτερικοί χρήστες και η διαχείριση
- τα παραπάνω συν οι πελάτες και άλλοι εξωτερικοί χρήστες

Η σύγχυση όλων των παραπάνω ορισμών είναι μια γόνιμη πηγή σφαλμάτων και τρωτών σημείων. Σε γενικές γραμμές ο πωλητής και ο εκτιμητής του συνόλου επικεντρώνονται στο πρώτο και και στον δεύτερο ορισμό ενώ μια επιχείρηση στον έκτο. Θα συναντήσετε πολλά παραδείγματα συστημάτων που διαφημίζονται ή ακόμα χειρότερα έχουν πιστοποιηθεί ως ασφαλή, μόνο και μόνο επειδή ήταν το υλικό ασφαλές, αλλά είχε άσχημες επιπτώσεις όταν μια εφαρμογή δεν μπορούσε να τρέξει, ή όταν ο εξοπλισμός χρησιμοποιήθηκε με τρόπο που οι σχεδιαστές δεν είχανε προβλέψει. Το να αγνοήσει κάποιος τις ανθρώπινες συνιστώσες και να παραμελήσει ζητήματα ευχρηστίας, είναι από τις μεγαλύτερες αιτίες της αποτυχίας ενός συστήματος ασφαλείας.
Το επόμενο σύνολο προβλημάτων προέρχεται από την έλειψη σαφήνειας σχετικά με το ποιοί θα είναι οι παίκτες και τι προσπαθούν να αποδείξουν. Στη βιβλιογραφία σχετικά με την ασφάλεια και την κρυπτογράφηση, είναι μια σύμβαση εντολών στα πρωτόκολλα ασφαλείας που προσδιορίζονται από τα ονόματα που επιλέγονται. Π.χ. "Η Alice πιστοποιεί τον ευατό της στον Bob". Αυτό μπορεί να κάνει το κείμενο πολύ πιο ευανάγνωστο αλλά δεν είναι ο ακριβής προσδιορισμός αυτού που θέλουμε να εννοηθεί. Εννοούμε πως η Alice αποδεικνύει στον Bob ότι το όνομα της είναι στην πραγματικότητα αυτό ή ότι αποδεικνύει ότι έχει μια συγκεκριμένη πιστοποίηση; Εννοούμε ότι η Alice είναι ένας άνθρωπος ή μια έξυπνη κάρτα ή ένα λογισμικό που ενεργεί ως εργαλείο ως αντιπρόσωπος της; Αυτά τα ερωτήματα και πολλά άλλα μας οδηγούν στο συμπέρασμα πως δεν μπορούμε να γνωρίζουμε αν κάποιος έχει την κάρτα της Alice ή έχει χακάρει τον υπολογιστή της ή οτιδήποτε.

Τέλος, ένα γενικότερο συμπέρασμα για την ασφάλεια του υλικού είναι πως θα πρέπει να επισημοποιούνται οι πολιτικές ασφαλείας και οι στόχοι τους. Μπορεί πολλές φορές να είναι ενοχλητικό για τους πελάτες που επιθυμούν να πάρουν μαζί τους κάποιο υλικό, όμως γενικότερα η καλές κατασκευές ασφαλείας απαιτούν και σαφής στόχους για την προστασία της.
Εμείς θα αναλύσουμε δύο κατηγορίες υλικού που είναι και οι πιο διαδεδομένες στον κλάδο αυτό. Η πρώτη είναι τα ASIC(application-specific integrated circuit) και η δεύτερη είναι τα FPGA(field programmable gate array).

4.3 ΣΕΝΑΡΙΑ ΕΦΑΡΜΟΓΩΝ PUF

4.3.1 ΣΥΣΤΗΜΑ ΑΝΑΓΝΩΡΙΣΗΜΟΤΗΤΑΣ

Λόγω της φυσικής τους ιδιότητας μη κλωνοποιησιμότητας, χρησιμοποιώντας τα PUFs για αναγνωρισημότητα είναι πολύ ενδιαφέρον για αντιπαραχαρακτικές τεχνολογίες. Οι PUF έξοδοι μπορούν να χρησιμοποιηθούν για αναγνωρισημότητα με παρόμοιο τρόπο όπως σε βιομετρική αναγνωρισημότητα συστημάτων. Κατά τη διάρκεια μιας φάσης εγγραφής, ένας αριθμός CRP's από κάθε PUF από τον πληθυσμό είναι αποθηκευμένα σε μια βάση δεδομένων, μαζί με την ταυτότητα
του φυσικού συστήματος ενσωματώσεως του PUF. Κατά την αναγνωρισημότητα, η επαλήθευση διαλέγει μια τυχαία CRP από τις CRP's που είναι αποθηκευμένες στην βάση δεδομένων για το υπάρχον σύστημα και με το οποίο αμφισβητεί το PUF. Εάν η παρατηρούμενη έξοδος είναι αρκετά κοντά στην είσοδο της βάσης δεδομένων, τότε η αναγνώριση είναι επιτυχής, αλλιώς ανεπιτυχής.

Προκειμένου να αποτραπούν οι επαναλαμβανόμενες επιθέσεις, κάθε CRP πρέπει να χρησιμοποιηθεί μόνο μια φορά για κάθε PUF και να διαγραφεί από την βάση δεδομένων μετά την αναγνώριση.

Το κατώτατο όριο που χρησιμοποιείται για να αποφασίσει σχετικά με το θετικό αναγνωριστικό εξαρτάται από τον διαχωρισμό ανάμεσα στα ιστογράμματα intra-distance και inter-distance. Αν και τα δύο ιστογράμματα δεν συμπίπτουν, μια αναγνώριση με λάθη μπορεί να φτιαχτεί αντικαθιστώντας το κατώτατο όριο κάπου στο κενό ανάμεσα από τα δύο ιστογράμματα. Εάν συμπίπτουν τότε καθορίζουν τις ποσότητες του κατώτατου όριου κάνοντας ανταλλαγή ανάμεσα στο λάθος ποσοστό αποδοχής FAR(false-acceptance rate) και το ποσοστό εσφαλμένης απόρριψης FRR(false-rejection rate). Ο προσδιορισμός της FAR και της FRR βασίζονται στο αν συμπτίπτουν τα ιστογραμμάτα δια- και ενδο-απόστασης. Η βέλτιστη επιλογή, είναι ελαχιστοποιώντας το άθροισμα των FAR και FRR, επιτυγχάνεται με τον καθορισμό του ορίου όταν συμπίπτουν τα δύο ιστογράμματα, αλλά άλλες ανταλλαγές μπορεί να είναι επιθυμητές από συγκεκριμένες εφαρμογές.

Επιπλέον, είναι προφανές πως μια μοναδική αναγνώριση είναι μόνο δυνατή με μεγάλη πιθανότητα, αν η έξοδος περιέχει αρκετή εντροπία σε σχέση με το μέγεθος του πληθυσμού (Μια απάντηση που περιέχει n bits εντροπίας επιτρέπει τον καλύτερο δυνατό τρόπο για μοναδική αναγνωρισημότητα σε έναν πλυθησμό με μέσο μέγεθος 2^(n/2) λόγω του παράδοξου).

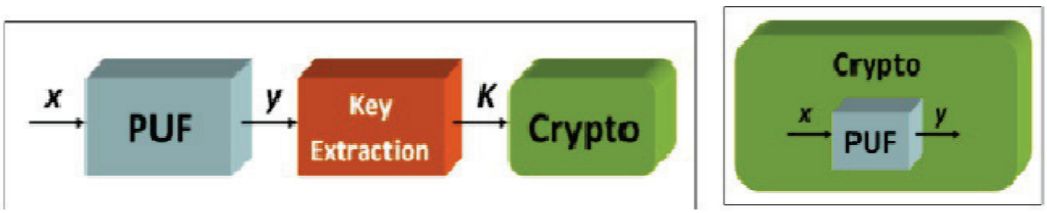
4.3.2 ΠΑΡΑΓΩΓΗ ΜΥΣΤΙΚΟΥ ΚΛΕΙΔΙΟΥ

Τα ενδογενή/εσωτερικά PUF σε ολοκληρωμένα κυκλώματα έχουν ενδιαφέρουσες ιδιότητες για χρήση της παραγωγής μυστικού κλειδιού και αποθήκευσης. Δεδομένου ότι το κλειδί παράγεται από την εσωτερική τυχαιότητα που παρουσιάστηκε από κατασκευαστική μεταβλητότητα, κανένα ρητό κλειδί-προγραμματιζόμενο βήμα δεν χρειάζεται, το οποίο απλοποιεί την κατανομή του κλειδιού.
Επιπλέον, δεδομένου ότι αυτή η τυχαιότητα είναι μόνιμα φτιαγμένη στις (υπό-)μικροσκοπικές φυσικές λεπτομέρειες του τσιπ, καμένα στατικό μεταβλητό κλειδί μνήμης δεν χρειάζεται. Αυτό επίσης, δίνει επιπλέον ασφάλεια κατά την ανίχνευση των επιθέσεων και ενδεχομένως και άλλων επιθέσεων από την πλευρά των καναλιών, δεδομένου ότι το κλειδί δεν αποθηκεύεται μόνιμα σε ψηφιακή μορφή, αλλά μόνο εμφανίζεται σε ευμετάβλητη μνήμη όταν απαιτείται από την
λειτουργία του. Τέλος, πιθανά παραποιημένα στοιχεία των PUF μπορούν να χρησιμοποιηθούν για να παρέχουν απαραβίαστα κλειδιά αποθήκευσης.
Για τους αλγόριθμους κρυπτογράφησης, απαιτούνται ομοιόμορφα τυχαία και απόλυτα αξιόπιστα και αληθινά κλειδιά. Από τότε που οι PUF εξόδοι είναι συνήθως θορυβώδης και περιέχουν μόνο ένα περιορισμένο ποσό εντροπίας, δεν μπορούνα να χρησιμοποιηθούν απευθείας ως κλειδιά. Ένα ενδιάμεσο στάδιο επεξεργασίας υποχρεούται να εξάγει ένα κρυπτογραφημένο κλειδί από τις εξόδους. Αυτό είναι ένα πρόβλημα που είναι γνωστό στη θεωρία πληροφοριών ως εκχύλιση μυστικού κλειδιού και γενικά επιλύεται από έναν αλγόριθμο δύο-φάσεων.
Κατά την αρχική φάση παραγωγής, το PUF ερωτάται και ο αλγόριθμος παράγει ένα μυστικό κλειδί μαζί με κάποιες επιπλέον πληροφορίες που συχνά αποκαλούνται βοηθητικά δεδομένα. Και τα δύο είναι αποθηκευμένα σε μία ασφαλή βάση δεδομένων από τον ελεγκτή, όμως όχι στην συσκευή. Κατά την φάση αναπαραγωγής, ο ελεγκτής παρουσιάζει τα βοηθητικά δεδομένα στον αλγόριθμο ο οποίος τα χρησιμοποιεί για να εξάγει το ίδιο κλειδί από το PUF όπως στο στάδιο παραγωγής. Με τον τρόπο αυτό, η συσκευή που περιέχει το PUF και ο ελεγκτής έχουν καθιερώσει ένα κοινό μυστικό κλειδί. Είναι δυνατόν να κατασκευαστούν αυτοί οι αλγόριθμοι έτσι ώστε το κλειδί να είναι απόλυτα μυστικό, ακόμη και αν τα βοηθητικά δεδομένα παρατηρούνται, δηλ., τα βοηθητικά δεδομένα μπορούν μα ανακοινώνονται δημοσίως από τον ελεγκτή στην συσκευή.

4.3.3 ΚΡΥΠΤΟΓΡΑΦΙΑ 'ΜΠΕΡΔΕΜΕΝΟΥ' ΥΛΙΚΟΥ

Ένα πρόσφατα παρουσιασμένο σενάριο εφαρμογής υπερβαίνει την παραγωγή μυστικών κλειδιών από PUFs για χρήση σε υπάρχοντα κρυπτογραφικά εργαλεία. Σε αντίθεση με αυτά που γνωρίζουμε ενσωματώνει πλώρως το PUF, οδηγώντας το λεγόμενο υλικό(hardware) να εμπλακεί στα κρυπτογραφικά εργαλεία. Κανένα κλειδί δεν παράγεται πια, αλλά το μυστικό στοιχείο του εργαλείου είναι η πλήρως μοναδική CRP συμπεριφορά του PUF στιγμιοτύπου στην ενσωματωμένη συσκευή. Η θεμελιώδης διαφορά ανάμεσα στην κλασική κρυπτογραφία με ένα PUF-βασισμένο σε κλειδί και στην κρυπτογραφία του 'μπερδεμένου' υλικού είναι εμφανής και από τις λέξεις.

Τα εργαλεία κρυπτογραφίας 'μπερδεμένου' υλικού είναι βασικά χωρίς κλειδί, δηλ., ότι όχι σε οποιοδήποτε σημείο στον αλγόριθμο ένα μυστικό ψηφιακό κλειδί είναι αποθηκευμένο στη μνήμη, αλλά ούτε και σε μια ευμετάβλητη ή μεταβλητή μνήμη. Αυτό όχι μόνο απλά προσφέρει πλήρης ασφάλεια ενάντια στους μεταβλητής μνήμης επιτιθέμενους, όπως συνέβη ήδη για την περίπτωση του PUF-βασισμένο στην παραγωγή κλειδιού, αλλά επιπλέον απαγορεύει σε μεγάλο βαθμό τους επιτιθέμενους από το να μάθουνε οτιδήποτε χρήσιμο. Κατά την άποψη αυτή, η κρυπτογραφία 'μπερδεμένου' υλικού είναι άμεσα συνδεδεμένη με το πεδίο της αποδεικτικής φυσικής ασφαλείας.



Η παραπάνω εικόνα κάνει εμφανή την διαφορά ανάμεσα σε ένα σύστημα κρυπτογραφίας με παραγωγή κλειδιού και στο σύστημα μπερδεμένου υλικού, το οποίο δεν χρησιμοποιεί καθόλου κλειδιά.

4.4 Η ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΤΑ PUFS

Η έννοια της κρυπτογραφίας όπως την έχουμε αναφέρει έχει ως στόχο γενικότερα την ασφάλεια μιας συσκευής ή μιας επικοινωνίας από ένα άκρο σε ένα άλλο. Βασικές έννοιες της κρυπτογραφίας όπως αναλύσαμε και παραπάνω είναι η εμπιστεύτικότητα, η πιστοποίηση, η ακεραιότητα των δεδομένων και η μη απάρνηση και επιτυγχάνεται χρησιμοποιώντας αλγόριθμους κρυπτογράφησης και κρυπτογραφίας.
Τα PUFs είναι εν μέρη ένα παρακλάδι της κρυπτογραφίας αφού χρησιμοποιούνται την παρούσα στιγμή σε εφαρμογές με ανάγκες για υψηλή ασφάλεια και λειτουργούν γενικότερα σε ενσωματωμένα κυκλώματα. Έχουνε στόχους να είναι απρόβλεπτα, αξιολογίσημα, μοναδικά, μη κλωνοποιήσιμα, να έχουν αναπαραγωγή και αν υπάρξει κάποια παραβίαση να γίνει άμμεσα αντιληπτή.
Παρακάτω γίνεται μια σύγκριση των PUFs με τον τρόπο λειτουργίας των συστήματων ασφαλείας – αλγόριθμοι κρυπτογράφησης (δεν αναφέρονται τα είδη των αλγορίθμων αναλυτικά – η σύγκριση γίνεται για να κατανοήσουμε ακόμα καλύτερα την γενικότερη δομή και τρόπο λειτουργίας ενός PUF).

PUFs VS Συστήματα ασφαλείας

ΔΙΑΦΟΡΕΣ	ΟΜΟΙΟΤΗΤΕΣ
Στα PUFs δεν υπάρχει η λέξη αποκρυπτογράφηση – η λεγόμενη αντίστροφη διαδικασία (σε θεωρητικό επίπεδο μόνο).	Ανάγκη ύπαρξης μνήμης.
Η κατανομή ενός κλειδιού στα PUF είναι απλοποιημένη συγκριτικά με τα συστήματα ασφαλείας.	Αναπαραγωγή μυστικού κλειδιού. PUF -> εσωτερική τυχαιότητα Συστήματα -> γεννήτρια ψευδοτυχαίων αριθμών
Για τους αλγόριθμους κρυπτογράφησης, απαιτούνται ομοιόμορφα τυχαία και απόλυτα αξιόπιστα και αληθινά κλειδιά. Οι PUF εξόδοι είναι συνήθως θορυβώδης και περιέχουν μόνο ένα περιορισμένο ποσό εντροπίας, δεν μπορούν να χρησιμοποιηθούν απευθείας ως κλειδιά.	Χρησιμοποίηση πανομοιώτυπων μεθόδων και διαδικασιών (π.χ. μυστικά κλειδιά-δημόσια, ιδιωτικά, blocks, κρυπταναλύσεις-ιστογράμματα κτλ.).
Υπάρχουν πλέον τεχνολογίες κρυπτογραφίας – μέσω PUF – που λειτουργούν χωρίς κλειδί (κρυπτογραφία μπερδεμένου-υλικού).	
Πιθανά παραποιημένα στοιχεία των PUF μπορούν να χρησιμοποιηθούν για να παρέχουν απαραβίαστα κλειδιά αποθήκευσης, τα κοινά συστήματα ασφαλείας δεν έχουν την δυνατότητα αυτή.	
Τα PUFs δεν χρειάζονται κλειδί για την μνήμη.	
Ο όρος μεταβλητότητα (αλληλουχία εντολών) στα PUF δεν είναι απαραίτητος, στα γνώριμα συστήματα ασφαλείας είναι.	

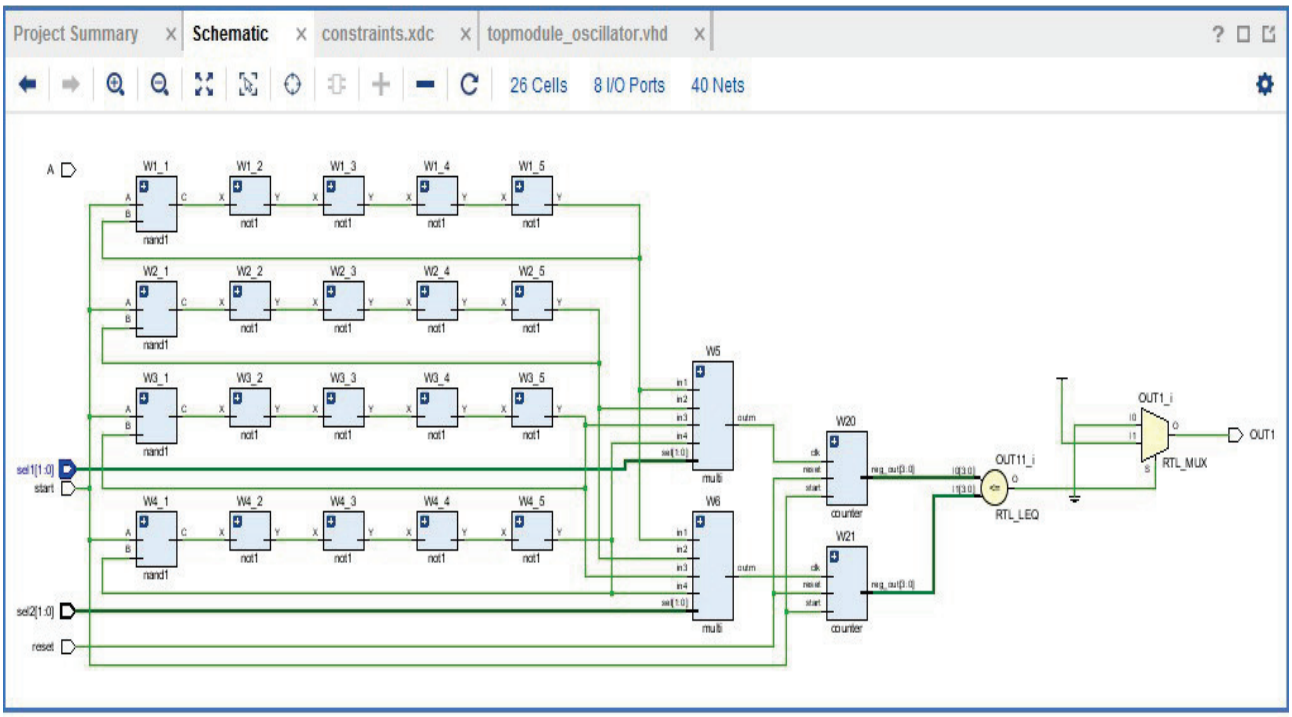
ΚΕΦΑΛΑΙΟ 5

ΠΑΡΑΔΕΙΓΜΑΤΑ

Το φάσμα των PUF' s είναι αρκετά μεγάλο για αυτό επιλέκτηκαν δύο από αυτά για την σχεδίαση του κώδικα τους και την ανάλυση τους με περισσότερες λεπτομέρειες. Τα PUF' s που επιλέκτηκαν είναι δύο PUF' s τα οποία βασίζονται και τα δύο στην καθυστέρηση (delay based instrinsic). Το ένα είναι ο PUF κριτής (arbiter) και το δεύτερο είναι το δαχτυλίδι – ταλαντωτής PUF (ring oscillator).
Ο κώδικας των δύο αυτών PUF έγινε σε γλώσσα VHDL και η σχεδίαση και η προσωμοίωση για την εξακρίβωση τυχόν λαθών στο πρόγραμμα ISE Webpack της Xilinx.

5.1 OSCILLATOR PUF

Όπως είδαμε και πιο αναλύτικά στο κεφάλαιο των PUF' s στο δαχτυλίδι ταλαντωτής PUF η έξοδος αντιστρέφεται και γυρίζει στην ίδια του την είσοδο και έτσι ορίζεται η συχνότητα με αποτέλεσμα από αυτό κιόλας να εξαρτάται και η καθυστέρηση όπως είναι λογικό. Αυτό όπως είπαμε κιόλας παραμετροποιείται από τον ίδιο τον κατασκευαστή του PUF.
Η εικόνα που υπάρχει παρακάτω δείχνει την δομή του oscillator PUF που δημιούργησα στο πρόγραμμα.



Επίσης εδώ αναγράφεται και το βασικό σκέλος του κώδικα του.

```
library IEEE;
use IEEE.STD_LOGIC_1164.ALL;
USE ieee.std_logic_arith.all;
USE ieee.std_logic_unsigned.all;

entity topmodule_oscillator is
PORT( A : IN STD_LOGIC;
                reset : IN STD_LOGIC;
                sel1 : IN STD_LOGIC_VECTOR (1 DOWNTO 0);
                sel2: IN STD_LOGIC_VECTOR (1 DOWNTO 0);
                start: IN STD_LOGIC;
                OUT1 : OUT STD_LOGIC);
end topmodule_oscillator;

architecture Behavioral of topmodule_oscillator is

component nand1
PORT( A, B : IN STD_LOGIC;
                 C   : OUT STD_LOGIC);
end component;

component not1
PORT( X : IN STD_LOGIC;
                 Y :OUT STD_LOGIC);
end component;

component multi
PORT(in1,in2,in3,in4 : IN STD_LOGIC;
                        sel : IN STD_LOGIC_VECTOR (1 DOWNTO 0);
                        outm : OUT STD_LOGIC);
end component;

component counter
PORT (clk, reset : IN STD_LOGIC;
                        start: IN STD_LOGIC;
        reg_out: OUT integer range 0 to 15);
end component;

SIGNAL
outm1,outm2,X1,X2,X3,X4,X5,X6,X7,X8,X9,X10,X11,X12,X13,X14,X15,X16,C1
,C2,C3,C4 : STD_LOGIC:='0';
signal fA,fB : integer range 0 to 15;
```

```
begin

W1_1 : ENTITY WORK.nand1 PORT MAP (A=>start, B=>C1, C=>X1);
W1_2 : ENTITY WORK.not1 PORT MAP (X=>X1, Y=>X2);
W1_3 : ENTITY WORK.not1 PORT MAP (X=>X2, Y=>X3);
W1_4 : ENTITY WORK.not1 PORT MAP (X=>X3, Y=>X4);
W1_5 : ENTITY WORK.not1 PORT MAP (X=>X4, Y=>C1);

W2_1 : ENTITY WORK.nand1 PORT MAP (A=>start, B=>C2, C=>X5);
W2_2 : ENTITY WORK.not1 PORT MAP (X=>X5, Y=>X6);
W2_3 : ENTITY WORK.not1 PORT MAP (X=>X6, Y=>X7);
W2_4 : ENTITY WORK.not1 PORT MAP (X=>X7, Y=>X8);
W2_5 : ENTITY WORK.not1 PORT MAP (X=>X8, Y=>C2);

W3_1 : ENTITY WORK.nand1 PORT MAP (A=>start, B=>C3, C=>X9);
W3_2 : ENTITY WORK.not1 PORT MAP (X=>X9, Y=>X10);
W3_3 : ENTITY WORK.not1 PORT MAP (X=>X10, Y=>X11);
W3_4 : ENTITY WORK.not1 PORT MAP (X=>X11, Y=>X12);
W3_5 : ENTITY WORK.not1 PORT MAP (X=>X12, Y=>C3);

W4_1 : ENTITY WORK.nand1 PORT MAP (A=>start, B=>C4, C=>X13);
W4_2 : ENTITY WORK.not1 PORT MAP (X=>X13, Y=>X14);
W4_3 : ENTITY WORK.not1 PORT MAP (X=>X14, Y=>X15);
W4_4 : ENTITY WORK.not1 PORT MAP (X=>X15, Y=>X16);
W4_5 : ENTITY WORK.not1 PORT MAP (X=>X16, Y=>C4);



W5 : ENTITY WORK.multi PORT MAP (in1=>C1, in2=>C2, in3=>C3,
in4=>C4,sel=>sel1,outm=>outm1 );
W6 : ENTITY WORK.multi PORT MAP (in1=>C1, in2=>C2, in3=>C3, in4=>C4,
sel=>sel2, outm=>outm2);

W20 : ENTITY WORK.counter PORT MAP
(clk=>clk,reset=>reset,start=>start,reg_out=>fA);
W21 : ENTITY WORK.counter PORT MAP
(clk=>clk,reset=>reset,start=>start,reg_out=>fB);

PROCESS(FA,FB)
BEGIN

IF fA <= fB THEN
```

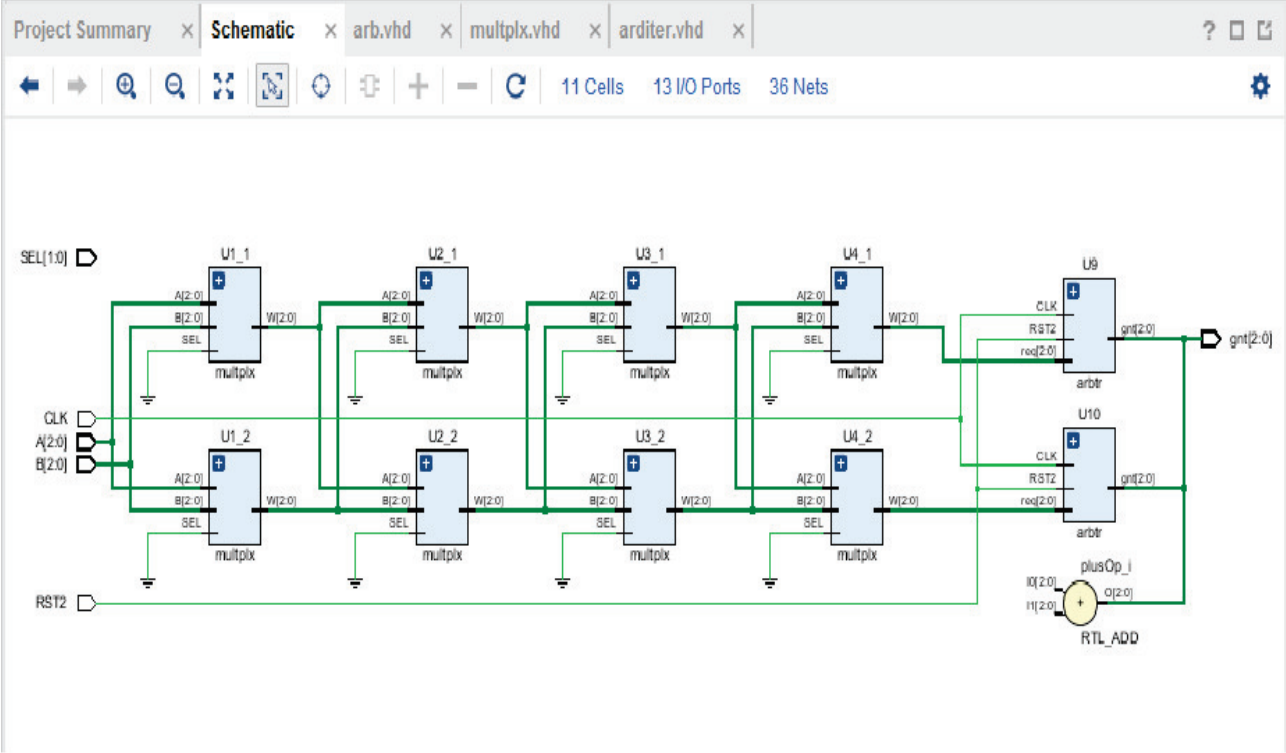
```
OUT1 <= '0';
ELSe
OUT1 <= '1';
END IF;
END PROCESS;

end Behavioral;
```

Συμπερασματικά ο oscillator από διάφορες έρευνες πανεπιστημιακών το ποσοστό του μ-inter (ποσοστό μοναδικότητας) είναι στο 46,15%, ποσοστό αρκετά ελπιδορφόρο για την προβλεψομότητα των αποτελεσμάτων. Το ποσοστό του μ-intra (ποσοστό θορύβου) είναι στο 0,48 , δείχνοντας να τείνει πολύ κοντά στο μηδέν που κανονικά είναι το ιδανικό.
Το μόνο κακό σε αυτό το PUF είναι πως για να αναπαραχθούν τα αποτελέσματα αυτά είναι πως από τα 8 ζευγάρια βρόγχων που δημιουργήθηκαν για το πείραμα τα 7 έμειναν αχρησιμοποίητα. Δηλαδή μόνο το ένα από αυτά είναι παραγωγικό.

5.2 ARBITER PUF

Η βασική ιδέα ενός PUF arbiter είναι ,όπως είδαμε και στο κεφάλαιο των PUF, δύο μονοπάτια (για την ακρίβεια δύο παράλληλα μονοπάτια καθυστέρησης) σε ένα ολοκληρωμένο σύστημα που 'διαγωνίζονται' και ο κριτής αποφασίζει πιο από τα δύο θα κερδίσει.

Η εικόνα που υπάρχει παρακάτω δείχνει την δομή του arbiter PUF που δημιούργησα στο πρόγραμμα.



Επίσης εδώ αναγράφεται και το βασικό σκέλος του κώδικα του.

```
library IEEE;
use IEEE.STD_LOGIC_1164.ALL;
USE ieee.std_logic_arith.all;
USE ieee.std_logic_unsigned.all;

entity arb is

PORT ( SEL: IN STD_LOGIC_VECTOR(1 DOWNTO 0);
                CLK, RST2 : IN STD_LOGIC;
                A,B: IN STD_LOGIC_VECTOR(2 DOWNTO 0);
                gnt  : OUT STD_LOGIC_VECTOR(2 DOWNTO 0)
                );
```

```
END arb;


architecture Behavioral of arb is

SIGNAL W1,W2,W3,W4,W5,W6,W7,W8,GNT1,GNT2:STD_LOGIC_VECTOR(2
DOWNTO 0);

begin

U1_1 : ENTITY WORK.multplx PORT MAP (A=>A, SEL=>'0', B=>B, W=>W1);
U1_2 : ENTITY WORK.multplx PORT MAP (A=>A,B=>B,SEL=>'0',W=>W2);
U2_1 : ENTITY WORK.multplx PORT MAP(A=>W1,B=>W2,SEL=>'0',W=>W3);
U2_2 : ENTITY WORK.multplx PORT MAP
(A=>W1,B=>W2,SEL=>'0',W=>W4);
U3_1 : ENTITY WORK.multplx PORT MAP
(A=>W3,B=>W4,SEL=>'0',W=>W5);
U3_2 : ENTITY WORK.multplx PORT MAP
(A=>W3,B=>W4,SEL=>'0',W=>W6);
U4_1 : ENTITY WORK.multplx PORT MAP
(A=>W5,B=>W6,SEL=>'0',W=>W7);
U4_2 : ENTITY WORK.multplx PORT MAP
(A=>W5,B=>W6,SEL=>'0',W=>W8);
U9 : ENTITY WORK.arbtr PORT MAP (CLK=>CLK, RST2=>RST2, req=>W7,
gnt=>gnt);
U10 : ENTITY WORK.arbtr PORT MAP (CLK=>CLK, RST2=>RST2, req=>W8,
gnt=>gnt);
gnt<=GNT1 + GNT2;
end Behavioral;
```

Αυτό που παρατηρείται πρώτο σε αυτό το PUF είναι η συμμέτρικη διαμόρφωση του, που έχει και ως αποτέλεσμα και τα δύο μονοπάτια να έχουν την ίδια καθυστέρηση.
Και εδώ από διάφορες έρευνες πανεπιστημιακών, στην πιο γνωστή από αυτές, το ποσοστό του μ-inter είναι στο 23%, το οποίο μας δείχνει ότι η μοναδικότητα του είναι επιφανειακή αλλά δίνει και μια ελπίδα στην επιστημονική κοινότητα. Το μ-intra δείχνει να είναι στο μικρότερο του 5%, πράγμα το οποίο μας δείχνει ότι είναι πολύ κοντά στο μηδέν, πράγμα το οποίο ζητάμε.
Το κακό σε αυτό το PUF είναι ότι όποιος μπορεί να φτιάξει ένα αντίστοιχο μαθηματικό μοντέλο, μπορεί απλά παρατηρώντας έναν αριθμό από καταμετρημένες εξόδους (CRP' s), να προβλέψει τις επόμενες. Άρα σε αυτήν την περίπτωση όσο περισσότερα blocks βάζουμε σε αυτό το PUF τόσο μειώνουμε την προβλεψιμότητα.
Στο πρόβλημα της προβλεψιμότητας έχουν απαντήσει οι ερευνητές Hopper & Blum δημιουργώντας ένα πρωτόκολλο για ασφαλή επαλήθευση και εξακρίβωση χωρίς

ανθρώπινη βοήθεια από τον υπολογιστή. Αυτό το πρωτόκολλο είναι βασισμένο στο πρόβλημα που μπορεί να λυθεί με βάση τον θόρυβο. Δηλαδή, στην πραγματικότητα χρησιμοποιεί το ίδιο το πρόβλημα ως μέσον λύσης.

ΚΕΦΑΛΑΙΟ 6

ΕΠΙΛΟΓΟΣ

Συμπερασματικά μέσα από την μελέτη αυτή της εργασίας γίνεται κατανοητό ότι η τεχνολογία των PUF είναι μια πολλά υποσχόμενη τεχνολογία με απεριόριστες δυνατότητες για μελλοντική ανάπτυξη και γενική αποδοχή της σημασίας και των πλεονεκτημάτων της. Ο λόγος που αυτό δεν έχει επιτευχθεί μέχρι σήμερα και οι δυνατότητες τους δεν έχουν αξιοποιηθεί ανάλογα είναι ότι τα προβλήματα στην ασφάλεια και την ιδιωτικότητα είναι αρκετά δύσκολο να ξεπερασθούν. Οι κίνδυνοι που επέρχονται σε ένα σύστημα ασφαλείας ποικίλουν και αυξάνονται καθημερινά, είτε είναι φυσικοί είτε είναι συστημικοί και αυτό κάνει την δουλειά των PUF πιο σημαντική όσο περνάει ο χρόνος.
Για αυτόν ακριβώς τον λόγο η ποικιλία τους είναι τόσο μεγάλη και όσο περνάει ο χρόνος αυξάνεται. Οι ερευνητές προσπαθούν να βρίσκουν τρόπους συνεχώς και νέες μεθόδους έτσι ώστε οι συναρτήσεις αυτές να είναι αδιαπέραστες και οι εξόδοι τους να μην μπορούν να κλωνοποιηθούν και να περαστούν στο οποιοδήποτε σύστημα για να το προσλάβουν.
Σαν αποτέλεσμα όλων αυτών που διαβάσαμε στα παραπάνω κεφάλαια πολύ βασική παράλειψη είναι ότι σε κανένα από αυτά τα συστήματα δεν υπάρχει ένα πρωτόκολλο πιστοποίησης. Σε όλα τα μέχρι συστήματα που χρησιμοποιεί ο άνθρωπος το ποιο σημαντικό πρωτόκολλο είναι αυτό της πιστοποίησης και της ασφάλειας των δεδομένων του. Μπορεί ένα πρωτόκολλο πιστοποίησης να είναι κάτι συνηθισμένο όμως είναι και ο τρόπος που αποτρέπονται οι πιο συνηθισμένες επιθέσεις και τα πιο βασικά προβλήματα που μπορεί να προκύψουν σε ένα σύστημα.
Μπορεί να μιλάμε για ασφάλεια επιπέδου όμως στα περισσότερα από τα PUF είναι χρήσιμο και μπορεί να υλοποιηθεί.
Σκοπός μου σε αυτή την εργασία ήταν να παρουσιάσω με τον καλύτερο συνατό τρόπο τις τεχνικές προστασίας των PUF που μέχρι τώρα έχουν αναπαραχθεί, αξιολογηθεί και υλοποιθεί.

Βιβλιογραφία - Λήμματα

[1] ebooks.edu.gr/modules/ebook/show.php/DSB103/173/1207,4410/
[2] architecture.di.uoa.gr/5sect351.html
[3] www.ece.unm.edu/~jimp/HOST/
[4] startingelectronics.com/software/VHDL-CPLD-course/tut9-SR-latch/
[5] www.lib.ntua.gr/gr/el_sources/ebooks/kagiafas/CHAPTER9.pdf
[6] infolab.gen.auth.gr/downloads/%CE%A0%CE%B5%CF%81%CE%B9%CE%BF%CF%81%CE%B9%CF%83%CE%BC%CE%BF%CE%AF%20%CE%91%CE%BA%CE%B5%CF%81%CE%B1%CE%B9%CF%8C%CF%84%CE%B7%CF%84%CE%B1%CF%82%20%CE%BC%CE%B5%20SQL%20240%20%CE%A0%CE%BB%CE%AE%CF%81%CE%B5%CF%82.pdf
[7] nemertes.lis.upatras.gr/jspui/bitstream/10889/7981/1/%CE%94%CE%B9%CF%80%CE%BB%CF%89%CE%BC%CE%B1%CF%84%CE%B9%CE%BA%CE%AE.pdf
[8] www.cl.cam.ac.uk/~rja14/book.html
[9] el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1#.CE.A4.CF.81.CE.AF.CF.84.CE.B7_.CE.A0.CE.B5.CF.81.CE.AF.CE.BF.CE.B4.CE.BF.CF.82_.CE.9A.CF.81.CF.85.CF.80.CF.84.CE.BF.CE.B3.CF.81.CE.B1.CF.86.CE.AF.CE.B1.CF.82_.281950_.CE.BC..CE.A7._-_.CE.A3.CE.AE.CE.BC.CE.B5.CF.81.CE.B1.29
[10] www.ics.uci.edu/~jmoorkan/vhdlref/compinst.html
[11] etd.ohiolink.edu/!etd.send_file?accession=toledo1371088101&disposition=inline
[12] www.eecs.ucf.edu/~jinyier/courses/EEE4932/lab2_PUF/
[13] di.ionio.gr/~emagos/security/Simeioseis-Asfaleia%20Part%20A.pdf
[14] www.ip.gr/el/dictionary/260-ASIC.php
[15] en.wikipedia.org/wiki/Application-specific_integrated_circuit
[16] www.google.com/patents/US4816823
[17] www.wisegeek.com/what-is-an-application-specific-integrated-circuit.htm
[18] eureka.lib.teithe.gr:8080/bitstream/handle/10184/2547/GKAXOPOULOU.pdf?sequence=2
[19] www.it.uom.gr/project/mycomputer/cpu/construc.html
[20] www.icsd.aegean.gr/website_files/proptyxiako/99289356.pdf
[21]nefeli.lib.teicrete.gr/browse/stef/epp/2009/MaurokostasKonstantinos,KenisKonstantinos/attached-document-1258542739-61226-25799/Maurokostas2009.pdf
[22] www.cslab.ntua.gr/courses/csintro/files/eky-assembly-2005.pdf
[23] www.slideshare.net/paterspyridon/m-38117810
[24] www.arl.wustl.edu/projects/fpx/class/resources/Libraries%20and%20Packages%20in%20VHDL.htm
[25] vhdlguru.blogspot.gr/2010/03/usage-of-components-and-port-mapping.html
[26] jason.sdsu.edu/adk/html/adk-3.html --/simulating HDL in modelsim/--

[27] fpgasite.wordpress.com/2016/04/16/vhdl-arbiter-part-ii/
[28] fpga-hdl.blogspot.gr/2012/07/test.html
[29] nemertes.lis.upatras.gr/jspui/bitstream/10889/8659/1/%CE%91%CE%BD%CE%AC%CE%BB%CF%85%CF%83%CE%B7_%CE%B8%CE%B5%CE%BC%CE%AC%CF%84%CF%89%CE%BD_%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82_%CF%83%CF%84%CE%B1_RFID_%CF%83%CF%85%CF%83%CF%84%CE%AE%CE%BC%CE%B1%CF%84%CE%B1.pdf
[30] eprint.iacr.org/2012/557.pdf
[31]drum.lib.umd.edu/bitstream/handle/1903/16242/Lai_umd_0117N_15873.pdf;jsessionid=287446B996E1DB4645F8D50CF31BC7FE?sequence=1
[31] vlsicoding.blogspot.gr/2013/10/design-fixed-priority-arbiter-in-vhdl.html
[31] citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.86.550&rep=rep1&type=pdf
[31] sid-vlsiarena.blogspot.gr/2013/06/simple-arbiter-example-in-verilog.html
[32] Physically Unclonable Functions: a Study on the state of the art and future research By Roel Maes and Ingrid Verbauwhede
[33] An area-optimized FPGA viterbi decoder for PUFs by Seesaw
[34] A secure and unclonable embedded system using instruction level PUF authentication by Jason X.Zheng, Dongfang Li and Miodrag Potkonjak
[35] Physical unclonable functions and public-key crypto for FPGA IP protection by Jorge Guajardo, Sandeep S.Kumar, Geert-Jan Schrijen and Pim Tuyler