



ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ
ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ: ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ
ΣΥΓΧΡΟΝΑ ΔΙΚΤΥΑ

Μελέτη και Αξιολόγηση SRAM PUF

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΟΥ

Αποστόλου Πίτσικου

Επιβλέπων : Δρ. Μεσαριτάκης Χάρης

Μέλη εξεταστικής επιτροπής:

Σάμος, Ιούλιος 2024

Πίνακα Περιεχομένων

ΠΕΡΙΛΗΨΗ	5
ABSTRACT	6
ΕΙΣΑΓΩΓΗ.....	7
Τι είναι ένα PUF;.....	7
Ορισμός του PUF	7
Θεωρητική προσέγγιση και βασικοί ορισμοί των PUFs	8
Κλάση PUF (P).....	8
Ενδεχόμενο PUF (puf)	8
Αξιολόγηση PUF (Puf Evaluation)	8
Εσωτερική απόσταση (intra-distance).....	9
Εξωτερική απόσταση (inter-distance)	10
ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΤΩΝ PUFs	11
Με βάση την τεχνολογία ανάπτυξης της διάταξης:.....	11
Ηλεκτρονικά PUF	11
Μη ηλεκτρονικά PUF	11
PUF πυριτίου	11
Με βάση τις ιδιότητες κατασκευής τους:	12
Εγγενή.....	12
Μη- εγγενή PUFs	12
Delay-based PUFs	13
PUF "Κριτής" (Arbiter PUFs)	13
PUF Ταλαντωτή Δακτυλίου (Ring Oscillator PUFs).....	14
PUF Παρεμβολών (Glitch PUFs).....	14
Memory-based PUFs.....	15
SRAM PUFs.....	15
Latch PUFs	16
Flip-Flop PUFs	16
Butterfly PUFs.....	16

Buskeeper PUFs.....	17
Bistable Ring PUFs (Δισταθές PUF Δακτυλίου)	17
Κατασκευές PUF Μεικτού Σήματος (Mixed Signal PUF Constructions)	17
ΑΞΙΟΛΟΓΗΣΗ PUF ΔΙΑΤΑΞΕΩΝ.....	19
Ευκολία κατασκευής	19
Ευκολία Αξιολόγησης	19
Ευκολία Αναπαραγωγής.....	20
Μοναδικότητα	20
Ευκολία αναγνώρισης.....	20
Ιδιότητα "μη Κλωνοποίησης"	21
Αδυναμία Πρόβλεψης	21
Μαθηματική και Πραγματική Μη Κλωνοποίηση	23
Αληθινή Μη Αντιγραφή	24
Ιδιότητα της Μονής Κατεύθυνσης	24
Απόδειξη Παραποίησης.....	24
ΤΕΧΝΙΚΕΣ ΚΑΙ ΒΕΛΤΙΩΣΗ	27
Έλεγχος Power-Up (Power-Ramp Tuning & Stabilizing Readouts)	27
Ιονίζουσα Ακτινοβολία (TID – Total Ionizing Dose).....	27
Επιλογή Σταθερών Cells (Stable-Cell Selection)	27
Fuzzy Extractors & Error-Correction Codes.....	27
Αντιμετώπιση Aging (Silicon Aging Compensation).....	27
Memory-Combining PUFs (π.χ. SRAM + DRAM).....	28
LED-PUF: Ξεκλειδωμένες δυνατότητες σταθερότητας.....	28
ΠΕΙΡΑΜΑΤΙΚΗ ΚΑΤΑΣΚΕΥΗ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗ SRAM PUF	29
Προσέγγιση του Πειράματος.....	29
Γενικός τρόπος λειτουργίας	32
Αξιολόγηση των δεδομένων	34
ΕΠΙΛΟΓΟΣ	39
ΠΑΡΑΡΤΗΜΑ Α	40
Πίνακες Μετρήσεων SRAM Chips	40

ΠΑΡΑΡΤΗΜΑ Β	48
Προγραμματισμός Υλοποίησης Πειράματος	48
Προγραμματισμός Arduino Μετρήσεων Τιμών SRAM	48
Προγραμματισμός Python υπολογισμού Μετρικών	49
ΒΙΒΛΙΟΓΡΑΦΙΑ	52

ΠΕΡΙΛΗΨΗ

Από την εμφάνιση των πρώτων ηλεκτρονικών υπολογιστών, η πρόοδος στο τεχνολογικό πεδίο γνώρισε μία αλματώδη ανάπτυξη. Παράλληλα αυξήθηκε και ο βαθμός στον οποίο κάποιος μπορούσε να παραβιάσει τα μέτρα ασφάλειας και να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα και πληροφορίες.

Τις τελευταίες δεκαετίες, αλλά ιδιαιτέρως σήμερα όπου έχει αποκτήσει μεγάλη δημοφιλία η Τεχνητή Νοημοσύνη και τα Μεγάλα Δεδομένα, έχει αναδυθεί η ανάγκη για τη χρήση νέων μεθόδων στην ασφάλεια της πληροφορικής, οι οποίες να ανταποκρίνονται στις νέες προκλήσεις, με βελτιωμένη αποτελεσματικότητα σε σχέση με τις αντίστοιχες παραδοσιακές.

Μία τεχνολογία, η οποία έχει προταθεί και υιοθετηθεί, σε έναν βαθμό, είναι και οι μη Κλωνοποιήσιμες Φυσικές Συναρτήσεις (Physical Unclonable Functions - PUFs). Στο πρώτο μέρος της παρούσας εργασίας επιχειρείται να παρουσιαστεί η προσέγγιση της τεχνολογίας αυτής στον τομέα της ασφάλειας, δίνεται μία εικόνα των διαφόρων τύπων αυτής, καθώς επίσης αναφέρονται και τα μετρήσιμα μεγέθη που χρησιμοποιούνται για την αξιολόγηση της αποτελεσματικότητάς της.

Επιπλέον, στο δεύτερο μέρος της εργασίας, γίνεται μία προσπάθεια για τη σχεδίαση και την ανάπτυξη με τη χρήση της πλατφόρμας Arduino και ενός τσιπ SRAM της Microchip, μίας γεννήτριας κωδικών PUF και η αξιολόγηση της αποτελεσματικότητάς του.

Λέξεις Κλειδιά: SRAM, PUF

ABSTRACT

Since the appearance of the first computers, the progress in the technological fields have experienced a great expand. At the same time, the degree to which someone could bleach the security measures and gain access to sensitive data and information increased also.

In recent decades, and especially today that Artificial Intelligence and Big Data have gained popularity, the necessity for using new methods in Information Technology domain has emerged; methods which should respond to the risen challenges with better efficiency than the corresponding traditional ones.

One such technology that has been proposed and adopted, to some extent, is the Physical Unclonable Functions (PUFs). In the first part of this thesis, is presented the approach of this technology in the IT security field, given the main different types of them, as well as the metrics that are used for the evaluation are also mentioned.

Furthermore, in the second part, an attempt is made to design and deploy a SRAM PUF with use of an Arduino platform and Microchip SRAM chip, evaluate its performance and provide the authentication protocol for exchanging keys between the PUF key generator and end devices.

Keywords: PUF, SRAM

ΕΙΣΑΓΩΓΗ

Τι είναι ένα PUF;

Οι μη Κλωνοποιήσιμες Φυσικές Συναρτήσεις (στο εξής το/τα PUF/PUFs) προσπαθούν να αξιοποιήσουν εκείνα τα φυσικά χαρακτηριστικά των διαφόρων αντικειμένων (τεχνητών ή μη), τα οποία είναι μοναδικά, δηλαδή κληρονομούνται από την εμφάνισή τους ή την κατασκευή τους και επιπλέον η αντιγραφή/αναπαραγωγή αυτών των χαρακτηριστικών είναι αδύνατη (ή τεχνικά πολύ δύσκολη). Χαρακτηριστικό ισοδύναμο παράδειγμα των PUFs είναι τα δακτυλικά αποτυπώματα των ανθρώπων.

Η μοναδικότητα αυτών των χαρακτηριστικών έγκειται στο γεγονός ότι στην όποια δημιουργία ή κατασκευή ενός πανομοιότυπου αντικειμένου, επιδρούν και εντελώς τυχαίες και ανεξέλεγκτες τεχνικά μεταβλητές του περιβάλλοντος. Σε ένα παράδειγμα κατασκευής ενός προϊόντος σε ένα οποιοδήποτε εργοστασιακό περιβάλλον, παρότι μακροσκοπικά μπορεί να μοιάζουν ολόδια, σε μικροσκοπικό έλεγχο είναι σίγουρο ότι διάφορες τυχαίες μεταβλητές έχουν επιδράσει στη διαδικασία κατασκευής ώστε τα εκάστοτε να εμφανίζουν διαφορετικά χαρακτηριστικά, είτε στην εμφάνιση, είτε στη λειτουργία τους, που στα μάτια ενός παρατηρητή φαντάζει ως κατασκευαστική «ανωμαλία».

Αυτές τις «ανωμαλίες» αποτελούν και το αντικείμενο μελέτης των PUFs, τις οποίες και χρησιμοποιούν στην Κρυπτογραφία για να βελτιστοποιήσουν τις υπάρχουσες τεχνικές και μεθόδους στον τομέα της Ασφάλειας Πληροφορικής.

Ορισμός του PUF

Από την εμφάνισή τους δόθηκαν αρκετοί ορισμοί που προσπάθησαν να περιγράψουν με σαφήνεια το τι είναι ένα PUF. 40 χρόνια μετά δεν έχει επικρατήσει ένας καθολικά αποδεκτός ορισμός από τους τεχνολογικούς οργανισμούς και την επιστημονική κοινότητα, παρότι κάποιος μπορεί να αντιληφθεί τη συνάφεια και να συμφωνήσει με την ορθότητα της κάθε περιγραφής.

Ο Maes στο βιβλίο του δίνει τον εξής ορισμό, ο οποίος και υιοθετείται στο πλαίσιο της παρούσης εργασίας:

«Μία συνάρτηση PUF είναι μία έκφραση ενός εγγενούς και μη αντιγράψιμου συγκεκριμένου μοναδικού χαρακτηριστικού ενός φυσικού αντικειμένου»,

διαχωρίζοντας τα συγκεκριμένα χαρακτηριστικά από τα οποιαδήποτε αντίστοιχα βιομετρικά, δίνοντας έμφαση στη μελέτη αυτών των χαρακτηριστικών πάνω σε φυσικά αντικείμενα.

Δεδομένου ότι ο ορισμός μίας έννοιας ή έκφρασης οφείλει να έχει καθολική αποδοχή και εφαρμογή σε οποιαδήποτε περίπτωση συνοδεύει, ο Maes παραθέτει και κάποιες επιπλέον έννοιες, ώστε να καταστήσει πληρέστερη την περιγραφή ενός PUF.

Θεωρητική προσέγγιση και βασικοί ορισμοί των PUFs

Κλάση PUF (P)

Η κλάση PUF (P) περιλαμβάνει το σύνολο μίας κατασκευής PUF. Περιγράφει μία στοχαστική διαδικασία (P.Create) μέσω της οποίας δημιουργούνται το σύνολο των ενδεχόμενων (instances) pu_f μίας κλάσης P.

Για να γίνει ένας εννοιολογικός σαφής διαχωρισμός μίας κλάσης P από την διαδικασία P.Create, μπορούμε να περιγράψουμε την P ως έναν πλήρη λεπτομερή σχεδιασμό μίας συνάρτησης PUF, ενώ η P.Create ως τη διαδικασία υλοποίησης αυτού του σχεδιασμού.

$$P.Create(r^c), \text{ όπου } r^c \leftarrow \{0,1\}^*$$

Ενδεχόμενο PUF (pu_f)

Ως ενδεχόμενο pu_f ορίζεται ένα συγκεκριμένο στιγμιότυπο μίας κλάσης P και εξ' ορισμού, όλα τα πιθανά στιγμιότυπα pu_f που δημιουργούνται μέσα από μία διαδικασία P.Create, αποτελούν την κλάση P.

$$P \equiv \{pu_{f_i} \leftarrow P.Create(r_i^c) : \forall i, r_i^c \leftarrow \{0,1\}^*\}$$

Θα μπορούσαμε να πούμε ότι τα στιγμιότυπα είναι αποτέλεσμα επεξεργασίας μίας τιμής εισόδου στη διαδικασία P.Create της συγκεκριμένης κλάσης PUF, όπως ακριβώς λειτουργεί μία οποιαδήποτε συνάρτηση, και επιπλέον, ένα μεμονωμένο στιγμιότυπο pu_f χαρακτηρίζει μία συγκεκριμένη κατάσταση (state) της κλάσης PUF.

Μέρος αυτής της συγκεκριμένης κατάστασης, σε ορισμένες κλάσεις PUF, δύναται να παραμετροποιηθεί και επηρεαστεί εξωτερικά. Αυτό το μέρος της κατάστασης state μίας κλάσης P ονομάζεται πρόκληση (challenge). Το σύνολο όλων των πιθανών προκλήσεων (challenges) που μπορούν να εφαρμοστούν πάνω σε ένα στιγμιότυπο pu_f μίας κλάσης P, ορίζεται ως X_p .

Αξιολόγηση PUF (Puf Evaluation)

Για να αξιολογήσουμε εκείνα τα χαρακτηριστικά μίας κλάσης P, που την καθιστούν μοναδική, αρκεί να διεξάγουμε ένα πείραμα αξιολόγησης ενός στιγμιότυπου pu_f , στο οποίο εισάγουμε στην διαδικασία P.Create συγκεκριμένες προκλήσεις (challenges) και καταγράφουμε κατά πόσο οι απαντήσεις (responses), τα αποτελέσματα δηλαδή της διαδικασίας P.Create είναι τα αναμενόμενα. Το σύνολο αυτών των απαντήσεων

(responses) ορίζεται ως Y_P και η διαδικασία της αξιολόγησης του στιγμιότυπου (instance) puf , ως $puf(x).Eval$.

Οπότε, συμπερασματικά, μέσω του πειράματος της αξιολόγησης επιδιώκεται να διευκρινιστεί κατά πόσο μία κλάση P δύναται να κοινοποιηθεί και επιπλέον να εκτιμηθεί η μοναδικότητά της.

Ένα πείραμα μίας κλάσης P , είναι ένα πείραμα στο οποίο εφαρμόζεται ένα σύνολο προκλήσεων N_{chal} πάνω σε έναν αριθμό τυχαίων στιγμιότυπων N_{puf} μίας συγκεκριμένης κλάσης P , όπου καταγράφονται οι N_{meas} απαντήσεις (responses) της διαδικασίας $P.Create.x$

$$Y_{Exp(P)} = N_{meas} \leftarrow N_{chal} \times N_{puf}$$

Κρίσιμα μετρήσιμα μεγέθη για την αξιολόγηση της κλάσης P είναι η ενδο-ή (intra-distance) και η εξωτερική απόσταση ή μεσοδιάστημα (inter-distance).

Εσωτερική απόσταση (intra-distance)¹²

Η εσωτερική απόσταση είναι μία μεταβλητή που περιγράφει την απόκλιση (απόσταση) μεταξύ δύο διαφορετικών απαντήσεων (responses) όταν εφαρμόζεται η ίδια ακριβώς πρόκληση (challenge) σε ένα μόνο συγκεκριμένο puf μίας κλάσης P και ορίζεται ως D_P^{intra} .

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

Η κατανομή της εσωτερικής απόστασης μίας κλάσης P φανερώνει την πιθανότητά της να αναπαραχθεί ακριβώς η ίδια. Αυτό από μόνο του καθιστά την εσωτερική απόσταση ως ένα από τα βασικότερα μετρήσιμα μεγέθη της ποιότητας μίας κλάσης P .

Ο υπολογισμός και η μελέτη των στατιστικών στοιχείων των διαφόρων δειγμάτων-απαντήσεων (responses), όπως η μέση τιμή κατανομής, η τυπική απόκλιση, το ιστόγραμμα και λογαριασμοί τάξεως παρέχουν μία ολοκληρωμένη εικόνα για τον υπολογισμό και την εκτίμηση της εσωτερικής απόστασης μίας κλάσης P .

Επίσης, είναι εξίσου σημαντικό να ληφθεί υπόψη, κατά τον υπολογισμό της εσωτερικής απόστασης μίας κλάσης P , το πώς αυτή μεταβάλλεται με τις ταυτόχρονες μεταβολές των περιβαλλοντικών μεταβλητών. Είναι γενική παραδοχή ότι η εσωτερική απόσταση μεταξύ δύο διαφορετικών απαντήσεων είναι μεγαλύτερη όταν ένα ενδεχόμενο puf μίας κλάσης P υπόκειται στην ίδια πρόκληση (challenge),

¹ Στο βιβλίο του ο Maes για τη μέτρηση της εσωτερικής απόστασης χρησιμοποιεί την απόσταση Hamming.

² Κατά μία άλλη μετάφραση ενδο-απόσταση.

αλλά με διαφορετικές συνθήκες περιβάλλοντος η κάθε μια, παρά κάτω από ένα περιβάλλον όμοιων συνθηκών. Παραδείγματα τέτοιων συνθηκών που δύναται να επηρεάσουν την εσωτερική απόσταση είναι η θερμοκρασία, η τάση τροφοδοσίας της διάταξης pu_{if} κ.ά..

Η σχεδίαση και η αξιολόγηση διατάξεων pu_{if} επιβάλλει την εξέταση του παραπάνω παράγοντα. Ο υπολογισμός της εσωτερικής απόστασης μεταξύ των ακραίων τιμών (corner cases) περιβαλλοντικών συνθηκών, που εκτιμάται ότι η διάταξη θα εκτεθεί, φανερώνει τον τρόπο με τον οποίο αυτή συμπεριφέρεται εντός αυτού του εύρους λειτουργίας της.

Εξωτερική απόσταση (inter-distance)³

Η εξωτερική απόσταση (inter-distance) μίας κλάσης PUF ορίζεται ως μία μεταβλητή η οποία περιγράφει την απόσταση μεταξύ δύο απαντήσεων (responses) δύο διαφορετικών στιγμιοτύπων PUF, όταν αυτά υπόκεινται στην ίδια πρόκληση (challenge).

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

Όπως και η εξωτερική απόσταση είναι ένα εξίσου σημαντικό μέγεθος για μία κλάση P, η μελέτη του οποίου υποδεικνύει τη **μοναδικότητα (uniqueness)** του κάθε διαφορετικού στιγμιοτύπου PUF της κλάσης. Η στατιστική μελέτη των απαντήσεων, επίσης είναι οδηγός για τον υπολογισμό της εξωτερικής απόστασης.

Και στην εξωτερική απόσταση η μεταβολή των εξωτερικών συνθηκών έχουν σημαντική επίπτωση στον υπολογισμό αυτής. Ωστόσο, είναι κοινή πρακτική να μη λαμβάνεται υπόψη η μέτρησής της σε ακραίες τιμές των διαφόρων περιβαλλοντικών συνθηκών, αλλά να υπολογίζεται μόνο σε μία δεδομένη τιμή αναφοράς a_{ref} αυτών.

³ Κατά μία άλλη μετάφραση δια-απόσταση.

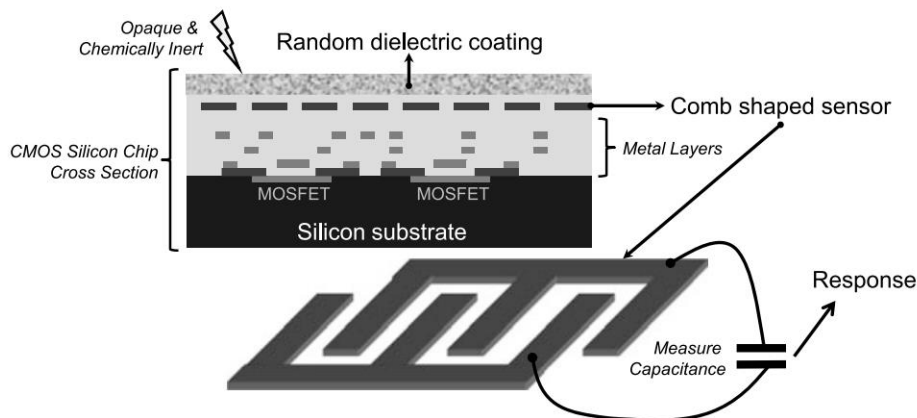
ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΤΩΝ PUFs

Μία γενική κατηγοριοποίηση των διαφόρων διατάξεων PUFs επιχειρείται να παρουσιαστεί ως εξής:

Με βάση την τεχνολογία ανάπτυξης της διάταξης:

Ηλεκτρονικά PUF

Στην κατηγορία αυτή εντάσσονται όλα τα PUFs των οποίων η κατασκευή βασίζεται στα ηλεκτρονικά χαρακτηριστικά του αντικειμένου προέλευσης, όπως είναι η αντίσταση και η χωρητικότητα αυτού. Η μέτρηση της χωρητικότητας στην επιφάνεια ενός ενσωματωμένου κυκλώματος είναι αντιπροσωπευτικό παράδειγμα των coating PUFs.



4

Εικόνα 1: Κατασκευή coating PUF (Tuyls et al.)

Μη ηλεκτρονικά PUF

Πρόκειται για PUFs των οποίων η προέλευσής τους προέρχεται από μη ηλεκτρονικές πηγές, όπως μπορεί να είναι για παράδειγμα το "αποτύπωμα" της ανάκλασης του φωτός στην επιφάνεια διατομής μίας οπτικής ίνας, χωρίς αυτό να προϋποθέτει ότι η επεξεργασία της απόκρισης δεν πραγματοποιείται με ηλεκτρονικά μέσα.

PUF πυριτίου

Αποτελεί μία υποκατηγορία ηλεκτρονικών PUF με ιδιαίτερο ενδιαφέρον, για τον λόγο ότι η κατασκευή τους αποτελεί μέρος ενός ενσωματωμένου κυκλώματος, επομένως και η ρυθ συμπεριφορά τους είναι ενσωματωμένη σε αυτό.

⁴ R. Maes, Physically Unclonable Functions (Constructions, Properties and Applications), Springer, 2013

Με βάση τις ιδιότητες κατασκευής τους:

Εγγενή

Στα εγγενή PUF εμπίπτουν όσες διατάξεις πληρούν ταυτόχρονα τις δύο εξής προϋποθέσεις πρώτον, οι μετρήσεις υλοποιούνται από ενσωματωμένη διάταξη και δεύτερον, τα τυχαία χαρακτηριστικά τους εισάγονται κατά τη διαδικασία παραγωγής τους. Όλες οι προτεινόμενες διατάξεις της κατηγορίας αυτής προέρχονται από πυρίτιο (silicon-based).

Μη- εγγενή PUFs

Σε αντίθεση με τα εγγενή PUF, στην κατηγορία αυτή εντάσσονται διάφορες διατάξεις των οποίων τα ζητούμενα χαρακτηριστικά εξετάζονται και αξιολογούνται κατόπιν εξωτερικής παρέμβασης. Χαρακτηριστικό παράδειγμα μη εγγενών PUF είναι τα οπτικά, των οποίων τα τυχαία τους χαρακτηριστικά παρατηρούνται εξωτερικά της διάταξης, καθώς μία δέσμη ακτίνων διαθλάται κατά την πρόπτωση της σε μία διάφανη επιφάνεια.

Επιπλέον των παραπάνω κατηγοριοποιήσεων, τα PUFs διακρίνονται ανάλογα με τα χαρακτηριστικά ασφάλειάς τους σε δυνατά και αδύναμα. Η διαφοροποίησή τους έχει να κάνει με την πιθανότητα πρόβλεψής και αναπαραγωγής τους. Στα δυνατά PUFs εντάσσονται εκείνες οι διατάξεις οι οποίες είναι αδύνατο να προβλεφθεί το αποτέλεσμα μίας πρόκλησης (challenge) στην οποία υποβάλλεται η διάταξη. Εξ ορισμού όλα τα δυνατά PUFs διαθέτουν μία συλλογή μεγάλου αριθμού προκλήσεων.

Δεδομένου ότι το περιεχόμενο της εργασίας αφορά τα SRAM PUFs, μία υποκατηγορία των εγγενών PUFs, θα εστιάσουμε σε αυτά και θα ακολουθήσει μία σύντομη περιγραφή των εγγενών διατάξεων που έχουν προταθεί και των οποίων η τυχειότητα που εμφανίζεται στη συμπεριφορά, τους είναι αποτέλεσμα εντελώς απρόβλεπτων και μη ελέγξιμων καταστάσεων και διεργασιών κατά το στάδιο της παραγωγής τους.

Επιπρόσθετα, τα εγγενή PUF, με βάση τις αρχές και τον τρόπο λειτουργίας τους, διακρίνονται σε επιπλέον τρεις υποκατηγορίες:

- Delay-based, όπου κύριο στοιχείο τους είναι οι μεταβολές στην καθυστέρηση των ψηφιακών κυκλωμάτων.
- Memory-based, οι διατάξεις των οποίων αξιοποιούν τη διαφοροποίηση μεταξύ ίδιων διατάξεων σε ό,τι αφορά τη συμπεριφορά των εξαρτημάτων μνήμης που εμπεριέχουν.
- Διατάξεις οι οποίες μετατρέπουν σε ψηφιακά, με τη χρήση αναλογικού/ψηφιακού μετατροπέα, τυχαία εγγενή αναλογικά σήματα.

Delay-based PUFs

PUF "Κριτής" (Arbiter PUFs)

Ανήκουν στη κατηγορία των delay-based PUFs και προτάθηκαν από τον Lee. Σε μία προσπάθεια ακριβής απόδοσης στην ελληνική του όρου, θα λέγαμε ότι πρόκειται για ένα PUF "κριτή". Η λειτουργία του βασίζεται στην εξής υπόθεση:

Στην ίδια διάταξη έχουν σχεδιαστεί δύο ψηφιακές "διαδρομές", οι οποίες συναγωνίζονται με βάση την καθυστέρηση άφιξης σε ένα κύκλωμα "κριτή". Εφόσον οι δύο διαδρομές έχουν σχεδιαστεί κατά τέτοιο τρόπο ώστε η καθυστέρηση που εισάγουν να είναι σχεδόν, αλλά όχι ακριβώς, ίδια, αυτό συνεπάγεται ότι δεν μπορεί να προκαθοριστεί ή να προβλεφθεί κατά το στάδιο της παραγωγής το ακριβές αποτέλεσμα, δηλαδή ποια είναι όντως η πιο "γρήγορη διαδρομή", εισάγοντας κατά αυτόν τον τρόπο μία εντελώς τυχαία κατάσταση λειτουργίας κατά το στάδιο της παραγωγής εισάγεται

Εκ των πραγμάτων, τα arbiter pufs είναι ξεχωριστά για κάθε συσκευή και παρουσιάζουν την ίδια συμπεριφορά κατά τη διάρκεια λειτουργίας τους, χωρίς να μεταβάλλεται η απόφαση και το αποτέλεσμα του κυκλώματος "κριτή". Μολονότι η συγκεκριμένη κατηγορία εγγενών PUF διαθέτει αυτήν την ικανότητα να διατηρούν την σταθερότητα του αποτελέσματος, υπάρχουν περιπτώσεις, στις οποίες η διαφορά στην καθυστέρηση είναι μηδαμινής κλίμακας, σε σημείο που η απόφαση του κυκλώματος "κριτή" να κινείται πάνω στο όριο (threshold) των δύο αποτελεσμάτων (0 ή 1). Συνυπολογίζοντας ταυτόχρονα διάφορες άλλες παραμέτρους κατά τη διάρκεια της πρόκλησης (challenge), όπως παράδειγμα η θερμοκρασία, οι οποίες δύνανται να επηρεάσουν το αποτέλεσμα κατά περίπτωση, οδηγεί σε μία αστάθεια του PUF, μετατοπίζοντας άλλοτε την απόφαση στο 0 και άλλοτε στο 1.

Η απλούστερη διάταξη PUF τέτοιου είδους αποτελείται από Set-Reset (S-R) Latches, τα οποία είναι ψηφιακά κυκλώματα με δύο εισόδους σημάτων και διαθέτουν την ιδιότητα να αποθηκεύουν ένα bit πληροφορίας και να διατηρούν αποθηκευμένη την πληροφορία έως ότου ανατροφοδοτηθούν οι είσοδοι από νέα σήματα.

Η προτεινόμενη από τον Lee διάταξη arbiter βασίζεται στη σύγκριση καθυστερήσεων μεταξύ δύο παράλληλων μονοπατιών σημάτων, τα οποία διαμορφώνονται δυναμικά με βάση μια συμβολοσειρά πρόκλησης (challenge). Κάθε στάδιο της διάταξης περιλαμβάνει ζεύγη διασταυρούμενων multiplexers, των οποίων ηδρομολόγηση ελέγχεται από τα bits της πρόκλησης. Στο τέλος των μονοπατιών, ένας διαιτητής (arbiter), συνήθως υλοποιημένος ως flip-flop, συγκρίνει

ποιο σήμα φτάνει πρώτο και παράγει ένα bit ως απάντηση. Οι μικρές, αναπόφευκτες μεταβολές στην καθυστέρηση των διαδρομών λόγω κατασκευαστικών ανομοιοτήτων προσδίδουν μοναδικότητα σε κάθε φυσική υλοποίηση, καθιστώντας τον Arbiter PUF κατάλληλο για εφαρμογές αυθεντικοποίησης και παραγωγής κρυπτογραφικών κλειδίων.

PUF Ταλαντωτή Δακτυλίου (Ring Oscillator PUFs)

Πρόκειται επίσης για άλλη μία delay-based προτεινόμενη διάταξη. Η αρχή λειτουργίας τους είναι παρόμοια με τα arbiter pufs, μόνο που σε αυτήν την περίπτωση χρησιμοποιούνται ταλαντωτές δακτυλίου (ring oscillators) και μετρητές συχνότητας. Μη ελέγξιμες μεταβλητές στο στάδιο της παραγωγής εισάγουν έναν βαθμό τυχαιότητας στην ακριβή συχνότητα ταλάντωσης των ταλαντωτών δακτυλίου. Συνεπώς καθίσταται απίθανη η ακριβής αναπαραγωγή δύο όμοιων τέτοιων ηλεκτρονικών στοιχείων.

Χαρακτηριστικό των ταλαντωτών δακτυλίου είναι ο υψηλός βαθμός επιρροής της θερμοκρασίας περιβάλλοντος, καθώς και της τάσης λειτουργίας, στην ακρίβεια και σταθερότητα των ιδιοτήτων τους ως διατάξεις PUF. Για τη βελτίωση της αυτής συμπεριφοράς τους, έχουν προταθεί διάφορες διατάξεις, με την χρήση είτε ζευγών ταλαντωτών και σύγκριση των αποτελεσμάτων τους, είτε μεγάλου πλήθους ταλαντωτών (σύνηθες σε FPGA κυκλώματα), με φανερό αντίκτυπο τόσο στις υψηλές απαιτήσεις πρόσθετων πόρων, όσο και στην πολυπλοκότητα της αρχιτεκτονικής τους.

PUF Παρεμβολών (Glitch PUFs)

Τα glitch Pufs δανείζονται τον ορισμό και βασίζουν την λειτουργία τους εκμεταλλευόμενα τις παρεμβολές (glitches) που εμφανίζονται στα ψηφιακά κυκλώματα. Τα glitches είναι ανεπιθύμητα φαινόμενα τα οποία δημιουργούνται εξαιτίας καθυστερήσεων που δημιουργούνται κατά τη μετάδοση σημάτων μέσω ενός συνδυαστικού αποτελούμενο από αριθμός λογικών πυλών ψηφιακού κυκλώματος. Επί της ουσίας, η καθυστερημένη άφιξη ενός σήματος επιβάλλει την λανθασμένη απάντηση στην έξοδο του κυκλώματος, η οποία αναφέρεται ως παρεμβολή (glitch).

Κατασκευαστικές και περιβαλλοντικές συνθήκες εξωθούν τα ψηφιακά κυκλώματα στην εμφάνιση αυτού του φαινομένου κατά εντελώς τυχαίο και απρόβλεπτο τρόπο, γεγονός το οποίο τα καθιστά ιδανικά στην χρήση τους ως διατάξεις PUF. Σε αυτές τις διατάξεις σκοπός είναι να εντοπιστούν κυκλώματα τα οποία εμφανίζουν σταθερή (παρότι εντελώς τυχαία) συμπεριφορά στην εμφάνιση των glitches. Ταυτόχρονα, με τη χρήση επιπρόσθετων τεχνικών (bit masking) επιχειρείται η επίτευξη αυτής της σταθερότητας σε κυκλώματα τα οποία εμφανίζουν ένα βαθμό αστάθειας.

Memory-based PUFs

SRAM PUFs

Τα PUF στατικής μνήμης τυχαίας προσπέλασης (Static Random Access Memory-SRAM) αποτελούν το βασικό αντικείμενο μελέτης της παρούσας εργασίας και για τον σκοπό αυτό θα επιχειρηθεί να παρουσιαστεί αναλυτικότερα.

Αποτελούν έναν τύπο PUF της memory-based κατηγορίας και ο τρόπος λειτουργίας τους βασίζεται στην ικανότητα αποθήκευσης μίας εκ των δύο καταστάσεων (0,1) κατά την έναρξη λειτουργίας τους. Η SRAM κατατάσσεται ως πτητική (volatile) μνήμη επειδή χάνει τις αποθηκευμένες πληροφορίες όταν αφαιρείται η τροφοδοσία. Αυτή η χαρακτηριστική ιδιότητα περιορίζει τη χρήση της σε εφαρμογές μακροχρόνιας αποθήκευσης, αλλά την καθιστά ιδανική για γρήγορη μνήμη cache σε CPU και άλλες ψηφιακές συσκευές όπου η γρήγορη πρόσβαση στα δεδομένα είναι κρίσιμη.

Η πιο κοινή μορφή SRAM είναι το κελί 6 τρανζίστορ (6T), το οποίο αποτελείται από 6 MOSFETS και είναι σχεδιασμένο να αποθηκεύει ένα bit πληροφορίας. Η βασική δομή της SRAM περιλαμβάνει δύο CMOS inverters και δύο τρανζίστορ πρόσβασης, που συνεργάζονται για να επιτρέψουν γρήγορη ανάγνωση και εγγραφή δεδομένων. Το βασικότερο τμήμα του κελιού αποτελείται από δύο διασταυρωμένα CMOS inverters. Κάθε inverter περιλαμβάνει έναν p-channel και έναν n-channel MOSFET. Αυτή η διάταξη δημιουργεί έναν θετικό βρόχο ανάδρασης, επιτρέποντας στο κελί να διατηρεί την τρέχουσα λογική του κατάσταση (0 ή 1) όσο παραμένει τροφοδοτούμενο με ρεύμα. Δύο επιπλέον τρανζίστορ προσπέλασης επιτρέπουν την ανάγνωση και την εγγραφή ενός bit πληροφορίας στη μνήμη.

Η διάταξη των δύο CMOS inverters κατά τη διάρκεια τροφοδοσίας έχει τρία πιθανά σημεία λειτουργίας, δύο σταθερά (stable) και ένα μεταστατικό (metastable). Τα σταθερά σημεία είναι οι καταστάσεις 0 και 1 και οι οποίες αντιπροσωπεύουν τις λογικές τιμές που αποθηκεύονται στο κελί. Αυτές οι καταστάσεις είναι ανθεκτικές σε μικρές παρεμβάσεις ή θόρυβο, καθώς σε περίπτωση οποιασδήποτε διαταραχής το κύκλωμα επιστρέφει στην αρχική του κατάσταση. Το κύκλωμα μπορεί να παραμείνει προσωρινά στο μεταστατικό σημείο λειτουργίας, πριν καταλήξει σε μία από τις δύο σταθερές καταστάσεις. Στην κατάσταση αυτή τα SRAM κελιά καθίστανται ευαίσθητα σε θορύβους, γεγονός που μπορεί να οδηγήσει σε αλλαγές στην αποθηκευμένη πληροφορία.

Latch PUFs

Μία παρόμοια προσέγγιση memory-based PUF χρησιμοποιεί τα SR-latches (Set-Reset) latches, τα οποία στη γενική τους κατασκευαστική μορφή αποτελούνται από δύο πύλες NOR ή NAND. Η ενεργοποίηση ενός σήματος στην είσοδο επαναφοράς (reset) ενός SR latch ρυθμίζει την έξοδό του σε χαμηλή κατάσταση ($Q=0$). Όταν απελευθερωθεί το σήμα επαναφοράς, αν δεν ενεργοποιηθούν άλλες είσοδοι, το latch διατηρεί αυτή την κατάσταση μέχρι να γίνουν περαιτέρω αλλαγές.

Το πρακτικό πλεονέκτημα των latch PUFs σε σύγκριση με τα SRAM PUFs έγκειται στην ικανότητά τους να παράγουν μοναδικές απαντήσεις χωρίς να εξαρτώνται από μια συγκεκριμένη κατάσταση εκκίνησης. Σε αντίθεση με τα SRAM PUFs, τα οποία απαιτούν να είναι η συσκευή ενεργοποιημένη και αρχικοποιημένη για να παραγάγουν σταθερές εξόδους, τα latch PUFs μπορούν να ενεργοποιηθούν οποιαδήποτε στιγμή όσο η συσκευή είναι σε λειτουργία. Αυτή η ευελιξία επιτρέπει πιο ποικιλόμορφες εφαρμογές στην ασφαλή ταυτοποίηση και στα κρυπτογραφικά συστήματα.

Flip-Flop PUFs

Μία παραλλαγή των D-Latch PUFs είναι τα Flip-Flop, τα οποία συναντώνται ως επί το πλείστον σε FPGA συστήματα. Ενώ τα πρώτα βασίζονται στην τιμή αποθήκευσης κατά την διαδικασία εκκίνησης-τροφοδοσίας τους, στην δεύτερη περίπτωση πραγματοποιείται μία προ-επεξεργασία των δεδομένων. Συγκεκριμένα, ομαδοποιούνται γειτονικά Flip-Flop Latches και διενεργείται μία πλειοψηφική ψηφοφορία των δυαδικών τιμών τους για επαναλαμβανόμενες μετρήσεις. Το αποτέλεσμα της ψηφοφορίας καθορίζει και την τιμή που αποδίδεται στην εκάστοτε ομάδα. Ο τρόπος αυτός προσέγγισης βελτιώνει το χαρακτηριστικό της μοναδικότητας της PUF διάταξης.

Butterfly PUFs

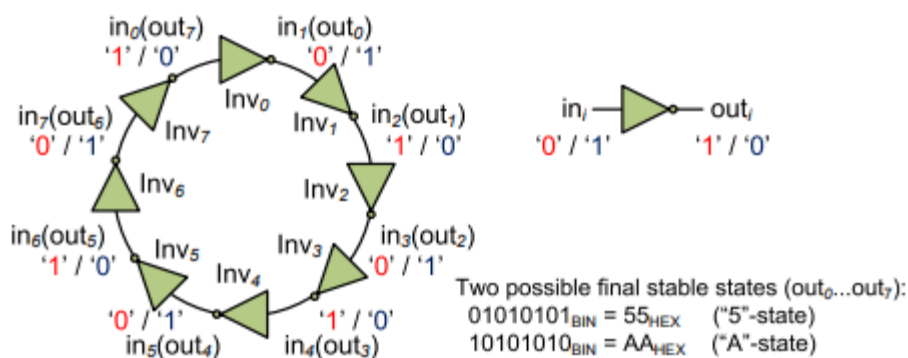
Οι μνήμες sram δε μπορούν να αξιοποιηθούν ως διατάξεις PUF στα κυκλώματα fpga, και αυτό διότι τα fpga εξαναγκάζουν σε μηδενισμό των τιμών στις sram αμέσως μετά την τροφοδοσία τους. Τα Butterfly PUFs προσφέρουν μια ελκυστική εναλλακτική λύση σε σχέση με άλλους τύπους PUFs, συνδυάζοντας την ανθεκτικότητα στην πλαστογραφία με την απλότητα σχεδίασης και την αποτελεσματικότητα. Αυτοί οι τύποι PUFs βασίζονται σε μια αρχιτεκτονική που ονομάζεται "Butterfly", η οποία εκμεταλλεύεται τις φυσικές παραλλαγές στις ηλεκτρονικές διατάξεις για να δημιουργήσει μοναδικές και μη επαναλήψιμες απαντήσεις σε προκλήσεις.

Buskeeper PUFs

Πρόκειται για διατάξεις με PUF συμπεριφορά. Συνήθως αποτελούνται από ένα απλό λατς, συνδεδεμένο σε έναν δίαυλο ενσωματωμένου κυκλώματος, με την ιδιότητα να διατηρεί την κατάσταση του τελευταίου bit πληροφορίας που διακινήθηκε στον δίαυλο. Ένα πλεονέκτημα που παρουσιάζουν τα buskeeper PUFs είναι το μικρότερο μέγεθός τους σε σχέση με τα D Flip-Flops και τα συνηθισμένα latches.

Bistable Ring PUFs (Δισταθές PUF Δακτυλίου)

Ένας συνδυασμός Ταλαντωτή δακτυλίου και SRAM PUF είναι και το δισταθές PUF δακτυλίου. Η βασική του δομή παρουσιάζεται από έναν δακτύλιο αποτελούμενο από περιττό αριθμό λογικών πυλών αντιστροφών (inverters). Κατά τη διαδικασία εκκίνησης της τροφοδοσίας του, ή γενικά κατά τη μετάβαση από μία ασταθή κατάσταση, η διάταξη αυτή εμφανίζει την τάση να λαμβάνει και να διατηρεί συγκεκριμένη τιμή, κατά τον ίδιο τρόπο με τις SRAM



5

Εικόνα 2: Δύο πιθανές καταστάσεις ενός Bistable Ring PUF

Κατασκευές PUF Μεικτού Σήματος (Mixed Signal PUF Constructions)

Πέρα των προαναφερθέντων διατάξεων PUF, οι οποίες εκμεταλλεύονται τα χαρακτηριστικά PUF που παρουσιάζουν κατά την επεξεργασία των ψηφιακών σημάτων που διακινούνται μέσω αυτών και πιθανών καταστάσεων τιμών που λαμβάνουν ενσωματωμένα σε αυτές λογικά κυκλώματα, μία ξεχωριστή κατηγορία PUF αποτελούν τα επονομαζόμενα PUF μεικτού σήματος. Στα υπόψη PUF πραγματοποιείται εκμετάλλευση αναλογικών σημάτων/ χαρακτηριστικών

⁵ https://www.researchgate.net/figure/Two-possible-stable-states-of-an-eight-stage-bistable-ring_fig2_221337250

των ενσωματωμένων διατάξεων και αναλογικό - ψηφιακή μετατροπή αυτών στην πορεία. Προτεινόμενες διατάξεις αυτού του είδους είναι τα Integrated Circuit Identification (ICID), Inverter Gain, Super High Information Content και τα SRAM failure PUFs.

ΑΞΙΟΛΟΓΗΣΗ PUF ΔΙΑΤΑΞΕΩΝ

Για την αξιολόγηση των διαφόρων διατάξεων PUF ως κύρια μετρήσιμα μεγέθη χρησιμοποιείται η εσωτερική απόσταση (intra-distance) και η εξωτερική απόσταση (inter-distance), όπως ορίστηκαν προηγουμένως. Εκτός από τα συγκεκριμένα μεγέθη, είναι σημαντικό να εξετάζονται και άλλες μετρήσεις ποιότητας, όπως η μοναδικότητα, η αξιοπιστία, η τυχαιότητα και η σταθερότητα. Αυτές οι επιπλέον μετρήσεις παρέχουν μια πιο ολοκληρωμένη εικόνα της απόδοσης των PUFs και της πρακτικής τους εφαρμογής σε πραγματικά σενάρια. Έτσι, μια ολιστική αξιολόγηση των PUFs απαιτεί τη συστηματική εξέταση αυτών των παραμέτρων για να εξασφαλιστεί η αποτελεσματικότητα και η ασφάλεια τους.

Ευκολία κατασκευής

Μια κατηγορία PUF θεωρείται κατασκευάσιμη αν είναι εύκολο να κληθεί η διαδικασία δημιουργίας της και να παραχθεί μια τυχαία εμφάνιση PUF.

$$puf \leftarrow P.Create(r^C \overset{\$}{\leftarrow} \{0,1\}^*)$$

Η κατασκευασιμότητα είναι απαραίτητη για την αξιολόγηση των PUFs και σχετίζεται με τη δυνατότητα κατασκευής τους σύμφωνα με τους νόμους της φυσικής, καθώς και με το κόστος παραγωγής τους.

Ευκολία Αξιολόγησης

Η ευκολία αξιολόγησης είναι μια ιδιότητα των PUF που υποδεικνύει ότι μία κατασκευάσιμη κατηγορία είναι, επίσης εύκολο να αξιολογηθεί για οποιαδήποτε τυχαία εμφάνιση PUF και πρόκληση. Το μέγεθος της ευκολίας αξιολόγησης εξαρτάται από την εφαρμογή και σχετίζεται με την ικανότητα εκτέλεσης αξιολογήσεων εντός καθορισμένων περιορισμών όπως ο χρόνος, η ισχύς και το κόστος.

Η αξιολόγηση είναι κρίσιμη για τη συζήτηση των PUFs, καθώς οι κατασκευές που δεν είναι αξιολογήσιμες παρουσιάζουν προβλήματα. Σε θεωρητικό επίπεδο, το "εύκολο" σημαίνει ολοκλήρωση σε πολυωνυμικό χρόνο, ενώ σε πρακτικό επίπεδο απαιτεί συμμόρφωση με τις λειτουργικές παραμέτρους που επιβάλλονται από τις εφαρμογές. Αυτή η διάκριση αναδεικνύει την πολυπλοκότητα της αξιολόγησης των PUFs σε διαφορετικά συμφραζόμενα.

Ευκολία Αναπαραγωγής

Μια κατηγορία PUF εμφανίζει αναπαραγωγιμότητα αν είναι αξιολογήσιμη και εφόσον η πιθανότητα η εσωτερική απόσταση να είναι μικρή αυξάνεται. Η αναπαραγωγιμότητα είναι κρίσιμη για τη διασφάλιση ότι τα PUFs μπορούν να παράγουν αξιόπιστα συνεπείς εξόδους, κάτι που είναι απαραίτητο για την αποτελεσματικότητα τους σε εφαρμογές ασφάλειας. Αν μια κατασκευή PUF δεν μπορεί να αναπαράγει σταθερά τις απαντήσεις, μπορεί να θέσει σε κίνδυνο τις εγγυήσεις ασφάλειας που αναμένονται από τη χρήση της. Επομένως, η κατανόηση και η μέτρηση της αναπαραγωγιμότητας είναι ζωτικής σημασίας για την αξιολόγηση της ανθεκτικότητας και της αξιοπιστίας των συστημάτων που βασίζονται σε PUF.

Μοναδικότητα

Η θεμελιώδης ιδιότητα ασφάλειας των PUFs είναι η μοναδικότητα, η οποία αναφέρεται στην ικανότητα μιας απάντησης PUF να αντιπροσωπεύει μια μέτρηση ενός τυχαίου και συγκεκριμένου χαρακτηριστικού της εμφάνισης.

Μια κατηγορία PUF εμφανίζει μοναδικότητα αν είναι αξιολογήσιμη και αν η πιθανότητα η εσωτερική απόσταση να είναι μεγάλη, αυξάνεται. Αυτό σημαίνει ότι με υψηλή πιθανότητα, οι απαντήσεις από την αξιολόγηση της ίδιας πρόκλησης σε διαφορετικές κατασκευές PUF θα πρέπει να είναι μη παρόμοιες, δηλαδή μακριά η μία από την άλλη σύμφωνα με το μέτρο απόστασης. Η μοναδικότητα αξιολογείται γενικά υπό κανονικές συνθήκες λειτουργίας, επομένως δεν χρειάζεται να επεκταθεί αυτός ο ορισμός για μεταβαλλόμενες συνθήκες αξιολόγησης. Ένας υψηλός βαθμός μοναδικότητας μειώνει την πιθανότητα συγκρούσεων—περιπτώσεις όπου διαφορετικές PUFs παράγουν την ίδια απάντηση—ενισχύοντας έτσι την ασφάλεια. Συνοψίζοντας, η μοναδικότητα είναι μια κρίσιμη ιδιότητα για τα PUFs, επιτρέποντάς τους να λειτουργούν ως αξιόπιστοι αναγνωριστές σε εφαρμογές ασφάλειας διασφαλίζοντας ότι οι απαντήσεις είναι διακριτές μεταξύ διαφορετικών εμφανίσεων.

Ευκολία αναγνώρισης

Μια κατηγορία PUF χαρακτηρίζεται από την ιδιότητα της ευκολίας αναγνώρισης όταν χαρακτηρίζεται, επίσης, από υψηλή ευκολία αναπαραγωγής και επιπλέον υψηλή μοναδικότητα. Αυτό υποδηλώνει ότι οι απαντήσεις από ένα συγκεκριμένο ενδεχόμενο ruf (σε σχέση με την ίδια πρόκληση) είναι πιο παρόμοιες μεταξύ τους από ό,τι οι απαντήσεις από διαφορετικά ενδεχόμενα. Κατά συνέπεια, τα ενδεχόμενα ruf μπορούν να καθορίσουν μια στατική ταυτότητα που είναι πολύ

πιθανό να είναι μοναδική. Η δυνατότητα αναγνώρισης μιας κατηγορίας PUF εκτιμάται συχνά γρήγορα συγκρίνοντας τις μέσες παρατηρούμενες εσωτερικές και εξωτερικές αποστάσεις (inter/intra distances). Τέτοιες στατιστικές πληροφορίες είναι κρίσιμες για να διασφαλιστεί ότι οι διατάξεις PUF μπορούν να λειτουργήσουν αξιόπιστα ως μοναδικοί αναγνωριστές σε εφαρμογές ασφάλειας. Η αναγνωρισιμότητα είναι μια κρίσιμη ιδιότητα για τις διατάξεις PUF, επιτρέποντάς τους να διακρίνονται η μία από την άλλη με βάση τις απαντήσεις τους. Διασφαλίζοντας ότι οι απαντήσεις από το ίδιο ενδεχόμενο είναι πιο παρόμοιες από αυτές που προέρχονται από διαφορετικά ενδεχόμενα, οι διατάξεις PUF μπορούν να παρέχουν ένα αξιόπιστο μέσο αναγνώρισης σε διάφορα πρωτόκολλα ασφάλειας.

Ιδιότητα "μη Κλωνοποίησης"

Για να διασφαλιστεί η ιδιότητα μοναδικότητας των Φυσικών Μη Αντιγράφων Λειτουργιών (PUFs) παρουσία ενός αντιπάλου που μπορεί να επηρεάσει τη διαδικασία δημιουργίας, μπορούν να εφαρμοστούν αρκετές στρατηγικές. Αυτός ο αντίπαλος θα μπορούσε να χειριστεί τις συνθήκες, τις παραμέτρους και τις πηγές τυχαιότητας κατά τη διάρκεια της δημιουργίας των PUF, οδηγώντας ενδεχομένως σε περιπτώσεις που είναι πιο παρόμοιες από όσο αναμενόταν.

Μια κατηγορία PUF P παρουσιάζει φυσική μη αντιγραφή αν είναι αξιολογήσιμη και αν είναι δύσκολο να εφαρμοστεί και/ή να επηρεαστεί η διαδικασία δημιουργίας P . Create με τέτοιο τρόπο ώστε να παραχθούν δύο διακριτές περιπτώσεις PUF $ruf1$ και $ruf2$ για τις οποίες ισχύει ότι:

$$\Pr(\text{dist}[Y \leftarrow puf(X); Y' \leftarrow puf'(X)] < D_p^{\text{inter}}(X) \text{ is high, for } X \leftarrow X_P)$$

Η δυσκολία παραγωγής ενός μη μοναδικού ζεύγους PUF, όπως περιγράφεται στον ορισμό, συνδυαζόμενη με την κατασκευασιμότητα, η φυσική μη αντιγραφή μπορεί να συνοψιστεί ως εξής: είναι εύκολο να δημιουργηθεί μια τυχαία PUF, αλλά δύσκολο να δημιουργηθεί μια συγκεκριμένη. Μια κατηγορία PUF που παρουσιάζει φυσική μη αντιγραφή έχει το ενδιαφέρον πλεονέκτημα ασφάλειας ότι ακόμη και ο γνήσιος κατασκευαστής των PUF δεν έχει τρόπο να παραβιάσει την ιδιότητα της μη κλωνοποίησης.

Αδυναμία Πρόβλεψης

Πολλές εφαρμογές των PUF βασίζονται στη λειτουργία πρόκλησης-απάντησης τους, δηλαδή στην ικανότητα υποβολής μιας πρόκλησης και λήψης μιας τυχαίας απάντησης σε αντάλλαγμα. Σε αυτό το πλαίσιο, ενώ η μοναδικότητα και, κατά

συνέπεια, η φυσική μη αντιγραφή είναι σημαντικές, μπορεί να μην είναι επαρκείς για να διασφαλίσουν την ασφάλεια. Είναι επίσης απαραίτητο να διασφαλιστεί η αδυναμία πρόβλεψης μεταξύ των απαντήσεων που παράγονται από μια μόνο περίπτωση PUF.

Μια κατηγορία PUF παρουσιάζει μη προβλεψιμότητα αν είναι αξιολογήσιμη και αν είναι δύσκολο να κερδίσει κανείς το παρακάτω παιχνίδι για ένα τυχαίο ενδεχόμενο ruf :

- Σε μια φάση εκμάθησης, επιτρέπεται η αξιολόγηση του ruf σε περιορισμένο αριθμό προκλήσεων και η παρατήρηση των απαντήσεων.
- Σε μια φάση πρόκλησης, παρουσιάζεται μια τυχαία πρόκληση. Απαιτείται να γίνει μια πρόβλεψη για την απάντηση σε αυτή την πρόκληση.

Το παιχνίδι κερδίζεται όταν::

$$\Pr(\text{dist}[Y_{pred} \leftarrow \text{predict}(X); Y \leftarrow ruf(X)] < D_p^{inter}(X) \text{ is high})$$

Ο αλγόριθμος πρόβλεψης έχει εκπαιδευτεί σε ένα προηγούμενα παρατηρηθέν σύνολο προκλήσεων και απαντήσεων στο ίδιο ενδεχόμενο ruf . Χρησιμοποιούμε μια περιγραφή βασισμένη σε παιχνίδι για την μη προβλεψιμότητα προκειμένου να αποφύγουμε να επιβάλουμε περιορισμούς στον αλγόριθμο πρόβλεψης, δηλαδή η μη προβλεψιμότητα ορίζεται σε σχέση με τον καλύτερο φανταστικό αλγόριθμο πρόβλεψης που μπορεί να κατασκευαστεί, να εκπαιδευτεί και να αξιολογηθεί εντός των δυνατοτήτων του αντιπάλου. Στην καλύτερη περίπτωση, μπορεί κανείς να δείξει ότι οι απαντήσεις σε διαφορετικές προκλήσεις είναι εντελώς ανεξάρτητες, πράγμα που σημαίνει ότι δεν μπορούν να προβλεφθούν από κανέναν αλγόριθμο πρόβλεψης. Ωστόσο, μια τόσο ισχυρή ποιότητα σπάνια μπορεί να αποδειχθεί για μια κατασκευή PUF και το καλύτερο που μπορεί κανείς να υποθέσει είναι ότι ισχύει για ορισμένα PUF με βάση μια φυσική κίνηση.

Για άλλες κατασκευές PUF, οι απαντήσεις δεν είναι ανεξάρτητες και η μη προβλεψιμότητα τους εξαρτάται από την υπολογιστική δυσκολία κατασκευής, εκπαίδευσης και αξιολόγησης ενός κατάλληλου αλγορίθμου πρόβλεψης. Σε αυτή την περίπτωση, η έκταση της μη προβλεψιμότητας μπορεί να εκτιμηθεί μόνο σε σχέση με την καλύτερα γνωστή επίθεση μοντελοποίησης, καθώς δεν υπάρχει εγγύηση ότι δεν υπάρχουν καλύτερες επιθέσεις. Αυτό είναι παρόμοιο με την κατάσταση για τις περισσότερες κρυπτογραφικές συμμετρικές πρωτότυπες, π.χ. έναν μπλοκ κρυπτογράφο όπως το AES, όπου ένα πρωτότυπο είναι ασφαλές μόνο όσο υποδεικνύεται από την καλύτερα γνωστή επίθεση. Η αρχή του

Kerckhoffs συνήθως ισχύει επίσης για τα PUFs, δηλαδή ένας αντίπαλος έχει πλήρη γνώση σχετικά με τις λεπτομέρειες σχεδίασης και υλοποίησης μιας συγκεκριμένης κατασκευής PUF, εκτός από τα τυχαία χαρακτηριστικά που εισάγονται κατά τη διαδικασία δημιουργίας.

Μαθηματική και Πραγματική Μη Κλωνοποίηση

Στον ορισμό της μη προβλεψιμότητας, ένας αντίπαλος περιορίζεται στο να μάθει έναν περιορισμένο αριθμό (πιθανώς τυχαίων) ζευγών πρόκλησης-απάντησης, τα οποία χρησιμοποιεί για να εκπαιδεύσει τον αλγόριθμο πρόβλεψης του. Αυτό είναι συνήθως το γεγονός σε ένα πρωτόκολλο βασισμένο σε πρόκληση-απάντηση, όπου ο αντίπαλος υποκλέπτει τις επικοινωνίες του πρωτοκόλλου. Ωστόσο, πρέπει να εξεταστεί ένα ισχυρότερο μοντέλο αντιπάλου όταν ο αντίπαλος έχει απεριόριστη φυσική πρόσβαση σε μια περίπτωση PUF. Αυτό σημαίνει ότι μπορεί να μάθει όσα περισσότερα ζευγάρια πρόκλησης-απάντησης είναι ικανός να αποθηκεύσει και πιθανώς να κάνει χρήσιμες παρατηρήσεις της περίπτωσης PUF πέρα από τη λειτουργικότητα πρόκλησης-απάντησης.

Μια κατηγορία PUF παρουσιάζει μαθηματική μη αντιγραφή αν είναι απρόβλεπτη, ακόμη και αν δεν υπάρχει περιορισμός πρόσβασης στην διάταξη PUF κατά τη διάρκεια της φάσης εκμάθησης (όπως περιγράφηκε προηγουμένως), εκτός από τις δικές του ικανότητες. Η μαθηματική μη αντιγραφή είναι επομένως η επέκταση της μη προβλεψιμότητας σε έναν αντίπαλο με απεριόριστη φυσική πρόσβαση σε μια διάταξη PUF. Είναι προφανές ότι η μαθηματική μη αντιγραφή υποδηλώνει την μη προβλεψιμότητα.

Μία άμεση προϋπόθεση για μια κατηγορία PUF να είναι μαθηματικά μη αντιγράψιμη είναι ότι το σύνολο προκλήσεων να είναι πολύ μεγάλο, κατά προτίμηση εκθετικό σε κάποια παραμετρο κατασκευής του PUF. Αν αυτό δεν ισχύει, ένας αντίπαλος με απεριόριστη φυσική πρόσβαση σε μια διάταξη PUF μπορεί να αξιολογήσει το πλήρες σύνολο προκλήσεων και να αποθηκεύσει τις παρατηρηθείσες απαντήσεις σε έναν πίνακα. Αυτός ο πίνακας στη συνέχεια λειτουργεί ως ένα τέλειο μοντέλο πρόβλεψης για την εξεταζόμενη διάταξη PUF και η ιδιότητα της μη προβλεψιμότητας παραβιάζεται. Το ίδιο επιχείρημα ισχύει αν το σύνολο προκλήσεων είναι μεγάλο, αλλά αν μπορεί να εκπαιδευτεί ένας σχεδόν τέλειος αλγόριθμος πρόβλεψης απαντήσεων με βάση ένα μικρό υποσύνολο αυτών των προκλήσεων.

Αληθινή Μη Αντιγραφή

Έχουμε ορίσει δύο διαφορετικές έννοιες μη αντιγραφής: τη φυσική και τη μαθηματική μη αντιγραφή. Και οι δύο περιγράφουν μια ιδιότητα με τον ίδιο στόχο, δηλαδή είναι δύσκολο να κλωνοποιηθεί μια περίπτωση PUF, αλλά από εντελώς διαφορετικές προοπτικές. Η φυσική μη αντιγραφή ασχολείται με πραγματικούς φυσικούς κλώνους των περιπτώσεων PUF, ενώ η μαθηματική μη αντιγραφή ασχολείται μόνο με την κλωνοποίηση της συμπεριφοράς πρόκλησης-απάντησης μιας διάταξης PUF. Για μια κατηγορία PUF να παρουσιάσει αληθινή μη αντιγραφή, πρέπει να πληρούνται και οι δύο ιδιότητες.

Μια κατηγορία PUF παρουσιάζει αληθινή μη αντιγραφή αν είναι τόσο φυσικά όσο και μαθηματικά μη αντιγράψιμη.

Ιδιότητα της Μονής Κατεύθυνσης

Έστω ένας φυσικά μη αντιγράψιμος μετασχηματισμός (PUF) και μία αυθαίρετα επιλεγμένη απάντηση (response) που προέρχεται από αυτόν. Θεωρείται ότι δεν υπάρχει αποδοτικός αλγόριθμος αντιστροφής ο οποίος, γνωρίζοντας την υλοποίηση του PUF και την εν λόγω απάντηση, να μπορεί να προσδιορίσει κάποια πρόκληση (challenge) που να παράγει την ίδια ή παρόμοια απόκριση.

Η ιδιότητα αυτή είναι ανάλογη με την κλασική έννοια της μονόδρομης συνάρτησης στην κρυπτογραφία, ωστόσο, στην περίπτωση των PUFs, επηρεάζεται επιπρόσθετα από την πρακτική διαστασιμότητα των χώρων προκλήσεων και απαντήσεων. Συγκεκριμένα, σε PUF κατασκευές με περιορισμένο πλήθος προκλήσεων, η αντιστροφή καθίσταται εφικτή μέσω εξαντλητικής αναζήτησης (brute-force). Αντίστοιχα, όταν ο χώρος απαντήσεων είναι μικρός, ένας επιτιθέμενος μπορεί να εντοπίσει αντιστροφή μέσω επαναλαμβανόμενων τυχαίων ερωτημάτων.

Συνεπώς, η έννοια της μονόδρομης λειτουργίας στους PUFs είναι ουσιαστικά συνδεδεμένη με το μέγεθος και την πολυπλοκότητα των διαστημάτων πρόκλησης-απόκρισης, πέραν της υπολογιστικής δυσκολίας της ίδιας της αντιστροφής.

Απόδειξη Παραποίησης

Η παρέμβαση (tampering) αναφέρεται στην εσκεμμένη και μόνιμη αλλοίωση της φυσικής ακεραιότητας ενός συστήματος, με σκοπό την τροποποίηση της λειτουργικότητάς του κατά μη εξουσιοδοτημένο τρόπο. Στην περίπτωση ενός

PUF, αυτό σημαίνει την πραγματοποίηση φυσικών μετασχηματισμών στην υλοποίηση του.

Τέτοιου είδους παρεμβάσεις αποτελούν σοβαρές επιθέσεις που μπορεί να οδηγήσουν είτε σε παράκαμψη μηχανισμών ασφαλείας, είτε σε διαρροή εμπιστευτικών δεδομένων.

Για να προστατευθεί ένα σύστημα από τέτοιες επιθέσεις, απαιτείται όχι μόνο η ανίχνευση της παρέμβασης, αλλά και η κατάλληλη αντίδραση, όπως π.χ. η καταστροφή κρίσιμων δεδομένων ή η πλήρης απενεργοποίηση της λειτουργίας. Κρίσιμη για την ανίχνευση είναι η έννοια των αποδείξεων παρέμβασης (proofs of tamper evidence): κάθε μεταβολή πρέπει να έχει μετρήσιμο και αναπόφευκτο αντίκτυπο στη συμπεριφορά του PUF.

Ορισμένες υλοποιήσεις PUF, ιδιαίτερα όσες βασίζονται σε ευαίσθητες φυσικές παραμέτρους, δεν μπορούν να παραβιαστούν χωρίς να προκληθεί εμφανής μεταβολή στη συμπεριφορά πρόκλησης-απάντησης (challenge-response).

Μια κατηγορία PUFs παρουσιάζει αποδείξεις παρέμβασης εάν, για οποιαδήποτε φυσική μεταβολή της μορφής:

$$\Pr(\text{dist}[Y \leftarrow \text{puf}(X); Y' \leftarrow \text{puf}'(X)] > D_p^{\text{intra}}(X)) \text{ is high,}$$

και σε ιδανική περίπτωση ταυτόχρονα,

$$\Pr(\text{dist}[Y \leftarrow \text{puf}(X); Y' \leftarrow \text{puf}'(X)] < D_p^{\text{inter}}(X)) \text{ is low}$$

ισχύει ότι:

- Η απόσταση μεταξύ των απαντήσεων πριν και μετά την αλλοίωση, είναι υψηλή (σημαντικά μεγαλύτερη από τη φυσική αναξιопιστία),
- ενώ η πιθανότητα να μοιάζει η αλλοιωμένη έκδοχή με μια νέα, τυχαία PUF

είναι χαμηλή.

Με απλά λόγια: οποιαδήποτε φυσική επέμβαση σε έναν PUF πρέπει να αλλοιώνει ουσιαστικά την συμπεριφορά του, σε σημείο που να φαίνεται ότι πρόκειται για άλλη συσκευή.

Η έννοια των αποδείξεων παρέμβασης είναι ορθολογικά ανεξάρτητη από τη φυσική μη αντιγραφή (physical unclonability):

- Η φυσική μη αντιγραφή διασφαλίζει ότι δύο διαφορετικοί PUFs δεν μπορούν να μοιάζουν περισσότερο απ' όσο είναι φυσιολογικά πιθανό.
- Οι αποδείξεις παρέμβασης διασφαλίζουν ότι ένας παραποιημένος PUF δεν μπορεί να μοιάζει με την αρχική του μορφή περισσότερο από όσο θα έμοιαζε ένας άλλος, διαφορετικός PUF.

Έτσι, οι PUFs με αποδείξεις παρέμβασης θεωρούνται αυτοπροστατευόμενοι: κάθε φυσική επέμβαση προκαλεί αλλοίωση της συμπεριφοράς, που μπορεί να ανιχνευθεί και να ενεργοποιήσει μηχανισμούς ασφαλείας.

Επιπλέον, τέτοιοι PUF μπορούν να ενσωματωθούν σε μεγαλύτερα συστήματα για να τα καταστήσουν ανθεκτικά σε παρεμβάσεις, ενσωματώνοντας τη λειτουργία τους στη φυσική ακεραιότητα του PUF.

ΤΕΧΝΙΚΕΣ ΚΑΙ ΒΕΛΤΙΩΣΗ

Για να καταστήσουμε τους PUF πιο ανθεκτικούς, αξιόπιστους και κατάλληλους για χρήση σε κρίσιμες εφαρμογές, εφαρμόζονται πολυάριθμες τεχνικές βελτίωσης:

Έλεγχος Power-Up (Power-Ramp Tuning & Stabilizing Readouts)

Μελέτες έχουν δείξει ότι η ταχύτητα και το σχήμα της τροφοδοσίας κατά την εκκίνηση επηρεάζουν σημαντικά τη σταθερότητα των SRAM PUF. Οι ελεγχόμενες τεχνικές “power-up control” (π.χ. περιορισμένες περιοχές ανάγνωσης, ρυθμιζόμενες κλίσεις τάσης) μειώνουν τον αριθμό ασταθών bit.

Ιονίζουσα Ακτινοβολία (TID – Total Ionizing Dose)

Ερευνητές πρότειναν τη χορήγηση μικρών δόσεων ιονίζουσας ακτινοβολίας σε εμπορικά SRAM chips, με στόχο τη μείωση της intra-chip απόστασης Hamming που προκαλείται από θόρυβο εκκίνησης.

Επιλογή Σταθερών Cells (Stable-Cell Selection)

Με βάση παρατηρήσεις ότι κάποια bits είναι εξ ορισμού πιο αξιόπιστα, εφαρμόζεται φίλτρο επιλογής. Με μεθόδους όπως systematic bit selection και convolution-based επεξεργασία, επιλέγονται μόνο όσα bits έχουν σχεδόν μηδενικό BER ανεξάρτητα από θερμοκρασία, τάση ή γήρανση (aging). Παράδειγμα μνημών όπως BCH δίνουν BER πολύ κοντά στο μηδέν.

Fuzzy Extractors & Error-Correction Codes

Τα Fuzzy Extractors (όπως BCH, Reed–Solomon, Golay, Polar codes) σχηματίζουν τη backbone των PUF συστημάτων με θόρυβο. Οι κώδικες βοηθούν στη διόρθωση bit-flips και εξασφαλίζουν ότι το ίδιο output μπορεί να αναπαραχθεί σταθερά — χωρίς απώλεια εντροπίας από τα **helper data**. Για παράδειγμα, το code-offset fuzzy extractor με BCH και Reed–Solomon έδειξε αξιοπιστία μέχρι 10^{-9} error rate.

Αντιμετώπιση Aging (Silicon Aging Compensation)

Η μακροπρόθεσμη χρήση προκαλεί drift: η αξιοπιστία συχνά μειώνεται ~19% μετά από δύο χρόνια λειτουργίας υπό φυσιολογικές συνθήκες. Οι anti-aging τεχνικές περιλαμβάνουν:

- Αναμετάδοση *thresholds* μέσω μεθόδων like continuous enrollment.
- *Ionization επανεκπαίδευση* (TID).
Με αυτές, η σταθερότητα μπορεί να διατηρηθεί για μακρά χρονική διάρκεια.

Memory-Combining PUFs (π.χ. SRAM + DRAM)

Ο συνδυασμός πολλαπλών μνήμων δημιουργεί μεγαλύτερο Challenge-Response χώρο και αυξάνει την ποικιλότητα. Εργασίες δείχνουν ότι η μίξη SRAM+DRAM βελτιώνει την αντοχή σε noise, ρύθμιση aging, ενώ επιτρέπει υψηλότερη ασφάλεια, ιδιαίτερα σε σχετικά μικρές μνήμες

LED-PUF: Ξεκλειδωμένες δυνατότητες σταθερότητας

Ο LED- PUF χρησιμοποιεί τοπικά προσαρμοσμένες ατέλειες (Directed Self- Assembly) για να επιτυγχάνει **0% intra-HD** χωρίς τη χρήση fuzzy extraction ή ECC – παρέχοντας παράλληλα ιδανική **εντροπία (~1)** και inter-distance $\approx 50\%$, με απλή αρχιτεκτονική και σταθερή συμπεριφορά.

ΠΕΙΡΑΜΑΤΙΚΗ ΚΑΤΑΣΚΕΥΗ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗ SRAM PUF

Προσέγγιση του Πειράματος

Στο συγκεκριμένο κεφάλαιο γίνεται μία προσπάθεια κατασκευής μίας διάταξης SRAM PUF και ταυτόχρονης ποιοτικής αξιολόγησης αυτού με τα παρακάτω φθηνά υλικά τα οποία βρίσκονται εύκολα στο εμπόριο:

- Μικροελεγκτής Arduino UNO Board



Εικόνα 3: Arduino UNO R3⁶

Πρόκειται για μία δημοφιλή πλακέτα η οποία χρησιμοποιείται ευρέως σε εκπαιδευτικές και πρωτότυπες ηλεκτρονικές κατασκευές. Χρησιμοποιεί τον μικροελεγκτή 8-bit ATmega328P της εταιρείας Microchip με τα παρακάτω χαρακτηριστικά λειτουργίας:

- Ονομαστική τάση λειτουργίας: 5V
- Ταχύτητα ρολογιού μικροελεγκτή: 16 MHz
- Αναλογικές/ψηφιακές είσοδοι: 6/14
- Μνήμες Flash/SRAM/EEPROM: 32/2/1 KB
- Πρωτόκολλα επικοινωνίας/διασύνδεσης: USB, UART, SPI, I2C

Αρχικά επιχειρήθηκε η υλοποίηση του πειράματος με πλακέτα Raspberry-Pi, ωστόσο στη συλλογή των δεδομένων εμφανίστηκαν αρκετές δυσκολίες με εντελώς διαφορετικές τιμές σε κάθε ξεχωριστή μέτρηση με αποτέλεσμα να εγκαταλειφθεί η προσπάθεια αυτή.

Αυτό οφείλεται εν μέρη στην πολυπλοκότητα της αρχιτεκτονικής, καθώς η συγκεκριμένη πλακέτα διαθέτει μικροεπεξεργαστή (και όχι μικροελεγκτή,

⁶ <https://store.arduino.cc/products/arduino-uno-rev3-smd>

όπως στο Arduino) και πρόκειται επί της ουσίας για έναν mini H/Y και στο γεγονός ότι πιθανώς οι μετρήσεις να προέρχονταν από την εσωτερική μνήμη της πλακέτας, χωρίς τη δυνατότητα να απομονωθεί.

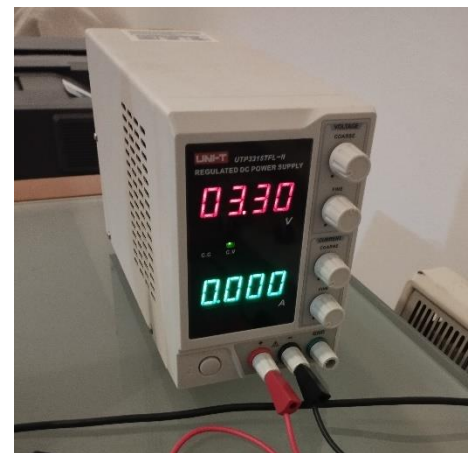
- Μνήμη SRAM Microchip 23K640 (SPI/DIP-8)



Εικόνα 4: Microchip SRAM 23K640⁷

Πρόκειται για μία στατική μνήμη SRAM της εταιρείας Microchip. Ένα από τα χαρακτηριστικά της είναι ότι η μνήμη είναι μη-πτητική (non-volatile), δηλαδή δε διατηρεί τα αποθηκευμένα δεδομένα της σε κάθε επανεκκίνηση, βασική προϋπόθεση για την χρήση της σε διατάξεις PUF. Επιπλέον βασικά χαρακτηριστικά όπως παρακάτω:

- Χωρητικότητα: 8KB (8192 x 8 bits)
- Πρωτόκολλο επικοινωνίας/διασύνδεσης: SPI
- Τάση λειτουργίας: 2.7V - 3.6V
- Καταστάσεις προσπέλασης: Byte/Sequential Mode
- Ταχύτητα λειτουργίας SPI: 20 MHz
- Ηλεκτρονικές αντιστάσεις.
- Καλώδια διασύνδεσης (jumper).
- Breadboard.
- Εξωτερικό γραμμικό (linear) τροφοδοτικό DC ρεύματος/ρυθμιζόμενης τάσης UNI-T (UTP3315TFL-II) με τα παρακάτω κύρια χαρακτηριστικά:
 - Έξοδος: 0–30V/0–5A
 - Ακρίβεια ρύθμισης: 10mV/1mA
 - Παραμόρφωση / Θόρυβος (Ripple & Noise):
 $\leq 2\text{mVrms}$
 - Καταστάσεις λειτουργίας: Constant Voltage (CV) - Constant Current (CC) modes



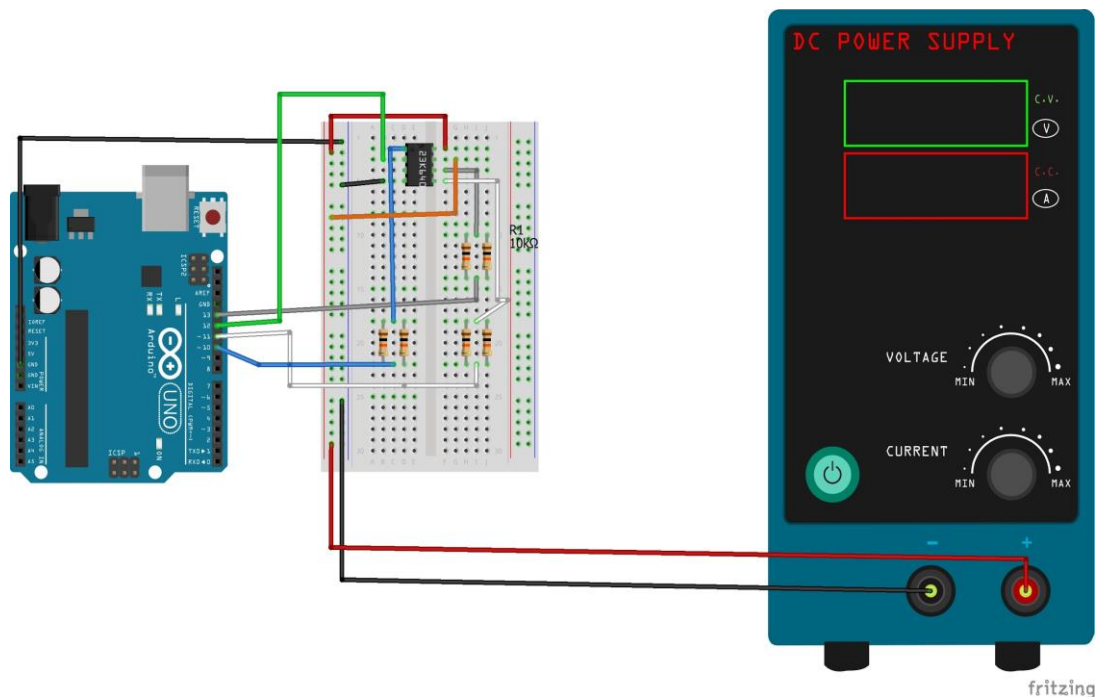
⁷ <https://www.microchip.com/en-us/product/23k640>

Εικόνα 5: Τροφοδοτικό UNI-T (UTP3315TFL-II)

Η κατασκευή και μελέτη περιλαμβάνει τα παρακάτω στάδια:

- Συνδεσμολογία των υλικών.

Η διασύνδεση των υλικών είναι πρωτίστης σημασίας, καθότι λάθη ή αστοχίες στο στάδιο αυτό μπορεί να επηρεάσουν την εξέλιξη του πειράματος σε τέτοιο βαθμό που μπορεί να οδηγήσει είτε σε εσφαλμένες μετρήσεις, αποτελέσματα και συμπεράσματα, είτε ακόμη και σε μη αναστρέψιμη καταστροφή των επιμέρους ηλεκτρονικών διατάξεων. Η διασύνδεση του Arduino board και της μνήμης SRAM υλοποιείται μέσω πρωτοκόλλου διασύνδεσης Serial Peripheral Interface (SPI).



Εικόνα 6: Γραφική απεικόνιση συνδεσμολογίας

- Σύνταξη και υλοποίηση του κώδικα.

Για τη συλλογή των μετρήσεων χρησιμοποιήθηκε η γλώσσα προγραμματισμού Arduino μέσα από το ομώνυμο IDE με χρήση πρωτοκόλλου επικοινωνίας SPI. Όλα τα συνταχθέντα προγράμματα του πειράματος παρατίθενται στο Παράρτημα Β.

- Συλλογή των δεδομένων.

Κατόπιν, συλλέγονται οι μετρήσεις και αποθηκεύονται σε εξωτερικό αρχείο για μετέπειτα επεξεργασία. Για την αξιολόγηση της διάταξης πραγματοποιήθηκαν μετρήσεις σε 3 διαφορετικές τιμές τάσης λειτουργίας της μνήμης SRAM (εντός των ορίων λειτουργίας που αναφέρεται στο φυλλάδιο λειτουργίας αυτής), στα 2.8V, 3V και 3.3V, ώστε να δύναται να αξιολογηθεί ο βαθμός που επηρεάζει η τάση λειτουργίας τα χαρακτηριστικά της μνήμης ως PUF.

Επιπλέον, συλλέχθηκαν τιμές από 2 διαφορετικές μνήμες SRAM Microchip 23K640 της ίδιας παρτίδας παραγωγής, όπως ταχυδρομήθηκαν από την εταιρία παραγωγής, με σκοπό τον έλεγχο του βαθμού αναπαραγωγιμότητας ίδιων χαρακτηριστικών PUF (αξιολόγηση intra-distance μετρήσεων).

Για κάθε μνήμη συλλέχθηκαν 50 επαναλαμβανόμενες τιμές σε κάθε τάση λειτουργίας για να ελεγχθεί η σταθερότητας παραγωγής των τιμών των εξεταζόμενων κελιών της μνήμης.

Η θερμοκρασία είναι ένας επιπλέον παράγοντας, εκτός από την τάση λειτουργίας, που επηρεάζει το αποτέλεσμα, ωστόσο στο παρόν πείραμα δεν εξετάστηκε. Για την οικονομία του πειράματος όλες οι μετρήσεις λήφθηκαν σε κλιματιζόμενο χώρο με θερμοκρασία 24°C.

Οι πίνακες των συλλεγόμενων τιμών παρατίθενται στο Παράρτημα Α.

- Αξιολόγηση των δεδομένων.

Τα δεδομένα κατόπιν αξιολογήθηκαν με γνώμονα τα ποιοτικά χαρακτηριστικά τους, όπως περιγράφηκαν προηγουμένως, για την επιλογή του κατάλληλου chip μνήμης ως PUF γεννήτρια.

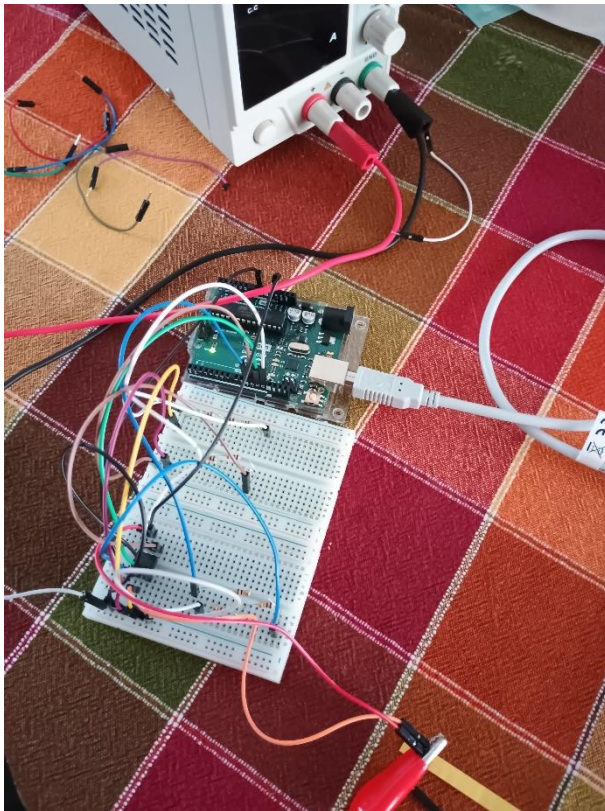
- Εφαρμογή τεχνικής βελτίωσης του PUF.

Παρατηρήθηκε ότι οι διαφοροποιήσεις μεταξύ των μετρήσεων, οφείλονταν κατά κύριο λόγο σε ασταθή κελιά μνήμηςː κελιά τα οποία κατά το αρχικό στάδιο τροφοδοσίας τους (start-up) λαμβάνουν διαφορετικές τιμές κάθε φορά, λόγω κατασκευαστικών απρόβλεπτων καταστάσεων. Δεδομένου ότι οι μετρήσεις συλλέχθηκαν από τα πρώτα 128 κελιά μνήμης, επιχειρείται η απομόνωση αυτών των ασταθών κελιών και η επιλογή καταλληλότερων από ευρύτερη περιοχή της μνήμης.

Γενικός τρόπος λειτουργίας

Πρωταρχικό στάδιο της εκτέλεσης του πειράματος αυτού είναι να συλλεχθούν τα δεδομένα αμέσως μετά την τροφοδοσία (start-up) της μνήμης SRAM. Η μνήμη

πρέπει να τροφοδοτείται ανεξάρτητα από την πλακέτα μικροελεγκτή, έτσι ώστε κατά τη διαδικασία απενεργοποίησης (power off) να αποφορτίζεται εντελώς και να μη διατηρείται φορτίο στο κύκλωμα. Η διαδικασία αποφόρτισης επαναφέρει τη μνήμη στην αρχική της κατάσταση ηρεμίας, χωρίς να διατηρεί τα δεδομένα στη μνήμη της, επιτρέποντας με τον τρόπο αυτό την ομαλή εξέλιξη του πειράματος.



Εικόνα 7: Συνδεσμολογία πειράματος

⁸Για τη συλλογή των δεδομένων η μνήμη συνδέεται με την πλακέτα μικροελεγκτή και επικοινωνεί με το πρωτόκολλο SPI (Serial Peripheral Interface). Το SPI είναι ένα πρωτόκολλο σειριακής επικοινωνίας πλήρους αμφίδρομης λειτουργίας (full-duplex), που χρησιμοποιείται ευρέως για την ταχεία μετάδοση δεδομένων μεταξύ ενός μικροελεγκτή (master) και περιφερειακών συσκευών (slaves). Λειτουργεί με τέσσερις βασικές γραμμές: MOSI (Master Out Slave In), MISO (Master In Slave Out), SCK (Serial Clock) και SS/CS (Slave Select/Chip Select). Το SPI προσφέρει απλότητα, υψηλές ταχύτητες επικοινωνίας και σταθερό χρονισμό, καθιστώντας το ιδανικό για σύνδεση με συσκευές όπως

αισθητήρες, οθόνες ή μνήμες τύπου SRAM.

Μετά από κάθε νέα ενεργοποίηση της τροφοδοσίας, επανεκκινείται ο κώδικας συλλογής της μέτρησης μέσω του reset button της πλακέτας. Η μέτρηση καταγράφεται στην οθόνη του H/Y και αποθηκεύεται ως νέα εγγραφή σε αρχείο κειμένου.

Το στάδιο αυτό αποδείχθηκε το περισσότερο χρονοβόρο, καθώς απαιτήθηκε να αντιμετωπιστούν αρκετές δυσκολίες και εμπόδια, ώστε να δύναται με σχετική ασφάλεια να χαρακτηριστούν οι μετρήσεις ακριβείς. Η τάση λειτουργίας στις επαφές SPI της επικοινωνίας μνήμης και πλακέτας μικροελεγκτή, σύμφωνα με τις

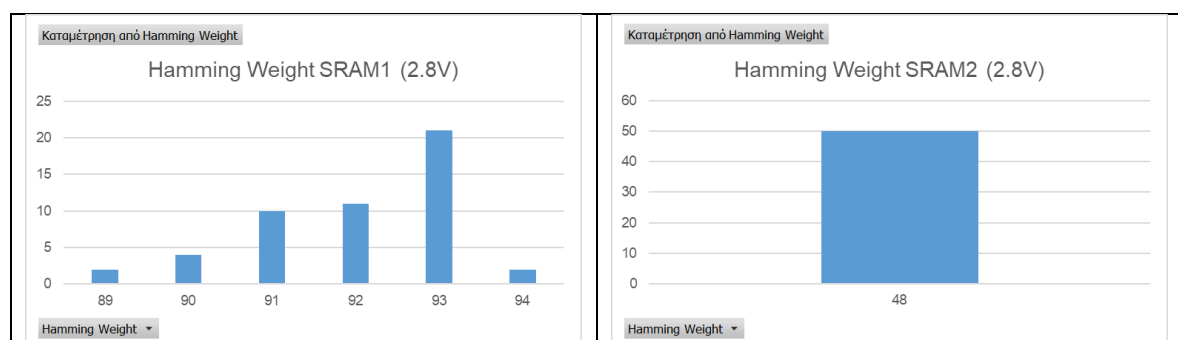
προδιαγραφές του κατασκευαστή της πλακέτας ανέρχεται στα 5V, εκτός περιοχής λειτουργίας της μνήμης. Για τον λόγο αυτό χρησιμοποιήθηκαν διαιρέτες τάσης στις συγκεκριμένες επαφές. Εκτός αυτού, οι μείωση του μήκους των χρησιμοποιούμενων καλωδιώσεων, ήταν ένας επιπλέον παράγοντας βελτίωσης των μετρήσεων.

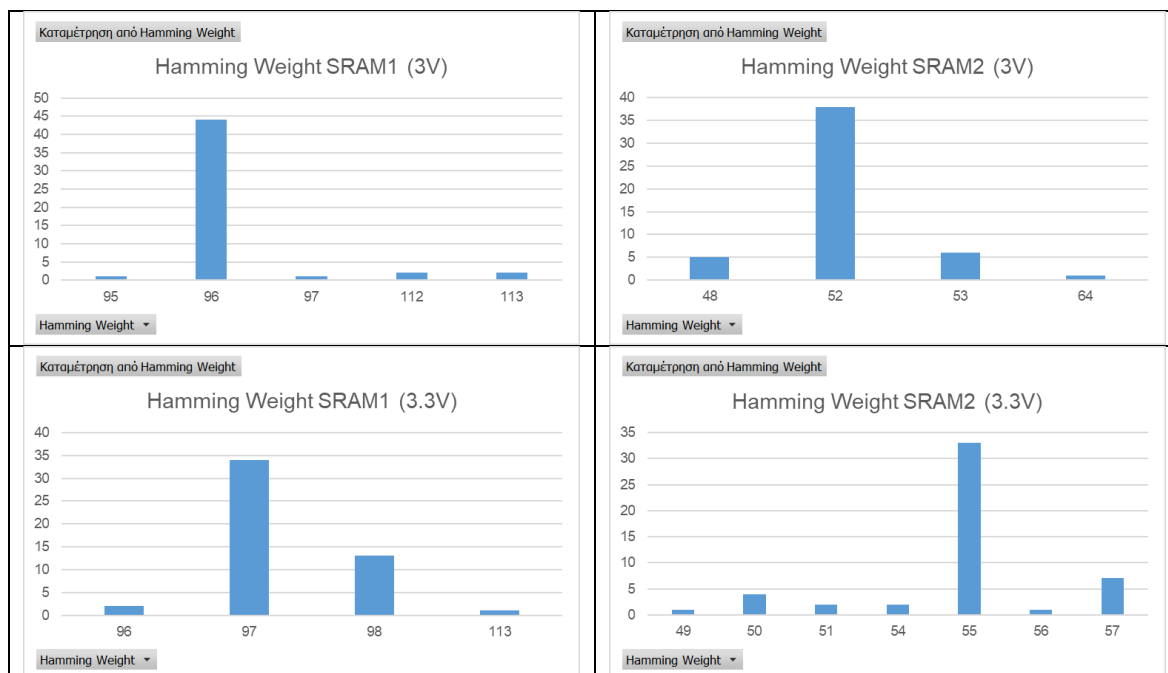
Επιπλέον, η χρήση μικρότερων καλωδίων SPI μείωσε δραστικά τη χωρητικότητα και βελτίωσε την ποιότητα των σημάτων, καθώς το SPI, συμπεριφέρεται σαν υψηλής ταχύτητας ψηφιακή γραμμή· οι μεγάλες χωρητικότητες από μακριά καλώδια οδηγούν σε αργό χρόνο ανόδου (rise time), καθυστερήσεις και πιθανές ανακλάσεις. [M. Hendry, “A Systems-Level Approach to SPI Communication,” Texas Instruments, Application Report SLYT441, Mar. 2012]

Αξιολόγηση των δεδομένων

Όπως προαναφέρθηκε, κάθε καταγραφή περιέχει τα πρώτα 16 bytes (128 bits στο σύνολο) της κάθε μνήμης. Οι μετρήσεις ελήφθησαν με όσο το δυνατόν πιο σύντομη καθυστέρηση μετά την τροφοδοσία, ώστε να αποτυπώνεται η φυσική αρχική κατάσταση των bits (power-up state).

Ένα βασικό μέγεθος στην αξιολόγηση των μετρήσεων είναι το βάρος Hamming της κάθε εγγραφής ενός PUF, καθώς εκφράζει τον αριθμό των bit που έχουν τιμή ‘1’ μέσα σε μια ακολουθία δυαδικών δεδομένων. Για κάθε μέτρηση των 128 bits, υπολογίστηκε ο συνολικός αριθμός των ‘1’, ώστε να ελεγχθεί αν η κατανομή είναι στατιστικά ισορροπημένη, δηλαδή κοντά στον ιδανικό αριθμό **64** (το 50% του συνόλου). Η ισορροπία αυτή αποτελεί ένδειξη υψηλής εντροπίας και απουσίας προκατειλημμένων καταστάσεων, γεγονός απαραίτητο για την ποιότητα της PUF. Σε κάθε επανάληψη του πειράματος, οι τιμές Hamming Weight καταγράφηκαν και αναλύθηκαν ως προς την κατανομή τους, τη σταθερότητά τους και την απόκλισή τους από την αναμενόμενη τιμή, με σκοπό να εντοπιστούν ενδείξεις αξιοπιστίας ή κατευθυνόμενης συμπεριφοράς των bits.

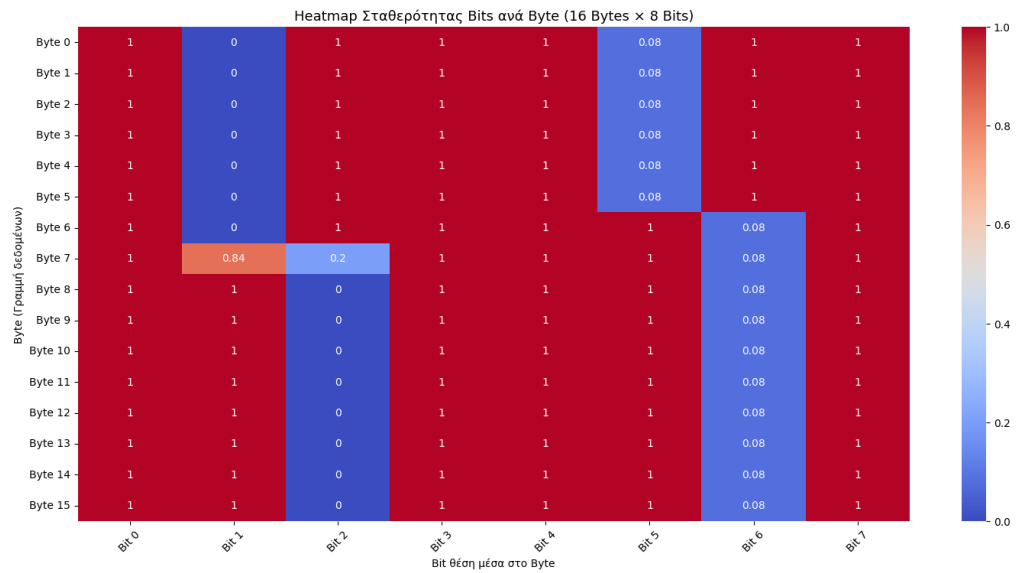
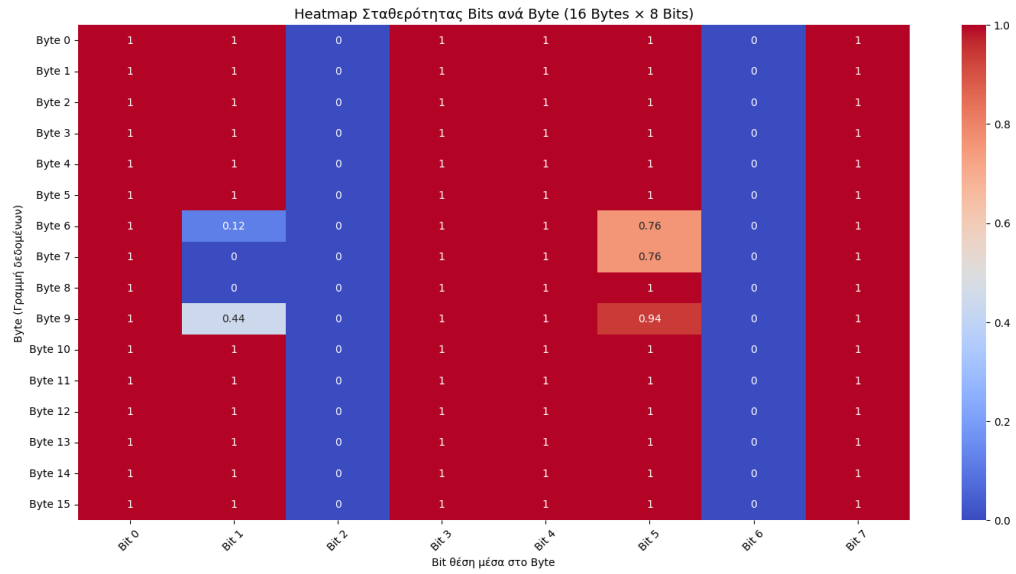


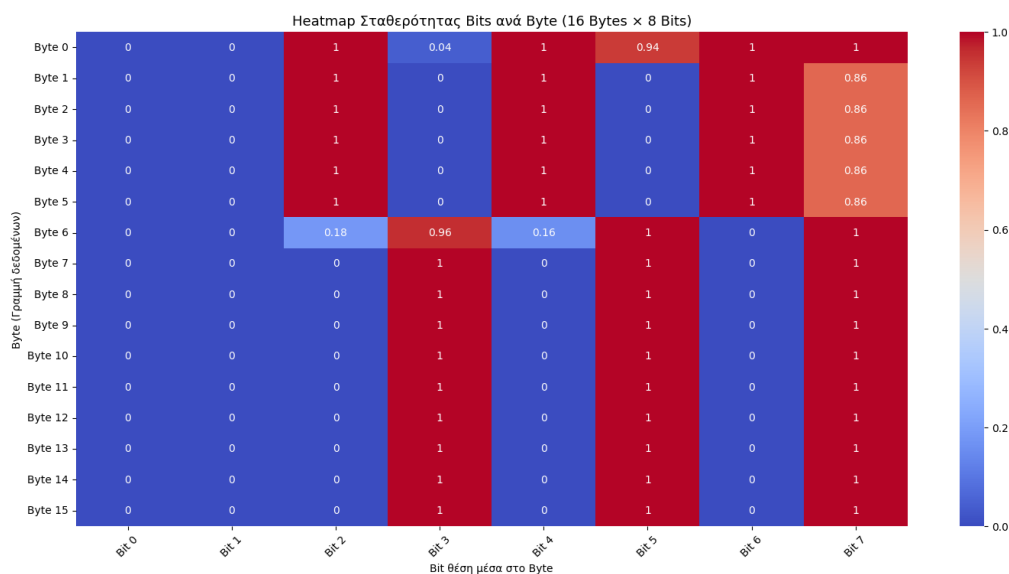
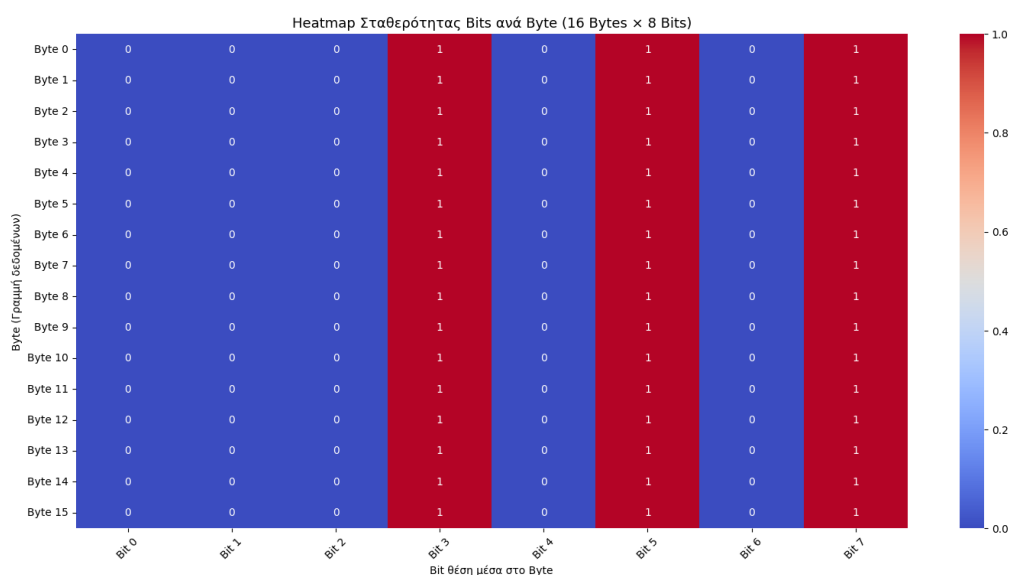
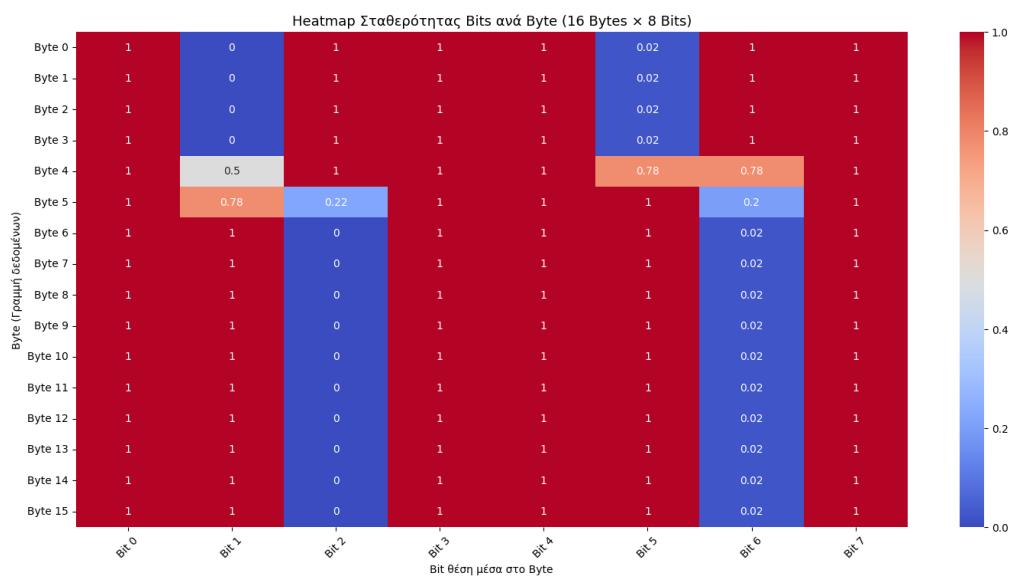


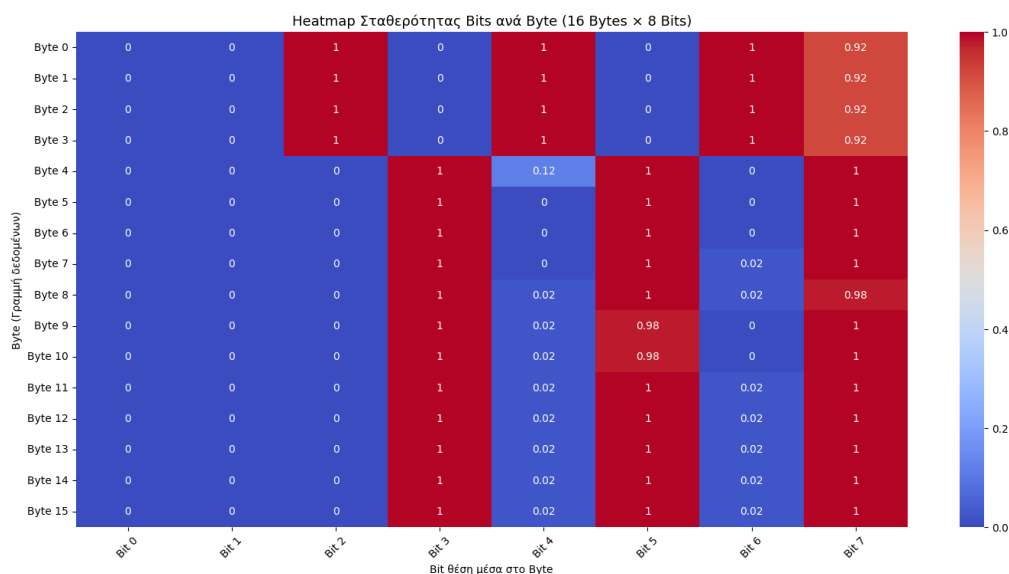
Πίνακας 1: Μετρήσεις Απόστασης Hamming

Μετρικές	SRAM1			SRAM2		
	2.8V	3V	3.3V	2.8V	3V	3.3V
Unstable Bits	5/128	18/128	20/128	0/128	10/128	23/128
Unstable Bits (%)	3.91	14.06	15.62	0	7.81	17.97
Intra-distance (bits)	1.58	3	2.8	0	2.08	1.54
Intra-distance (%)	1.23	2.35	2.19	0	1.62	1.2
Bit Entropy	0.0268	0.0609	0.0527	0	0.0394	0.0366

Πίνακας 2: Τιμές Μετρικών Αξιολογήσεων PUF







Εντροπία

Από τα στοιχεία του Πίνα 2 διαπιστώνουμε ότι η εντροπία και των 2 τσιπ πλησιάζει την τιμή 0 (ιδανικά η εντροπία θα έπρεπε να προσεγγίζει την τιμή 0.5). Αυτό από μόνο του υποδεικνύει ότι η έξοδος (το pattern) του ruf, δεν είναι εντελώς τυχαία, αλλά εμφανίζει μία επαναληψιμότητα. Για να χρησιμοποιηθούν οι εν λόγω έξοδοι ως PUF γεννήτριες κωδικών, θα πρέπει να εφαρμοστούν τεχνικές βελτίωσης.

ΕΠΙΛΟΓΟΣ

Στην παρούσα εργασία επιχειρήθηκε η συστηματική μελέτη των Μη Κλωνοποιήσιμων Φυσικών Συναρτήσεων (PUFs), παρουσιάζοντας τόσο τη θεωρητική τους βάση όσο και τις τεχνολογικές υλοποιήσεις που έχουν προταθεί στη διεθνή βιβλιογραφία. Ιδιαίτερη έμφαση δόθηκε στα SRAM PUFs, μια από τις πιο ώριμες και πρακτικά εφαρμόσιμες μορφές εγγενών PUF, λόγω της απλότητας κατασκευής τους, της υψηλής εντροπίας και της άμεσης αξιοποίησής τους σε εφαρμογές ασφάλειας.

Η υλοποίηση του πειραματικού μέρους ανέδειξε τις προκλήσεις και τα πλεονεκτήματα της χρήσης εξωτερικών SRAM ως PUF γεννήτριας. Η συλλογή των δεδομένων υπό διαφορετικές συνθήκες τάσης, καθώς και η σύγκριση δύο μνημών της ίδιας παρτίδας, αποτύπωσαν με σαφήνεια τις ιδιότητες αναπαραγωγιμότητας, μοναδικότητας και την επίδραση ασταθών κελιών στη συνολική ποιότητα του PUF. Παράλληλα, έγινε εμφανές πως οι πρακτικοί παράγοντες —όπως η καθαρότητα των σημάτων στο SPI, η ποιότητα της τροφοδοσίας, η αποφόρτιση της μνήμης και η ακρίβεια των υλικών— επηρεάζουν καθοριστικά την αξιοπιστία των μετρήσεων.

Μέσα από την εφαρμογή τεχνικών βελτίωσης, όπως η επιλογή σταθερών κελιών, φάνηκε ότι ακόμη και απλές διαδικασίες μπορούν να ενισχύσουν σημαντικά την απόδοση ενός SRAM PUF, μειώνοντας το ποσοστό ασταθειών και αυξάνοντας την προβλεψιμότητά του σε επαναλαμβανόμενες μετρήσεις. Τα ευρήματα αυτά επιβεβαιώνουν τη χρησιμότητα της τεχνολογίας των PUFs σε περιβάλλοντα χαμηλού κόστους και περιορισμένων υπολογιστικών πόρων, όπως αυτά των μικροελεγκτών.

Συνολικά, η εργασία ανέδειξε ότι τα PUFs αποτελούν μια πολλά υποσχόμενη λύση για την ασφάλεια υλικού (hardware security), προσφέροντας ιδιότητες που δεν μπορούν να επιτευχθούν με παραδοσιακές κρυπτογραφικές μεθόδους. Η φυσική μη κλωνοποιήσιμη φύση τους, η δυσκολία μοντελοποίησης και η δυνατότητα ενσωμάτωσής τους σε απλές ηλεκτρονικές διατάξεις τα καθιστούν κατάλληλα για εφαρμογές αυθεντικοποίησης, δημιουργίας κλειδιών και ανίχνευσης παρέμβασης.

Η περαιτέρω έρευνα θα μπορούσε να επεκταθεί στη μελέτη της επίδρασης της θερμοκρασίας, της γήρανσης (aging) των κυκλωμάτων, στην εφαρμογή fuzzy extractors, καθώς και στην υλοποίηση ενός ολοκληρωμένου πρωτοκόλλου αυθεντικοποίησης βασισμένου στο SRAM PUF που αναπτύχθηκε. Παρά τους περιορισμούς που τέθηκαν στο πλαίσιο της παρούσας μελέτης, τα αποτελέσματα είναι ενθαρρυντικά και καταδεικνύουν ότι η τεχνολογία των PUFs αποτελεί βασικό πυλώνα για την επόμενη γενιά συστημάτων ασφάλειας.

Chip1 (2.7V)

Chip1 (3V)

10111011,10111011,10111011,10111011,10111011,10111011,10111101,11011101,11011101,11011101,11011101,11011101,11011101,11011101,11011101,11011101,96

Απόστολος Πίτσικος, Πανεπιστήμιο Αιγαίου, Τμ. Μηχ/κών Π.Ε.Σ. 41

[illegible]

00101011,00101011,00101011,00101011,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,52

00101011,00101011,00101011,00101011,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,52

00101010,00101010,00101010,00101010,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,48

00101011,00101011,00101011,00101011,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,52

00101011,00101011,00101011,00101011,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,52

00101011,00101011,00101011,00101011,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,52

00101011,00101011,00101011,00101011,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,00010101,52

ΠΑΡΑΡΤΗΜΑ Β

Προγραμματισμός Υλοποίησης Πειράματος

Προγραμματισμός Arduino Μετρήσεων Τιμών SRAM

```
//Αρχική ρύθμιση/ Εισαγωγή βιβλιοθηκών
#include <SPI.h>
#define CS_PIN 10
#define READ_CMD 0x03

//Ρύθμιση πρωτοκόλλου σύνδεσης SPI
void setup() {
  Serial.begin(9600);
  SPI.begin();
  pinMode(CS_PIN, OUTPUT);
  digitalWrite(CS_PIN, HIGH); // CS inactive

  delay(1000); // Αναμονή σταθεροποίησης SRAM
  Serial.println("-> SPI SRAM Reader");

  readSRAM128Bits();
}

void loop() {

  // Ανάγνωση των πρώτων 128 bits (16 bytes) της μνήμης SRAM
  void readSRAM128Bits() {
    uint8_t buffer[16];
    digitalWrite(CS_PIN, LOW);
    SPI.transfer(READ_CMD);
    SPI.transfer(0x00); // Address high byte
    SPI.transfer(0x00); // Address mid byte
    SPI.transfer(0x00); // Address low byte

    for (int i = 0; i < 16; i++) {
      buffer[i] = SPI.transfer(0x00);
    }
    digitalWrite(CS_PIN, HIGH);

    // Εκτύπωση σε δυαδική μορφή με κόμμα
    Serial.print("PUF Pattern (binary): ");
    for (int i = 0; i < 16; i++) {
      printByteAsBinary(buffer[i]);
      if (i < 15) Serial.print(",");
    }
    Serial.println();
  }
}
```

```
// Υπολογισμός Hamming Weight
int hammingWeight = 0;
for (int i = 0; i < 16; i++) {
    hammingWeight += countBits(buffer[i]);
}
Serial.print("Hamming weight: ");
Serial.println(hammingWeight);
}

// Εκτυπώνει ένα byte ως 8-bit binary
void printByteAsBinary(uint8_t b) {
    for (int i = 7; i >= 0; i--) {
        Serial.print(bitRead(b, i));
    }
}

// Μετράει τα bits 1 σε ένα byte
int countBits(uint8_t b) {
    int count = 0;
    while (b) {
        count += b & 1;
        b >>= 1;
    }
    return count;
}
```

Προγραμματισμός Python υπολογισμού Μετρικών

```
# --- αρχείο: puf_intra_analysis.py ---
# Διαβάζει ένα αρχείο με PUF μετρήσεις και υπολογίζει:
# - Unstable bits
# - Intra-distance
# - Heatmap σταθερότητας

import numpy as np
import matplotlib.pyplot as plt
import seaborn as sns
import pandas as pd

# === ΟΡΙΣΕ ΤΟ ΟΝΟΜΑ ΤΟΥ ΑΡΧΕΙΟΥ ΣΟΥ ΕΔΩ ===
file_path = "file1.txt" # π.χ. "puf_records_sram1_2.7v.txt"

# === ΔΙΑΒΑΣΗ BIT PATTERNS ===
with open(file_path, "r") as f:
    raw_lines = f.readlines()

bit_arrays = []
```

```

for line in raw_lines:
    line = line.strip()
    if line:
        parts = line.split(",")[:-1] # αγνοούμε το τελευταίο πεδίο (Hamming weight)
        bitstring = "".join(parts)
        bit_array = [int(b) for b in bitstring]
        bit_arrays.append(bit_array)

bit_matrix = np.array(bit_arrays)

# === ΥΠΟΛΟΓΙΣΜΟΣ UNSTABLE BITS ===
bit_prob = bit_matrix.mean(axis=0) # πιθανότητα 1 για κάθε bit
bit_std = np.std(bit_matrix, axis=0) # διακύμανση ανά bit
unstable_mask = bit_std > 0
num_unstable_bits = np.sum(unstable_mask)
total_bits = bit_matrix.shape[1]
unstable_percent = (num_unstable_bits / total_bits) * 100

print(f"Unstable bits: {num_unstable_bits} / {total_bits} ({unstable_percent:.2f}%)")

# === ΥΠΟΛΟΓΙΣΜΟΣ INTRA-DISTANCE ===
total_distance = 0
num_pairs = 0
for i in range(len(bit_matrix)):
    for j in range(i + 1, len(bit_matrix)):
        dist = np.sum(bit_matrix[i] != bit_matrix[j])
        total_distance += dist
        num_pairs += 1

mean_intra = total_distance / num_pairs if num_pairs else 0
mean_intra_percent = (mean_intra / total_bits) * 100
print(f"Intra-distance: {mean_intra:.2f} bits ({mean_intra_percent:.2f}%)")

# === ΣΧΕΔΙΑΣΗ HEATMAP ΣΤΑΘΕΡΟΤΗΤΑΣ ===
bit_grid = bit_prob.reshape((8, 16)) # για 128 bits
plt.figure(figsize=(14, 6))
sns.heatmap(
    bit_grid,
    annot=False,
    cmap="coolwarm",
    cbar=True,
    vmin=0,
    vmax=1,
    xticklabels=[f"Bit {i}" for i in range(16)],
    yticklabels=[f"Row {i}" for i in range(8)]
)
plt.title("Heatmap Σταθερότητας Bits (0.00 = πάντα 0, 1.00 = πάντα 1)")
plt.xlabel("Θέση Bit ανά Byte")

```

```
plt.ylabel("Ομάδα Bit (16 bits ανά σειρά)")  
plt.xticks(rotation=45)  
plt.yticks(rotation=0)  
plt.tight_layout()  
plt.show()
```

[9]

ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1] R. Maes, *Physically Unclonable Functions (Constructions, Properties and Applications)*, Springer, 2013.
 - [2] F. N. H. A. K. C. L. & N. C. Farha, "SRAM-PUF-Based Entities Authentication Scheme for Resource_Constrained IoT Devices," *IEEE Internet of Things Journal*, p. 5904–5913, April 2021.
 - [3] C. H. M. & P. W. Bohm, "A microcontroller SRAM-PUF," 5th International Conference on Network and System Security, 2011.
 - [4] A. R. A. F. C. B. & P. C. Korenda, "A Proof of Concept SRAM-based Physically Unclonable Function (PUF) Key Generation Mechanism for IoT Devices," *16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, 2019.
 - [5] T. I. H. & B. M. Idriss, "A PUF-based paradigm for IoT security," *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 2016.
 - [6] K. R. M. T. F. D. H. Y. S. M. & T. M. Xiao, "Bit selection algorithm suitable for high-volume production of SRAM-PUF," *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2014.
-
- 1. T. Zhang *et al.*, "Radiation Effects on SRAM-Based PUFs," *Electronics*, vol. 9, no. 9, MDPI, 2020.
 - 2. Anonymous, "Improving Reliability of SRAM-based PUFs with Convolution Filtering," *Journal of Cryptographic Engineering*, Springer, 2020.
 - 3. X. Wang and U. Guin, "Systematic Stable Bit Selection in Noisy SRAM PUFs," *IEEE Access*, 2022. [Online]. Available:
 - 4. Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. CHES 2010*, IACR, 2010.
 - 5. Tuyls, P., Schrijen, G.-J., Škoric, B., van Geloven, J., Verhaegh, N., & Wolters, R. (2006). 'Read-proof hardware from protective coatings. In *Lecture notes in computer science (LNCS)*: Vol. 4249. Workshop on

- cryptographic hardware and embedded systems—CHES 2006 (pp. 369–383). Berlin: Springer.
6. J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, S. Devadas, *“Technique to Build a Secret Key in Integrated Circuits for Identification And Authentication Applications,”* In Proc. IEEE Symposium on VLSI Circuits, 2004.