Μη-Αντιγράψιμα Φυσικά Συστήματα για Εφαρμογές Κρυπτογραφίας σε διατάξεις στο διαδίκτυο των πραγμάτων

ΠΡΟΓΡΑΜΜΑ ΠΡΟΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΒΑΣΙΛΕΙΟΣ ΑΛΕΒΙΖΟΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ
ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

Διπλωματική εργασία για ολοκλήρωση υποχρεώσεων απόκτυσης
πτυχίου της επιστήμης των πληροφοριακών συστημάτων

ΤΜΗΜΑ ΜΠΕΣ Σάμος, Ιούνιος 2021

"What exactly an individual should or should not do partly depends on actions taken by other actors at other levels in the science governance hierarchy and, for that matter, in the military institutions of which science laboratories and the like might be a part."

— Miller, S. *Dual use science and technology, ethics and weapons of mass destruction.*

Δήλωση

Δηλώνω ότι, εκτός εάν γίνεται ειδική αναφορά στο έργο άλλων, το περιεχόμενο αυτής της διπλωματικής εργασίας είναι πρωτότυπο και δεν έχει υποβληθεί εν όλο ή εν μέρει για εξέταση για οποιοδήποτε άλλο πτυχίο ή προσόντα σε αυτό ή οποιοδήποτε άλλο πανεπιστήμιο. Αυτή η εργασία είναι δική μου δουλειά και δεν περιέχει τίποτα που να είναι το αποτέλεσμα της εργασίας που έγινε σε συνεργασία με άλλους, εκτός από ό, τι ορίζεται στο κείμενο και τις Ευχαριστίες. Αυτό το έργο περιλαβάνει λιγότερες από 65.000 λέξεις συμπεριλαμβανομένων παραρτημάτων, βιβλιογραφίας, υποσημειώσεων, πινάκων και εξισώσεων και είναι λιγότερες από 250.

ΒΑΣΙΛΕΙΟΣ ΑΛΕΒΙΖΟΣ
Σάμος, Ιούνιος 2021

Ευχαριστίες

Η διαφήμιση της ορθής λειτουργίας της επιστήμης όταν ο κόσμος μαστίζεται από τόσα πολλά προβλήματα, τα οποία προκύπτουν ακριβώς από την αποτυχία διαχείρισης της τεχνολογίας - μπορεί να ακούγεται ειρωνικό. Αυτό το φαινόμενο προκύπτει λόγω δύο προβλημάτων. Πρώτον, ο υλικός ευδαιμονισμός της σύγχρονης κοινωνίας έχει επηρεάσει, όχι μόνο τον εγωκεντρικό τρόπο σκέψης, αλλά και λανθάνουσα ατοπήματα μέσα στην κρίση. Δεύτερον, το γεγονός ότι οικονομικοί παράγοντες που υπεισέρχονται για την εξυπηρέτηση συμφερόντων. Οι συμφεροντολογικές παρεμβολές έχουν επηρεάσει την ακαδημαϊκή μας κοινότητα, και νοοτροπία προς το χειρότερο. Δεδομένου αυτών των δυσκολιών, πολλοί δεν μερολήπτησαν τις αξίες που πρέπει να έχει ένας επιστήμονας, συνεχίζοντας μέχρι σήμερα να δίνουν το σωστό παράδειγμα στην σημερινή μας κοινωνία [1]. Η χρόνια ήταν γεμάτη πολλές οικονομικές και ψυχολογικές δοκιμασίες, διότι οι περιορισμοί και απότομες αλλαγές που υπήρξαν λόγο της πανδημίας του COVID-19, επηρέασαν όλους μας αρνητικά σε κάποιο επίπεδο.

Ειλικρινές και θερμές ευχαριστίες πρέπει να πάνε στην επιβλέποντα καθηγητή, της διατριβής μου, αναπληρωτή καθηγητή Δρ. Χάρη Μεσαριτάκη, για την ασύστολη υποστήριξη του, την αφοσίωση του , και φυσικά την καθοδήγησή του, κατά την διάρκεια της εκπόνησης της διατριβής — καθώς από την αρχή υπήρχε εμπιστοσύνη και συμπαραστάτη σε κάθε βήμα της ερευνητικής μου προσπάθειας. Παράλληλα, επωφελήθηκα πάρα πολύ από τα υπόλοιπα μέλη της επιτροπής. Εκτός από αυτό, πολλές ευχαριστίες πάνε στους συμφοιτητές, συνοδοιπόρους και, συναδέλφους, για τη συνεχή του ενθάρρυνση, και ψυχολογική υποστήριξη — από την αρχή έως τον τέλος του έργου. Ακόμη, ευχαριστήσω τους συνοδοιπόρους, Πολύμερο Ε., Τσίγκρος Α., Γιαννέλος Ν., Μπεγκβάρφαϊ Μ., Κοτσίφης Ν., Γιωργοστάθη Β., την κοινότητα του Τίμιου Σταυρού, και άλλοι πολλοί, για τη συνεχόμενη και αξιότιμη υποστήριξη τους σε σημαντικά σημεία της έρευνας αυτής.

Τέλος, ευχαριστώ την φοιτητική κοινότητα του Πανεπιστήμιου Αιγαίου για τη συνεχή υποστήριξή της στη μελέτη αυτή, τις ευκαιρίες, και γνώσεις που μου προσέφερε.

Αυτή η εργασία δεν θα είχε εμπλουτιστεί και υλοποιηθεί, εάν δεν υπήρχε αυτή η ψυχολογική υποστήριξη. Ελπίζω η νέα φουρνιά υποψήφιων φοιτητών, όχι μόνο να βιώσουν αξέχαστες εμπειρίες, αλλά και να δώσουν πίσω στην κοινότητα.

Abstract

Physical identity and vertex remains an essentially controversial concept, investigated and implanted across algorithmic data chain yet under political presumptions. The ambiguity of the intellectual validation dilemma not only was consensus in the field of cryptography but reached the table of multiple disciplines. In contrast, physical unclonable functions started as an academic attempt on elusive evaluation resulting from diverse security and skeptical contexts. To this end, SRAM memories have been prevailed as the backbone for embedded devices because of the inherent benefits and subsequently commitment to innovative security solutions; thus, this adoption of characteristics among other several stratagems for ambitious requirements.

This thesis stimulus occupation about true random cryptographic tangible keys – as a large scale of research opportunities addressed through novel trial and error. Highlights tolerance of contradiction towards previous findings, as provocative questions rarely have been analyzed in that depth before. Furthermore, official examination measurements through an exegesis have been thrust into the spotlight once more cumulative features of these devices wisely manipulated. Lastly, experimental machine learning attacks, albeit with limited methodologies, took place; the final phase ends with a discussion concerning overall results, learned lessons; while closing with future endeavors which might have positive ramifications for exotic norms, such as homomorphic encryption schemes and zero-knowledge proof protocols.

Key words: *PUF, ECC, Physical Unclonable Functions, BCH, Fuzzy extractor, Secure Sketch.*

Πρόλογος

Η φυσική ταυτότητα και ταυτοποίηση, αντιπροσωπεύουν δυο εξεζητημένες και αμφιλεγόμενης έννοιες, οι οποίες έχουν κεντρίσει τον ενδιαφέρον της επιστημονικής κοινότητας μέσα από ερευνητική συνεισφορά, επηρεάζοντας έτσι όχι μόνο στον κύκλο των αλγοριθμικών δεδομένων, αλλά και την αντίληψη της φιλοσοφίας στον τομέα αυτό. Το ασαφές δίλημμα της αμοιβαίας επικύρωσης δεν είναι υπαρκτή μόνο στον τομέα της κρυπτογραφίας, ωστόσο προβληματίστηκαν όλοι οι επιστημονικοί κλάδοι. Αντίθετα, οι φυσικές μη-αντιγράψημες συναρτήσεις ξεκίνησαν ως μια ακαδημαϊκή προσπάθεια αξιολόγησης που προκύπτει από ποικίλα πλαίσια ασφάλειας και πειραματισμού. Για το σκοπό αυτό, οι μνήμες SRAM έχουν επικρατήσει ως η ραχοκοκαλιά των ενσωματωμένων συσκευών, λόγω των εγγενών πλεονεκτημάτων και στη συνέχεια της δέσμευσης για καινοτόμες λύσεις ασφάλειας – έτσι, αυτή η υιοθέτηση των έμφυτων χαρακτηριστικών μεταξύ άλλων εμπλουτισμένων έρχονται σε αντιπαράθεση επάνδρωσης κρίσιμων απαιτήσεων.

Αυτή η διατριβή επικεντρώνεται με τα πραγματικά τυχαία κρυπτογραφικά στοιχεία της εξεταζόμενης τεχνολογίας, η οποία αποτελεί μεγάλη γκάμα ερευνητικού ενδιαφέροντος, και οι προβληματισμοί αντιμετωπίζονται μέσω ανατροφοδοτημένων πειραμάτων. Επισημαίνεται η ανοχή των αποτελεσμάτων σε σχέση με προηγούμενα ευρήματα, καθώς διαδραματίζονται διάφορα ακόρεστα ερωτήματα. Επιπλέον, λαμβάνουν χώρα επίσημες μετρήσεις εξέτασης μη αντιγράψημων πηγών για ένα σύνολο διαφορετικών συσκευών και κυκλωμάτων. Τέλος, πραγματοποιήθηκαν πειραματικές επιθέσεις μηχανικής μάθησης, αν και με περιορισμένες μεθοδολογίες, κλείνοντας έτσι σχολιάζοντας τα συνολικά αποτελέσματα, και προσκομίζοντας μελλοντικά πλάνα σε εξωτικά πρότυπα, όπως είναι για παράδειγμα σχήματα ομομορφικής κρυπτογράφησης και πρωτόκολλα μηδενικής γνώσης, για τα οποία πρόσφατα έχει γίνει αδυσώπητος αγώνας προσαρμογής τους.

Λέξεις Κλειδιά: *PUF, ECC, Physical Unclonable Functions, BCH, Fuzzy extractor, Secure Sketch.*

Πίνακας περιεχομένων

Λίστα εικόνων

Λίστα πινάκων

Ακρωνύμια

Roman Symbols

F complex function

Greek Symbols

π $\simeq 3.14\ldots$

Acronyms / Abbreviations

AES Advanced Encryption Standard

ASIC Application Specific Integrated Circuit

BCH Bose, Ray-Chaudhuri, Hocquenghem

BER Bit-Error Rate

CDF cumulative distribution function

CMOS Complementary Metal-Oxide-Semiconductor

CRP Challenge-Response Pair/s

EEPROM Electrically Erasable Programmable Read-Only Memory

FPGA Field-Programmable Gate Array

HDA helper data algorithm

HMAC keyed-hash message authentication code

IoT Internet of Things

KDF key derivation function

NIST National Institute of Standards and Technology

NVM Non-Volatile Memory

PDF probability density function

PMF probability mass function

PRNG Psuedo Random Number Generator

PUF Physically Unclonable Function

RSA Rivest–Shamir–Adleman

SHA Secure Hash Algorithm

SRAM Static Random Access Memory

TMV Temporal Majority Voting

TRNG True Random Number Generator

XOR Exclusive-or

Κεφάλαιο 1

Γενική εισαγωγή

"*The political principle that underlies the political mechanism is conformity. The individual must serve a more general social interest–whether that be determined by a church or a dictator or a majority*"

Friedman, Milton. *The social responsibility of business is to increase its profits.*

Στο πρώτο κεφάλαια της αναφοράς γίνεται μια σύντομη εισαγωγή στον σκοπό της έρευνας, γίνεται αναφορά σε όλους τους προβληματισμούς της βιβλιογραφίας, και κλείνει με την προοικονομία της αναμενόμενης ροής.

1.1 Πρόλογος

Την τελευταία δεκαετία οι ηλεκτρονικοί υπολογιστές όλο ένα και αυξάνεται η χρήση τους στην καθημερινότητά μας για την επίλυση διαφόρων προβλημάτων. Στα IoT εξειδικεύεται η λειτουργικότητά τους βασίζεται πάνω σε διάφορες συσκευές, στις οποίες δεν περιορίζεται η χρήση τους σε ένα μόνο προσωπικό χρήστη, αλλά από εξωτερικούς επισκέπτες. Το παρόν κεφάλαιο είναι δομημένο με την εξής σειρά. Πρώτα από όλα, σειρά έχει το κίνητρο αυτής της εργασίας ακολουθούμενο από την οργάνωση υλοποίησης της

αναφοράς, και εν συνεχεία η δομή της αναφοράς και ιστορική αναδρομή 1.2, έπειτα προσδιορίζεται η επιθυμία και επιδιώξεις του συγκραφέα 1.3, και κλείνει το κεφάλαιο με την σφαιρική εικόνα του εκπληρωμένου έργου 1.4.

1.2 Αρχές σχεδιασμού και προκλήσεις των ενσωματωμένων συσκευών

Ένα πρόβλημα που αντιμετωπίζει ο κλάδος της κρυπτογραφίας τα τελευταία χρόνια, είναι η αποδοτικότητα των αλγορίθμων σε μικροεπεξεργαστές και ενσωματωμένα συστήματα με περιορισμένες υπολογιστικές δυνατότητες ή ισχύ μπαταρίας. Το απαιτητικό κόστος πόρων οδήγησε σε συμβατές λύσεις, δηλαδή επεκτασιμότητας οργάνωσης των προσκομίζων προκλήσεων. Με επιρροή την σταθερότητα της αυθεντικοποίησης, τα βιομετρικά στοιχεία προτάθηκαν ως αποτελεσματικότερη αντιμετώπιση του προβλήματος. Ωστόσο, στον παραπάνω τρόπο παρατηρήθηκαν αρκετά προβλήματα συμβατότητας και τρωτότητες ασφάλειας [8], έτσι πολλές νέες εφεδρικές τεχνολογίες διερευνήθηκαν εκτενώς για την επίλυση των παραπάνω προβλημάτων.

Ανάλογα με τις προδιαγραφές αρχιτεκτονικής μιας εφαρμογής, τεχνικές και διαδικασίες διατήρησης σύμβασης προστασίας πνευματικής ιδιοκτησίας, έχουν πολύπλοκες πτυχές, όπως είναι για παράδειγμα υπηρεσίες νέφους, διαφορετικά πρωτόκολλα blockchain, και για πολλές αναδυόμενες εφαρμογές χρειάζεται εξαιρετική προσοχή στον εντοπισμό και τον έλεγχο ταυτότητας χρηστών. Σε όλα τα δυνητικά ευάλωτα στοιχεία ενσωματωμένων συσκευών, η αξία της δυσπροσδιόριστης εκτεθειμένης πληροφορίας ή δεδομένων στον κυβερνοχώρο, δεν είναι μονάχα ανεκτίμητη, αλλά λαμβάνεται υπόψη η κατάταξη, ανάλογα των θεμελιωδών στοιχείων του δικτύου στο οποίο βρίσκεται - επεξηγώντας τούτη την δήλωση, μοναδικά αναγνωριστικά χαρακτηρίζονται, η αναγνώριση συσκευής, αναγνωριστικό κατακερματισμού-ταυτότητας, και η δημιουργία κλειδιών. Γι' αυτό τον λόγο, οι μη-κλωνοποίησημα συστήματα αντικατέστησαν την μεθοδολογία των βιομετρικών στοιχείων, διότι μια μη-αντιγράψιμη πηγή όχι μόνο παράγουν έναν μοναδικό τρόπο αναγνώρισης του ολοκληρωμένου κυκλώματος, αλλά και εγγυάται αρτιότερή και εγγυημένη ασφάλεια λόγο της αυξημένης εντροπίας.

1.2.1 Μη κλωνοποιήσιμα συστήματα

Ένα μη-κλωνοποιήσημο σύστημα μπορεί να θεωρηθεί μια συνάρτηση κατακερματισμού στην οποία μια δεδομένη είσοδος θα οδηγήσει σε μια συγκεκριμένη έξοδο. Για λόγους σαφήνειας και συνεκτικότητας, ως βασική συνιστώσα παραλαβής έχει εκπονηθεί από μια πηγή, ονομάζεται πρόκληση(ή ζεύγος πρόκλησης-απόκρισης – Challenge-response pair), και η έξοδος αντίστοιχα, απάντηση. Αυτή η αλληλεπίδραση μεταξύ αυτών των δύο στοιχείων, μαζί με άλλους παράγοντες που επηρεάζουν την αποδοτικότητα, μπορούν να απεικονισθούν ως μη κλωνοποιήσεις επειδή σχεδιάζονται με τέτοιο τρόπο ώστε να είναι αδύνατη η απομίμηση και αντιγραφή τους. Ειδικότερα, το φαινόμενο αυτό οφείλεται σε μικρές παραλλαγές εγγενών χαρακτηριστικών που αναπτύσσονται κατά τη διάρκεια της κατασκευής – αυτές οι φυσικές παραλλαγές μπορεί να περιλαμβάνουν ιδιότητες όπως οι χρόνοι καθυστέρησης διάδοσης σήματος που υπάρχουν στα καλώδια και στις λογικές πύλες. Ωστόσο, αυτό εξασφαλίζει μόνο την παρουσία της ασφαλούς οντότητας, και δεν αντιπροσωπεύει την ακεραιότητα άλλων στοιχείων. Ακόμη, οι φυσικές συναρτήσεις χαρακτηρίζονται και ως πιθανολογική διαδικασία, επειδή σε μια μόνο έξοδο μπορούν να παραχθούν διαφορετικές τιμές λόγω του ανεξέλεγκτου τυχαίου θορύβου. Τέλος, όπως θα δούμε και σε σχετική ενότητα, η ποιότητα ενός μη-αντιγράψιμου συστήματος μπορεί να οριστεί χρησιμοποιώντας σχετικές μετρήσεις.

1.2.2 Ιστορική αναδρομή και μετάγενέστερο εξέλεγξη

Υπάρχουν πολλοί διαφορετικοί τρόποι να αναφερθούμε σε συστήματα ακεραιότητάς τα οποία δεν βασιζόντουσαν σε αριθμητικές υποθέσεις, από την αρχαιότητα, παρόλα ’αυτά η πρώτη καταγεγραμμένη προσπάθεια ή οποία είχε χορηγηθεί και υλοποιηθεί σε ερευνητικό έργο ήταν το 1983, και πιο συγκεκριμένα στην εφεύρεση τεχνολογίας υλικών για την παραγωγή χρημάτων της εποχής στην Αμερική [9]. Μέσα στην επόμενη δεκαετία, πολλοί ερευνητές πραγματεύτηκαν διάφορους τρόπους αυθεντικοποίησης, οι οποίοι θα παρέπεμπαν σε απομιμήσεις νομισμάτων, και για πρώτη φορά έγιναν πειράματα σε φωτόνια μέσα [10]. Ο ορισμός της μη-κλωνοποιήσημης πηγής οριστικοποιήθηκε από την διπλωματική του Pappu et all [11, 12], και η μέθοδος τεκμηριώθηκε ως φυσικές μονόδρομες λειτουργίες(physical one-way functions). Η εμπορευματοποίηση αυτής της καινοτόμα τεχνολογίας των μη-κλωνοποιήσημων γεννητριών, ξεκίνησε από ένα έργο στο MIT[1] το 2005 και μετατράπηκε σε start-up επιχείρησης με όνομα Verayo, και στην συνέχεια άλλες πολλές, στις οποίες τα προϊόντα έχουν δοκιμαστεί σε διάφορα

[1] https://deshpande.mit.edu/portfolio/project/verayo-inc

πειράματα [13] – ωστόσο οι επιχειρήσεις δραστηριοποιούνται σήμερα και επενδύουν σε μη-αντιγράψιμα συστήματα είναι STMicroelectronics[2], Rambus[3], και άλλες.

1.3 Σκοπός της υλοποίησης

Το βασικό κίνητρο πίσω από την υλοποίησή της έρευνας, είναι η παρούσα ανάγκη ολοκληρωμένου συστήματος αυθεντικοποίησης υλοποιημένο σε ολοκληρωμένα κυκλώματα (IC), με προεπιλεγμένο σχεδιασμό ο οποίος να ικανοποιεί κάποια κριτήρια ασφαλείας τα οποία έχουν οριστεί από δημόσιους οργανισμούς και μελέτες [14] (Κεφ. 4.1). Μέχρι σήμερα, έχουν αναπτυχθεί και μελετηθεί διάφορα φυσικά μέσα και αλγόριθμοι βελτιστοποίησης της ποιότητας και ασφάλειας, πραγματοποίησης μη-αντιγράψιμων πηγών. Παρ' όλα, σε τούτη την εργασία θα επικεντρωθούμε σε πειράματα μη κλωνοποίησιμων πηγών με μνήμες SRAM που έχουν κατακτήσει τον χώρο των ενσωματωμένων συσκευών λόγω της συμβατότητας με τη λογική διαδικασία και της χαμηλής καθυστέρησης, και τις τελευτές δεκαετίες έχουν πραγματοποιηθεί πολλοί πειραματισμοί σε μια μεγάλη ποικιλία φυσικών μέσων [15–21], εντούτοις λίγοι είναι οι συγγραφείς οι οποίοι κάνουν αντικειμενική σύγκριση των ευρημάτων τους ή να τονίσουν την ανάγκη για εφεύρεση άλλων πρωτοκόλλων, σε σχέση με άλλα επιστημονικά έργα – με κάποιες εξαιρέσεις. Ως εκ τούτου, ένα μεγάλο πρόβλημα που προκύπτει είναι το καμουφλάρισμα των πιθανών προβλημάτων της εργασίας, καθώς και λάθη και τον τρόπο αντιμετώπισής τους. Οπότε, κάποια ερωτήματα που θα μας απασχολήσουν είναι, Με άλλα λόγια, . Τέλος, πρέπει να σημειώσουμε πως, δεν υπάρχει κάποιο μοντέλο ανάλυσης τρωτοτήτων και σκλήρυνσης συστήματος, το οποίο να θωρακίζει, [22] – τα μη-κλωνοποίησημα συστήματα δεν είναι πανάκεια [23]. Ωστόσο, λείπει σε μεγάλο βαθμό η έρευνα για την κατηγοριοποίηση των σχημάτων διόρθωσης σφαλμάτων, σε σχέση με προηγούμενες έρευνες σε αντιπαράθεση με κανόνες. Έχοντας αυτούς τους προβληματισμούς από την μια, ερευνητικά έργα στον ίδιο εξοπλισμό δεν αναφέρθηκαν κάποιες μετρήσεις σε πειραματικό επίπεδο ή μόνο προσομοιώθηκαν. Άρα, αξιοποιώντας την βιβλιογραφία, πειραματιστήκαμε σε εγγενείς παραλλαγές της συσκευής, καθώς και εξάγαγε αποτελέσματα, τα οποία τα συγκρίναμε με θεωρητικούς ισχυρισμούς ασφαλείας [24].

[2] www.st.com
[3] www.rambus.com

1.3.1 Αναγκαιότητα ανάλυσης

Ο αυξανόμενος αριθμών των νέων τεχνολογιών τα τελευταία χρόνια, όχι μόνο έχει σαν αποτέλεσμα την δημιουργία νέων πρωτοκόλλων, αλλά πλέον όλες οι κατηγορίες κυκλωμάτων και συσκευών είναι διασυνδεδεμένες σε κάποιο δίκτυο, είτε δημόσιο ή ιδιωτικό, με αποτέλεσμα την βέλτιστή αξιοποίηση της τεχνολογίας αυτής. Δίνοντας έμφαση στην εξασφάλιση της ασφάλειας κάθε ενσωματωμένου μηχανήματος(έξυπνης συσκευής), μεγάλες προκλήσεις έχουν εμφανιστεί για'το λόγο ότι η γνώση των χαρακτηριστικών σε επίπεδο φυσικό(hardware) ή δικτύου, είναι ευρέων διαθέσιμη. Μάλιστα, ο πηγαίος κώδικας ή και τα ίδια εγχειρίδια των συσκευών είναι διαθέσιμα είτε από τον ίδιο κατασκευαστή είτε από κακόβουλους ή πολιτικά διχασμένους χρήστες [25]. Πρόσφατες μελέτες και αναλύσεις πάνω σε έξυπνες συσκευές που χρησιμοποιούνται σε διεργασίες, στις οποίες η ασφαλή ακεραιότητά και αυθεντικοποίηση είναι κρίσιμες με υψηλή προτεραιότητα [26, 6, 27], όπως τραπεζικές συναλλαγές, χρήση στρατιωτικού ή ιατρικού εξοπλισμού, τονίζουν την αναγκαιότητα της διερεύνησης ισχυρών συστημάτων ταυτοποίησης και ελέγχου ακεραιότητας. Περιττό να πούμε ότι οι τελευταίοι καινοτόμοι σχεδιασμοί κβαντικών υπολογιστών, με χαμηλή εντροπία και θόρυβο, μπορούν με κρυπτανάλυση να αναστρέψουν κρυπτο-αλγορίθμους [28, 29]. Έτσι, οι έξυπνες συσκευές με χαμηλές υπολογιστικές δυνατότητες και σε συνδυασμό με το ίδιο το κύκλωμα, μπορεί να εκμεταλλευτεί κάποια κατάσταση ή ιδιαιτερότητα της συσκευής, η οποία από την αρχική κατασκευή μπορεί να προσφέρει πραγματική τυχαιότητα (υψηλή εντροπία), και ταυτόχρονα μια μεγάλη ποικιλία εφαρμογών, σχετικές με την ασφάλεια και ιδιωτικότητα της συσκευής. Από την άλλη πλευρά, αρκετά προβλήματα ιδιωτικότητας προκύπτουν, καθώς η πλήρη εχεμύθεια είναι αναγκαία για την διασφάλιση της πιστοποίησης του εκδότη [30, 31]. Επιπρόσθετος, τρωτότητες στο φυσικό επίπεδο, ραγδαία έχουν επεκταθεί στο σημείο που οι εμπιστευτικές πληροφορίες μπορούνε να κλαπούν – αμφισβητόντας έτσι τα κλασικά σχήματα κρυπτογραφίας [32]. Αναμφίβολα μπορούμε να πούμε ότι η λύση στο πρόβλημα αυτό αναδύεται – ωστόσο η ομομορφική κρυπτογράφηση δεν είναι πρακτική σε όλα τα παρόντα μοντέλα αντιμετώπισης απειλών [33].

Πρόσφατες μελέτες αποδεικνύουν ότι ακόμη και μαθηματικά ασφαλείς αλγόριθμοι μπορούν να παραβιαστούν με την εκμετάλλευση ευπαθειών ευάλωτης υλοποίησης λογισμικού. Επιπλέον, οι λύσεις που άπτονται σε λογισμικό δεν αρκούν για να αποτρέψουν την αναπαραγωγή νέων ευμάθειών ή την ανακύκλωση προηγουμένων. Η ασφάλεια υλικού σχετίζεται με κάθε τεχνική αποτροπής και ελέγχου ακεραιότητας μεταξύ των χρηστών. Η επιτυχία των μη-κλωνοποίησιμων συστημάτων έγκειται στο

συστηματικό σχεδιασμό των συστατικών του συστήματος, για τον οποίο επιτρέπεται η συγκεκριμένη και αυστηρή αξιολόγηση των ιδιοτήτων ασφαλείας, όπως είναι η φυσική αδυναμία αντιγραφής και αξιοπιστία.

1.3.2 Κατανομή κρυπτογραγικών τεχνολογιών στο διαδίκτυο των πραγμάτων

Η μεγάλη κλίμακα αυτόνομων εφαρμογών σε όλους τους επαγγελματικούς τομείς, όπως είναι η βιομηχανία υγείας, εκμεταλλεύεται μεγάλος όγκος κατανεμημένων δεδομένων όπου περιέχονται ιδιωτικές πληροφορίες, για τις οποίες ενδέχεται να οδηγήσουν σε ανωμαλίες των δραστηριοτήτων. Αυτοί οι αυξανόμενοι κίνδυνοι, έρχονται σε αντιπαράθεση με τις προδιαγραφές της αρχιτεκτονικής του συστήματος, οι οποίες κατηγοριοποιούν την κάθε αλυσοδεμένη ομοσπονδιακή οντότητα στις ακόλουθες κύριες πτυχές, με βάση το ISO 27001, δηλαδή έλεγχος ταυτότητας, προστασία εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας, και επικύρωση μη αποποίησης. Η επικοινωνία μπορεί να θεωρηθεί ασφαλές, εάν τα δεδομένα δεν αποκρυπτογραφούνται ποτέ πριν από τον τελικό αποδέκτη. Λαμβάνοντας υπόψη την περιορισμένη υπολογιστική δύναμη των μικροεπεξεργαστών, ο επιστημονικός κλάδος της κρυπτογραφίας αφοσιώθηκε στην δημιουργία κρυπτογραφικών εργαλείων, από συναρτήσεις κατακερματισμού, ψηφιακών υπογραφών, υλοποίηση κρυπτογράφησης δημοσίου κλειδιού, πρωτόκολλα απόδειξης μηδενικής-γνώσης, και γεννήτριες τυχαίων αριθμών, όπως είναι ο αλγόριθμος κατακερματισμού Spongent. Ωστόσο, η ταχύτητα μετάδοσης είναι περιορισμένη, και μειώνετε περαιτέρω λόγω της εκθετικής αύξησης των νέων συνδεδεμένων συσκευών, για τις οποίες πρέπει να υποστεί προ-επεξεργασία σε πραγματικό χρόνο. Ακόμη, οι παραδοσιακοί αλγόριθμοι είναι ελλείπεις κρίσιμων χαρακτηριστικών, όπως είναι η δυνατότητα αναγέννησης ή ιδιωτικότητα κλειδιών. Εν κατακλείδι, είναι δύσκολο για το κλειδί να μεταφερθεί και να αποθηκευτεί στο δίκτυο, και οι παρούσες λύσεις δεν είναι κατάλληλες για προκαθορισμένο προϋπολογισμό πόρων – ως εκ τούτου, είναι ζωτικής σημασίας να βρεθεί ένας εναλλακτικός τρόπος για τη βελτίωση της ασφάλειας αυτών των προβληματικών συσκευών.

1.4 Επιστημονική συνεισφορά

Ο στόχος αυτού του ερευνητικού έργου είναι η ανάπτυξη μιας οικονομικά αποδοτικής, αρχιτεκτονική ασφάλειας περιορισμένου υλικού, ειδικά σχεδιασμένης για τον τομέα

του διαδικτύου των πραγμάτων – κυβερνώμενος προσδιορισμός αξιοποιώντας τα εγγενή χαρακτηριστικών. Ειδικότερα, παρακάτω αναφέρονται οι κύριοι λόγοι και περιέργεια υλοποίησής του έργου.

1.4.1 Ερευνητικά ερωτήματα

Σε αυτή τη διατριβή τα κύρια αντικείμενα μελέτης είναι οι τρόποι δημιουργία μυστικών κλειδιών με συσκευές SRAM, αντιμετώπιση των προκλήσεων κάθε μέτρησης της προδιαγραφής των πιο δημοφιλών τρόπων από την βιβλιογραφία, απαντώντας σε τέσσερα ερευνητικά ερωτήματα.

1.4.1.1 Ερώτημα πρώτο

Το κεντρικό ερώτημα της παρούσας διατριβής είναι η εκτίμηση εντροπίας μη κλωνοποιήσιμων πηγών μνημών τύπου SRAM, συγκρίνοντας το θεωρητικό υπόβαθρο της βιβλιογραφίας σε σύγκριση του αποτελέσματος αυτού με το ίδιο τσιπ. Το πρακτικό κομμάτι σε συνδυασμό με τους κανόνες επίσημων πρωτοκόλλων, σκοπεύει στην αποκάλυψη των εγγενών χαρακτηριστικών μοναδικότητας και τυχαιότητας.

1.4.1.2 Ερώτημα δεύτερο

Η παραδοσιακή επιστημονική προσέγγιση των κριτηρίων αξιολόγησης ενός κυκλώματος μη αντιγράψιμης πηγής, αρχικά θεωρείται ότι με την παρατήρηση προκατασκευασμένων τμημάτων μίας μνήμης SRAM ενδέχεται να κατασκευαστεί μια υπόθεση, η οποία στη συνέχεια ελέγχεται μέσω συλλογής δεδομένων και πειραματισμού, όπου τελικά βελτιώνεται σε θεωρητική εξήγηση ανεξάρτητα της τελικής κατάληξης, αποδεικνύοντας έτσι τις επιδόσεις σε πραγματικά σενάρια υλοποίησης.

1.4.1.3 Ερώτημα τρίτο

Ο κυριότερος παράγοντας υποβάθμισης της ποιότητας των μη αντιγράψιμων πηγών, θόρυβος, έχει βρεθεί στο επίκεντρο πολλών ερευνών τις τελευταίες δεκαετίες. Από την άποψη της ασφάλειας, κρίνεται σκόπιμο η επιθεώρηση σταθερών μπιτ του κυκλώματος σε διαχρονική δειγματοληψία. Έχουν αναπτυχθεί κώδικες διόρθωσης σφαλμάτων, αλλά ένα από τα πιο δημοφιλή είναι οι κώδικες BCH, για τους οποίους έχει πραγματοποιηθεί εκτεταμένες έρευνες και μεταρρυθμίσεις στο σχήμα αυτό.

1.4.1.4 Ερώτημα τέταρτο

Τα τρέχοντα ζητήματα περιλαμβάνουν σχέσεις μεταξύ της αξιοπιστίας των εγγενών χαρακτηριστικών και της βελτίωσης των αποκρίσεων. Ωστόσο, οι μη αντιγράψημες πηγές σε συσκευές SRAM χαρακτηρίζονται ως αδύναμες (weak PUF), οπότε επιθέσεις μηχανικής μάθησης μπορούν να δοκιμαστούν για ένα συγκεκριμένο εύρος ολίσθησης επαληθευμένης ρίζας (root-of-trust) – το στατιστικό κατώφλι σε αυτή την περίπτωση δεν έχει ερευνηθεί στο παρελθόν.

1.4.2 Δομή αναφοράς

Τα ακόλουθα κεφάλαια της εργασία είναι οργανωμένα ως εξής. Καταρχάς, στο κεφάλαια 2 παρουσιάζεται η βασική γνώση των επιστημονικών αντικειμένων που θα μας απασχολήσουν στην συνέχεια, ακόμη συζητιούνται οι αρχές της οργάνωσης μνήμης τύπου SRAM, μαζί με την λειτουργία τους. Πέρα από αυτό, στο κεφάλαιο 3 παρουσιάζονται τα ποιοτικά χαρακτηριστικά, καθώς και συγκρίνεται η φυσική μη-κλωνοποίησιμη πηγή με ψευδο-πραγματικούς αριθμούς – αποδεικνύοντας έτσι την μοναδικότητα κάθε συσκευής ως μη-κλωνοποίηση πηγή [34]. Στο κεφάλαια 4 καταβάλλονται οι προσπάθειες διόρθωσης σφαλμάτων, και παράλληλα ελέγχεται η αντοχή των μη-δυνατών PUF σε επίθεση τεχνίτης νοημοσύνης, ενάντιας των παραγόμενων ζευγαριών. Τέλος στο κεφάλαια 5 συνεπάγεται και συζητούνται τα συμπεράσματα όλου του έργου, και γίνεται αναφορά στις μελλοντικές αναβαθμίσεις και προτάσεις βελτίωσης.

Κεφάλαιο 2

Θεωρητικό υπόβαθρο

"Although rewards can control people's behavior—indeed, that is presumably why they are so widely advocated—the primary negative effect of rewards is that they tend to forestall self-regulation."

Deci, *A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation.*

Στην εισαγωγή γνωστοποιήθηκαν τα κίνητρα και προβληματισμοί της διατριβής, σε αυτό το κεφάλαιο γίνεται αιτιολογική έκθεση στις θεμελιώδεις πτυχές της σχεδίασης SRAM, τις σχεδιαστικές επιλογής πρωτοκόλλων ασφαλείας που κάνουν οι μηχανικοί και ερευνητές για να επιτύχουν απόδοση και αξιοπιστία. Το συμπέρασμά αυτό υποστηρίζεται στην κατάδοση αιτιών και τρόπους με τους οποίους οι μνήμες λειτουργούν, τρόποι βελτίωσης και αξιολόγησης για την ανίχνευση και τη διόρθωση αυτών των σφαλμάτων. Παρουσιάζονται οι ταξινομήσεις αστοχιών και τα διάφορα στοιχεία των μνημών στα οποία μπορεί να εμφανιστούν αυτές οι αστοχίες.

2.1 Ορισμοί

Στο τμήμα αυτό της ενότητας διερευνάτε η θεμελιώδης θεωρία των βασικών εννοιών της πραγματικής τυχαιότητας, και την επέκταση της ευρέως χρησιμοποιούμενης τεχνικές εξόρυξης και κατεργασίας των εγγενών χαρακτηριστικών μιας μη αντιγράψιμης πηγής, καθώς και τις επιβαρύνσεις υπολογιστικών πόρων και τα οφέλη που μπορούν να επιτευχθούν. Αρχικά συζητάτε η θεωρία της αμοιβαίας πληροφορίας, στη συνέχεια αναφέρονται τα μέτρα αξιολόγησης που παρέχουν τις υποδείξεις στη λογική κωδικοποίησης, παρέχοντας τα μέσα για την συλλογή δείγματος.

2.1.1 Μη αντιγράψιμα συστήματα

Πρώτου προχωρήσουμε παρακάτω, σκόπιμο είναι να διατυπωθούν οι βασικές έννοιες και ορισμοί, στους οποίους στη συνέχεια θα βασιστούν πιο πολυσύνθετες μαθητικές εφαρμογές, για τις οποίες η ασάφεια τους θα εξαλειφθεί. Όσον αναφορά τους εν λόγω ερευνητικούς τομείς όπως είναι η βαθμονόμηση των μη-κλωνοποίσημων συναρτήσεων και οι τρόποι υλοποίησης τους σε πρωτόκολλα θα μας απασχολήσει στο κεφάλαιο 3.1.2.

2.1.1.1 Φυσική πηγή τυχαιότητας

Φυσική πηγή τυχαιώτητας, φυσικό φαινόμενο. Αναφορικά μερικά παραδείγματα είναι, η μέτρηση εξωτερικών ηλεκτρομαγνητικών και κβαντικών φαινομένων, τα οποία παράγουν εγγενή τυχαιότητα (εντροπία) . Επίσης, οι φυσικοί παράμετροι που επιφέρουν τυχαίους αριθμούς, δηλαδή τάση, χρονική καθυστέρηση, συχνότητα, και άλλα εκμεταλλεύσιμα μέσα, μπορούν να συγκριθούν ως ξεχωριστές οντότητες σε μορφή δυαδικών ακολουθιών ή όπως αναφέρονται και στην βιβλιογραφία, ζεύγη απόκρισης παραμέτρου (CRP – Challenge-response Pairs), που ο Maes προσπάθησε να διαχωρίσει σε δύο μεγάλές κατηγορίες, αναλόγα εάν οι παράμετροι απόκρισης είναι διακριτού(μετρήσιμου) σύνολού CRP (Weak PUF), και από την αντίθετη πλευρά να παράγονται αμερόληπτα(άπειρα), ενοποιημένα ως ισχυρές μη-κλωνοποίησημες πηγές(Strong PUF). Εντούτοις, όπως θα δούμε σε βάθος, στις ακόλουθες ενότητες της αναφοράς, τα εγγενείς χαρακτηστικά μίας μη-κλωνοποίσημης ρίζας, χαρακτηρίζονται ως απρόβλεπτα μέχρι τη διάγνωση – καθιστώντας το φαινόμενο αυτό, μοναδικό. Τέλος, ιδανική περίπτωση των μη προβλέψιμων ιδιοτήτων, είναι όχι μόνο να παράγεται ίδια ακριβώς έξοδος(για την ίδια είσοδο), αλλά και απόσταση μεταξύ των σειρών bit, από την ίδια συσκευή να έχουν τις μισές αντίστοιχες τιμές μεταξύ – παράλληλα, αυτό καθιστά δύσκολη την αναπαραγωγή

στην πράξη, λόγο μεταβολών της θερμοκρασίας, τάσης τροφοδοσίας και φθοράς της συσκευής λόγο ηλικίας, εμφανίζοντας θόρυβο στις αποκρίσεις.

2.1.1.2 Φυσικές μονόδρομες συναρτήσεις

Φυσικές μονόδρομες συναρτήσεις αντιπροσωπεύουν τον ορισμό πως, μια ντετερμινιστική φυσική αλληλεπίδραση σε σταθερό χρόνο που είναι σταθερή, σε αντίθεση με την πιθανότητα αποκάλυψης στοιχείου είτε αμερόληπτα, είτε σε πεπερασμένο ανεξάντλητη μοντελοποίηση – χωρίς να λαμβάνεται υπόψη η έννοια του θορύβου. Ο ορισμός τους πρωτο-αναφέρθηκε στην διπλωματική διατριβή του Pappu [11], εποπτεύοντας τα έμφυτα οφέλη του οπτικού μέσου, στο οποίο ο ορισμός βασίζεται αποκλειστικά και μόνο.

2.1.1.3 Μη κλωνοποίσημες συναρτήσεις (Physically Unclonable Function – PUF)

Η σημαντικότερη έννοια αυτής της έρευνας, είναι οι φυσικές, μη-κλωνοποίσημες πηγές, γνωστές και ως PUF(Physically Unclonable Functions), οι οποίες αναφέρονται στην φυσική ιδιότητα ενός αντικειμένου, να παράγει εγγενή μοναδικά χαρακτηριστικά, χάρις τον αναπόφευκτο τρόπο δημιουργίας του από τον κατασκευαστής, τα οποία αντιπροσωπεύονται στην βιβλιογραφία επισημαίνονται ως CRP(Challenge-response pairs), και εξαγάγετέ ρητώς πραγματική τυχαιότα, γνωστή(True random number generators – TRNGs). Σε τούτη την εργασία, το φυσικό φαινόμενο για το οποίο, πραγματοποιήθηκαν όλα τα πειράματα, είναι τα ολοκλωμένα κυκλώματα στατικής μνήμης SRAM, και επειδή κάθε τρανζίστορ παρουσιάζει μοναδικά χαρακτηριστικά, τα οποία αναλυτικά είναι διατυπωμένα στο κεφάλαιο 3.0.1. Προκειμένου να θεωρηθούν ανεξάρτητοι, από την μία πλευρά οριοθετείτε ο τύπος εισόδου, αναλογικός ή δυαδικός(κατά προτίμηση), και από την άλλη, ο τρόπος δειγματοληψίας, καθώς προνομιούχες μέθοδοι προσφέρουν αντίστοιχα χαρακτηριστικά, όπως για παράδειγμα είναι ο θόρυβος. Το αντικείμενο αυτό αποτελείται από ιδιαίτερα εμπεριστατωμένης μελέτη, επειδή ακόμη και σε απόλυτα σταθερές εργαστηριακές συνθήκες, η ανταποκρισιμότητα δεν είναι ανταποκρίσιμη στο φαινόμενο γήρανσης.

2.2 Θεωρία πληροφορίας

Ένας κρίσιμος κλάδος της επιστήμης των υπολογιστών, η θεωρία πληροφορίας, και θα μας απασχολήσει η κωδικοποίησης και αποκωδικοποίηση σε διορθωμένη σειρά, σε συνδυασμό με χαρακτηριστικά μη αντιγράψημων συστημάτων. Σε αυτή την ενότητα παραθέτουνε οι κύριοι ορισμοί από τη θεωρία κωδικοποίησης που χρησιμοποιούνται σε όλα τα πειράματα της διατριβής.

2.2.1 Εντροπία

Η έννοια της εντροπίας σχετίζεται με μία μόνο τυχαία μεταβλητή, ή τυχαία κατάρτιση ολικής ή και περιορισμένης κλίμακας. Έστω X μια τυχαία μεταβλητή δυαδικού διανύσματος με μήκος N, όπου x είναι το αποτέλεσμα της, και με περιορισμό λογαριθμικής κλίμακας, έτσι ορίζεται ο περιορισμός της ελάχιστης εντροπίας. Σε μη-αντιγράψιμα συστήματα, εξ ορισμού. Άρα, η ελάχιστη εντροπία είναι η χειρότερη δυνατή εκτίμηση της προβλεψιμότητας μιας μυστικής μεταβλητής - και στην περίπτωση αξιολόγησης φυσικής πηγής, προκειμένου να εξασφαλιστεί ότι ένα μοναδικό μυστικό είναι πράγματι ομοιόμορφα κατανεμημένο πάνω στο σύνολο δεδομένων, πρέπει να εξαχθεί ένα αυστηρό κατώτερο όριο για την ελάχιστη εντροπία του σταθερού κλειδιού.

$$H_{\infty}(X) = -\log_2(max P(X = x)) \tag{2.1}$$

Τις τελευτές δεκαετίες έχουν επιτευχθεί καινοτόμες ανακαλύψεις στο κομμάτι της κωδικοποίησης σημάτων, καθώς και ερευνητική συνεισφορά του Shannon [35] μέχρι σήμερα έχει αποδείξει ότι πολλοί αλγόριθμοι όχι μόνο σε εργαστηριακές εγκαταστάσεις, αλλά και σε αντίξοες συνθήκες, πραγματεύονται σε ικανοποιητικά επίπεδα τον θόρυβο. Εν συντομία, αφού εισάχθηκαν οι κώδικες Χάμινγκ, το 1950 [36], οι Reed και Muller εφίβρησαν τους εκσυγχρονισμένους κωδικοποιητές-αποκωδικοποιητές, γνωστούς και ως Reed – Muller [37, 38].

2.2.2 Ελάχιστη εντροπία

Ένα από τα κυριότερα χαρακτηριστικά της κρυπτογραφίας είναι η απόκρυψη της πρόβλεψης ενός τυχαίου αριθμού [39]. Η πιθανότητα πρόβλεψης μιας τυχαίας

μεταβλητής η οποία προτάθηκε από τον Rényi [39], απαρτίζετε από x ορίζεται ως 2.3 που αντιπροσωπεύει την χειρότερη περίπτωση ανάκτησης της τυχαίας μεταβλητής. Το x έχει ελάχιστη εντροπία τουλάχιστον m , με την προϋπόθεση ότι $H_\infty(X) \geqslant m$ εάν ισχύ η σχέση 2.3. Η ελάχιστη εντροπία μιας διανομής μας λέει πόσα σχεδόν ομοιόμορφα τυχαία μπιτ μπορούν να εξαχθούν.

$$H_{min} : \quad H_\infty(X) = -\log_2 max P(X = x) \tag{2.2}$$

2.2.2.1 Υπολογισμός ελάχιστης εντροπίας

Η αμοιβαία πληροφορία μεταξύ του ζεύγους διακριτών τυχαίων μεταβλητών X και Y με τις αντίστοιχες τιμές τους x και y, ορίζεται ως εξής [40].

$$I(X;Y) \stackrel{\Delta}{=} -\sum_{x \in X} \sum_{y \in Y} p_{XY} \log_2 (\frac{p_{XY}(x,y)}{p_Y(x) p_Y(y)}) \tag{2.3}$$

2.2.3 Απόσταση Χάμινγκ

Μια παράμετρος της θεωρίας πληροφορίας, είναι οι κώδικες διόρθωσης σφαλμάτων Χάμινγκ, παρουσιάστηκε από τον Richard Hamming et al το 1950 - αντιπροσωπεύοντας τον αριθμό διαφορετικών στοιχείων μεταξύ δύο συμβολοσειρών ίδιου μήκους, με την βοήθεια της λογικής πράξης XOR [41], και παρακάτω στο σχήμα 2.1 υπάρχουν αναλυτικά οι μαθηματικές πράξεις με ένα παράδειγμα. Κατά συνέπεια, τα σφάλματα που προκαλούνται σε ένα θορυβώδες κανάλι ή μέσο αποθήκευσης μπορούν να μειωθούν σε οποιοδήποτε επιθυμητό επίπεδο χωρίς να θυσιάζεται ο ρυθμός μετάδοσης ή αποθήκευσης πληροφοριών – με άλλα λόγια, οι δυαδικές κωδικοποιημένες λέξεις, έστω των διανυσμάτων s και f, το βάρος Χάμινγκ είναι η διαφορά τους $s - f$, για την οποία ισχύει το αντιμεταθετό αξίωμα. Οι διαθέσιμες ιδιότητες είναι τρείς, και πιο συγκεκριμένα εάν το αποτέλεσμα της απόστασης Χάμινγκ είναι μεγαλύτερο του μηδέν, τότε τα διανύσματα εισόδου είναι μεταξύ τους ίσα. Αμέσως μετά, ισχύει η αντιμεταθετική ιδιότητα των διανυσμάτων, δηλαδή $h_d(s,f) = h_d(f,s)$. Τελευταία περίπτωση είναι πως το άθροισμα του επιμερισμού της αρχικής σχέσης $h_d(s,f)$ με $h_d(f,c)$, τότε θα είναι ίσο ή μεγαλύτερο του $h_d(s,c)$.

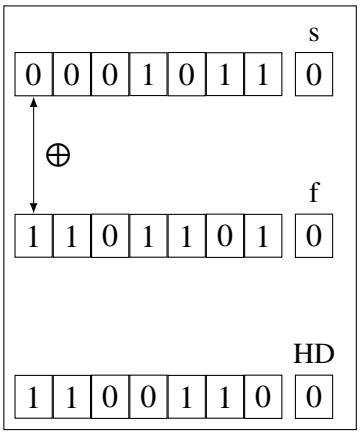

Fig. 2.1 Παράδειγμα απόστασης Χάμινγκ σειράς επτά μπιτ.

$$h_d : \quad h(s,f) = h_w(s-f) = h_w(f-s) \tag{2.4}$$

Η απόσταση Χάμινγκ μπορεί επίσης να εκφραστεί είτε ως αναλογία είτε σε ποσοστό, εκφραζόμενο ως κλάσμα μήκους των διανυσμάτων. Άρα, το αποτέλεσμα του αθροίσματος διαιρείται με το μήκος της συμβολοσειράς, και τελικά πολλαπλασιάζεται με το 100. Οπότε, για L ως μήκος του κώδικα, υπολογίζεται η απόσταση Χάμινγκ.

$$HD : \quad HD = (\frac{1}{L}\sum_{i=1}^{n} s_i + f_i \ \ mod\ 2) \times 100\% \tag{2.5}$$

2.2.4 Βάρος Χάμινγκ

Το βάρος Χάμινγκ h_w είναι απλά το άθροισμα των θετικών στοιχείων ενός διανύσματος τιμών $x = (x_0, x_1, ..., x_n - 1)$. Στην περίπτωση αυτή, τα μη-μηδινικά στοιχεία χαρακτηρίζοντια ως $x = \begin{cases} 1 & x_i \neq 0 \\ 0 & x_i = 0 \end{cases}$, αντίστοιχα.

Η απόσταση Χάμινγκ 2.2.3 και το βάρος Hamming μπορούν να χρησιμοποιηθούν για την διαχείριση σφαλμάτων ενός συγκεκριμένου κώδικα. Σε αντιπαράθεση με την θεμελιώδες αρχή των μη-κλωνοποίησιμων συστημάτων, η πραγματική στατιστική ομοιομορφία 3.0.6, ικανοποιείται με την ίσο χωρισμό μηδικών και άσσων, δηλαδή το

ποσοστό βάρους Χάμινγκ να είναι ίσο με 50% – σαφέστερα, η απόσταση Χάμινγκ κατανέμεται διωνικά 2.2.7.

$$h_w : \quad h_w(x) = \sum_{i=0}^{n-1} d(x_i, 0) \tag{2.6}$$

2.2.5 Εσωτερική κλάση Χάμινγκ

Η απόστασης Χάμινγκ μπορεί να προσαρμοστεί για την αξιολόγηση ενός συγκεκριμένου κυκλώματος μη-αντιγράψιμης πηγής, γνωστή και ως εσωτερική απόστασης HD_{intra} (intra ή intra-chip Hamming distance). Ειδικότερα, για ένα συγκεκριμένο διάνυσμα PUF, απόσταση μεταξύ ενός ζευγαριού ίδιων τιμών, σε σχέση με τον μεταβαλλόμενο χρόνο - η απόσταση και βάρος Χάμινγκ χρησιμοποιούνται για να υπολογίσουν τον αριθμό σφαλμάτων που εισήχθησαν στο κανάλι, δηλαδή το υπόλοιπο του κωδικοποιημένης τιμής σε σχέση με την ληφθείσα λέξη(πράξη βάρους Χάμινγκ). Ανακεφαλαιώνοντας, έχοντας την ίδια πηγή με δείκτη τιμής i, υπολογίζεται το άθροισμα της απόστασης Χάμινγκ σε διαφορετική δειγματοληψία (πχ. διαφορετική θερμοκρασία).

$$HD_{intra} : \quad HD_{intra} = \sum_{i=0}^{n-1} x_i \oplus x_i' \tag{2.7}$$

2.2.6 Εξωτερική κλάση Χάμινγκ

Από την άλλη μεριά, η απόσταση Χάμινγκ μπορεί επίσης να εφαρμοστεί σε δύο κατασκευαστικά ίδια, αλλά διαφορετικά κυκλώματα. Αυτό το σημαντικό μέτρο, είναι γνωστό ως inter Hamming Distance, και δείχνει την μοναδικότητα κάθε μη-κλωνοποιήσημης πηγής, και εάν ορισμένα ή φυσικά όλα τα bit είναι στατιστικά προκατειλημμένα προς μια συγκεκριμένη τιμή. Οπότε, για ένα σύνολο δειγμάτων ίδιου κυκλώματος αλλά με διαφορετικές συσκευές, υπολογίζεται η απόσταση Χάμινγκ την ίδιας θέσης μνήμης a, και x ορίζεται ο πανομοιότυπος εξοπλισμός.

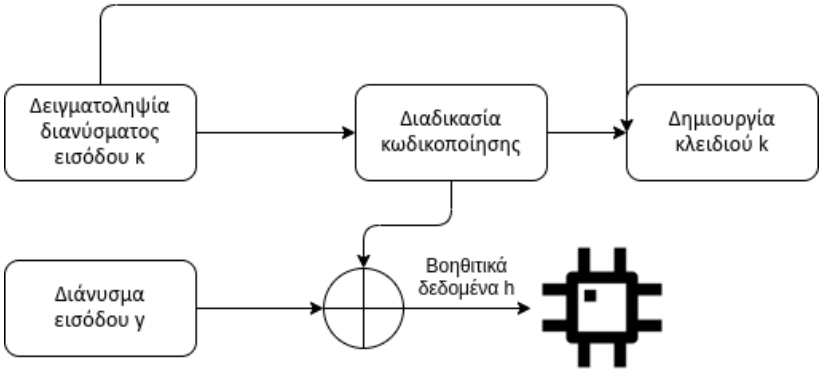

Fig. 2.2 Μπλοκ διάγραμμα εργασιών της κατασκευής.

$$HD_{inter} : \quad HD_{inter} = \sum_{a=0}^{a-1} x_a \oplus x'_a \tag{2.8}$$

2.2.7 Διωνυμική κατανομή

Ο μέσος όρος δειγματοληψίας, είναι το σύνολο της κατανομής των άσσων και μηδενικών x_i, μιας ή περισσότερων αποκρίσεων πλήθους n. Πρακτικά, οι μπιτοσερές των δειγμάτων αποτελούνται από τις τιμές, 0 ή 1, άρα η μέση τιμή μ , σε αναλογία με το πλήθος.

$$\mu : \quad \mu = \frac{1}{n} \sum_{i=0}^{n} x_i = / = o \tag{2.9}$$

Έτσι, υποθέτοντας ότι κάθε απόκριση εγγραφής κλειδιού (enrollment – δες 2.2) $x \in 0, 1$, και αντίστοιχα το σύνολο ανακατασκευής (reconstruction – δες 2.3) $y \in 0, 1$, η σχετικότητα μεταξύ αυτών των συνόλων μήκους n.

$$P(X^n = x^n, Y^n = y^n) = \prod_{c=1}^{n} C(x_c, y_c) \tag{2.10}$$

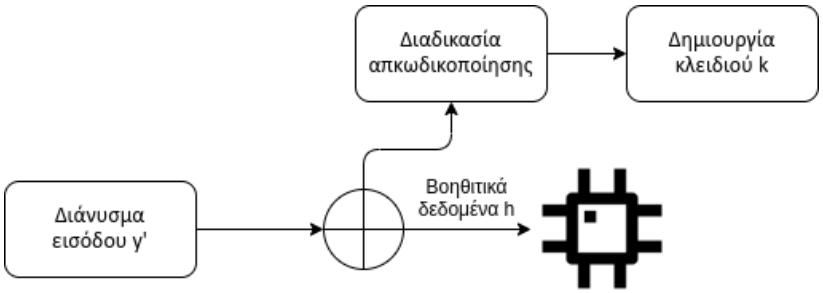

Fig. 2.3 Μπλοκ διάγραμμα εργασιών της ανακατασκευής.

2.3 Ροή δεδομένων

Μια από τις εφαρμογές των μη-αντιγράψημων πηγών που εκμεταλλεύεται τα εγγενή χαρακτηριστικά, δηλαδή η δημιουργία κλειδιών, είτε είναι η αστάθεια απόκρισης λόγο θορύβου, είτε οι προδιαγραφές ασφάλειας απαιτούν περεταίρω επεξεργασία για την αποφυγή φυσικών επιθέσεων επαφής. Για τους παραπάνω λόγους σε αυτή την ενότητα θα αναφερθούν τρόποι διόρθωσης και σφαλμάτων.

2.3.1 Κωδικοί αριθμοί ασφαλούς σχεδίου

Κατά το στάδιο εγγραφής ενός τυπικού βιομετρικού κρυπτοσυστήματος, το βιομετρικό πρότυπο κωδικοποιείται ουσιαστικά με ένα κλειδί για τη δημιουργία του προστατευμένου προτύπου, που ονομάζεται ασφαλές σχεδίου (ή Secure Sketch) [42], το οποίο προτάθηκε από τον Dodis et al έχοντας εμπνευστεί από την ιδέα του Buttler σε κβαντικά συστήματα at al [43], και είναι δημόσια διαθέσιμο, χωρίς να αποκαλύπτει σημαντικές πληροφορίες σχετικά με το σχετικό βιομετρικό πρότυπο ή κλειδί. Κατά τη διάρκεια του ελέγχου ταυτότητας, πρώτα έχει προηγηθεί η κατάσταση παραγωγής, κατά την οποία δημιουργεί τα bits των βοηθητικά δεδομένα, τα οποία είναι υπεύθυνα για την διόρθωση σφαλμάτων. Αντίστοιχα, στην μελλοντική αναπαραγωγή (ανάκτηση κλειδιού), έτσι, με την βοήθεια της απόστασης Χάμινγκ που αξιολογείται η ακρίβεια της κατασκευή, κατασκευάζεται το κλειδί χωρίς σφάλματα. Τα τελευταία χρόνια, στην πρόσφατη βιβλιογραφία έχουν προταθεί και αναλυθεί διαφορετικοί προσεγγιστικοί τρόποι με την χρήση γραμμικών κωδικών [44–51].

2.3.2 Σφάλμα σειρών bit

Κατά την πραγματοποίηση μη κλωνοποίσημων πηγών, υπάρχουν πολλές περιπτώσεις στις οποίες παρουσιάζονται σφάλματα, είτε στοχαστικά ή ντετερμινιστικά, κατά την δειγματοληψία —— λόγο ότι οι φυσικοί παράγοντες όπως είναι η θερμοκρασία, ηλικία και ιδιαίτερα χαρακτηριστικά εξοπλισμού, ελλοχεύει κινδύνους θορύβου στην σειρά διευθύνσεων της μνήμης (non-volatile ή όχι) —— ή αναλόγως το επιλεγμένο μέσο κατασκευής PUF. Παράλυτά, για το σενάριο χρήσης αυθεντικοποίησης, έχουν δοκιμαστεί τρόποι διορθωθείσης ενός συγκεκριμένου αριθμού μπιτ, με ικανοποιητικά αποτελέσματα. Ωστόσο, κάποιες εφαρμογές που είναι ευπαθές σε επιθέσεις με χρήση τεχνίτης νοημοσύνης [52], είτε η αρχιτεκτονική απαιτεί υψηλές απαιτήσεις σταθερότητας αποτελεσμάτων, όπως είναι έξυπνες εφαρμογές υλοποιημένες σε blockchain [53] ή σε ιατρικά και βιομηχανικά όργανα, στα οποία η ασφάλεια είναι κρίσιμη [54–56]. Επεκτείνοντας την ακρίβεια, τρόποι διόρθωσης περιορισμένων bit, όπως η απόσταση Χάμινγκ(Hamming Distance - HD) [41], έχουν αποδειχθεί αποτελεσματικοί ενάντιας στο πρόβλημα του θορύβου. Επιπλέων, το όργανο μέτρησης του ποσοστού σφαλμάτων, ή αλλιώς BER (Bit Error Rate). Μια ιδανική πηγή PUF πρέπει να έχει μηδενισμένο αυτό το μέτρο, δηλαδή ανύπαρκτη παρουσία θορύβου και σταθερότητα της ελάχιστης εντροπίας. Εκτός από την κλασική χρήση των βιομετρικών χαρακτηριστικών για αυθεντικοποίηση [57, 58], το κυριότερο μειονέκτημα αυτής της μεθοδολογίας, είναι πως το μέσο αυθεντικοποίησης πρέπει να αποθηκευτεί, προκειμένου να γίνει αυθεντικοποίησης ή πιστοποίηση μίας οντότητας – ελλοχεύοντας την ίδια στιγμή προβλήματα, ασφαλείας και ιδιοτικότητας. Γι' αυτό τον λόγο, μια πρωτοπόρα λύση σε τούτο το πρόβλημα, ήταν ο fuzzy extractor σε κλειστά διαστήματα [42, 59]. Στην συνέχεια της επόμενης παραγράφου ακολουθεί αναλυτική Περιγραφή, και ανασκόπηση των μεθόδων πάνω σε ασαφούς ανακτητές 2.3.3, οι οποίες έχουν χρησιμοποιηθεί σε αρκετές δημοσιεύσεις για διαφορετικά σενάρια και κώδικες διόρθωσης [60, 17, 61–66].

2.3.3 Ασαφής ανάκτηση

Ξεκινώντας από τον ορισμό, η καινοφανής έννοια της τυχαίας ασάφειας (ή Fuzzy extractor), αναφέρετε στην αστάθεια συμπεριφοράς εγγενών χαρακτηριστικών, τα οποία μεταμορφώνουν μια αναμενόμενη συμπεριφορά, είτε λόγω λανθασμένης κατανομής ως προς την ομοιομορφία, ή με τις (περιβαλοντικές)παρεμβολές τους, κατά την χρήση, με την πάροδο του χρόνου [67, 68]. Επίσης, από το σύστημα ενός ανακτητή ασάφειας ($FuzzyExtractor$ - FE), με είσοδο w, μια ομοιόμορφη τυχαία-συμβολοσειρά k, και,

δημόσια δεδομένα h – η οποία την ίδια στιγμή δεν πρέπει να αποκαλύπτει πληροφορίες σχετικά με το k [67]. Πρέπει να σημειωθεί πως, αναλόγως του σχήματος διόρθωσης, ο αριθμός των μπιτ που μπορούν να αντισταθμιστούν είναι κάθε φορά πεπερασμένος. Τέλος, το μυστικό k μπορεί να καιροφυλακτηθεί για ανάκτηση από το h και μια δεύτερη είσοδο w_0, εάν το w_0 είναι αρκετά κοντά στο w. Προκειμένου να παραχθεί έξοδος με πλήρη εντροπία, η διορθωμένη απόκριση w_0 είναι αποτέλεσμα από κάποιον αλγόριθμο κατακερματισμού [67].

Από την άλλη μεριά, τα μέτρα της απόστασης Χάμινγκ, τα οποία αναφερθήκαμε παραπάνω, και πιο συγκεκριμένα τα HD_{inter} και HD_{intra}, αντίστοιχα, μπορούν να προσδιορίσουν την απόκριση ενός ασαφή ανακτητή, υπό την προϋπόθεση πως η απόσταση κατωφλίου HD_{inter}, να είναι η μισή – κάτι που πρακτικά είναι δύσκολο.

2.3.4 Βοηθητικά δεδομένα

Καθοριστικής σημασίας απαίτηση για την αξιοπιστία την μη αντιγράψιμης πηγής είναι η σταθερότητα παραγωγής κλειδιών σε ένα ευρύ φάσμα συνθηκών θερμοκρασίας, τάσης και γήρανσης. Ωστόσο, οι μη αντιγράψημες πηγές βασίζονται στην εγγενή αναντιστοιχία μεταξύ δύο φυσικώς πανομοιότυπων συσκευών – επομένως η απόκριση(εξόδου) μπορεί να ανατραπεί οποιαδήποτε στιγμή με την παρουσία τυχαίου χρονικού θορύβου. Έτσι, για τη διόρθωση των ασταθών αποκρίσεων εφευρέθηκαν εφαρμογές σε ποικίλους τομείς, όπως είναι η επεξεργασία πριν ή μετά της εισόδου απόκρισης, συνυπολογίζοντας τα λειτουργικά σφάλματα θορύβου. Σε αυτό το πλαίσιο, οι θορυβώδεις αποκρίσεις αντιμετωπίζονται με κάποιες μεθόδους, οι οποίες αναφέρονται αναλυτικά παρακάτω, και λειτουργούν είτε ως διορθωτές σφαλμάτων μπιτ, ή για την αποφυγή αναστροφής κατάστασης μπιτ. Οι αλγόριθμοι βοηθητικών δεδομένων(ή Helper Data) εφαρμόζονται όταν μια θορυβώδεις απόκριση αμφισβητηθεί, δηλαδή τα βοηθητικά δεδομένα μπορούν να χρησιμοποιηθούν για τη διόρθωση σφάλματος, άρα για την ανακατασκευή της απόκρισης. Εντούτοις, πρέπει να σημειωθεί ότι υπάρχουν διάφορα μειονεκτήματα, πρώτον τα βοηθητικά δεδομένα αποκαλύπτουν πληροφορίες ευάλωτες πληροφορίες της μη αντιγράψιμης πηγής και έτσι καθιστούν τα μυστικά ευάλωτα σε επιθέσεις. Δεύτερον, προκύπτουν επιπλέον μαθηματικοί υπολογισμοί στη σχεδίαση λόγο υλοποίησης του συνδρόμου και της αποθήκευσης των βοηθητικών δεδομένων - κάτι που επιβαρύνει έξυπνες ενσωματωμένες συσκευές λίγων δυνατοτήτων.

2.3.4.1 Διεργασία αποκατάστασης δεδομένων

Πέρα τις πολλές προτάσεις αλγορίθμων διαχείρισης βοηθητικών δεδομένων, οι τεχνικές διόρθωσης σφαλμάτων γενικεύονται σε τρείς μεγάλες κατηγορίες σχημάτων, γραμμικών, μοτίβων, και σχήματα βασισμένα σε δείκτες [69] - αναλυτικά αναφέρονται μερικές δημοφιλείς προσεγγίσεις.

2.3.4.1.1 Κώδικες μετατόπισης

Ένα δημοφιλές γραμμικό σχήμα είναι οι κώδικες μετατόπισης (code-offset) λύνουν το πρόβλημα των εκτεθειμένων πληροφοριών ενός κλειδιού με την χρήση συνάρτησης κατακερματισμού, καθώς ο υπολογισμός των βοηθητικών δεδομένων είναι πανομοιότυπος με την ασαφή ανάκτηση. Υπό αυτή την έννοια, οι τιμές του συνδρόμου εντροπίας πρέπει να είναι όσο το δυνατόν μικρότερες, ώστε η διαρρέουσα πληροφορία να μην υπερβαίνει την εντροπία της μυστικής συμβολοσειράς, επομένως η εναπομένουσα εντροπία μετά την εκμετάλλευση του σχήματος αυτού, εξαρτάται από την ελάχιστη εντροπία των απαντήσεων της μη αντιγράψιμης πηγής, και τον αριθμού του συνδρόμου μπιτ [70].

2.3.4.1.2 Σχήματα διανυσμάτων σε μοτίβα

Τα διανύσματα προτύπων αντιστοιχούν σε πρότυπα πολλών ακολουθιών απαντήσεων, δηλαδή δημόσιες βοηθητικές πληροφορίες, οι οποίες χρησιμοποιούνται αργότερα ως ένα σύνολο προτύπων που συγκρίνονται με τα αναγεννημένα μπιτ απαντήσεων. Οπότε, σε κάθε ταύτιση η τιμή δείκτη της πρόκλησης που παράγει αυτή την αντιστοιχισμένη απάντηση θα χρησιμοποιηθεί ως υπο-κλειδί σε πεπερασμένος αριθμό επαναλήψεων.

Δεδομένου ότι μόνο ένα μικρό σύνολο προτύπων απόκρισης (βοηθητικά δεδομένα) απαντήσεων εκτίθεται, είναι σχεδόν αδύνατον να φτιαχτεί κάποιο μοντέλο ανακατασκευής [71].

2.3.4.1.3 Σχήματα βασισμένα σε δείκτες

Η βασική ιδέα του σχήματος συνδρόμου βασισμένοι σε δείκτες (Index-based syndrome coding – (IBS)), είναι πως οι κατανεμημένοι έξοδοι συνδρόμου, χρησιμοποιούνται ως δείκτης μιας ακολουθίας μιας απάντησης μη αντιγράψιμης πηγής, δεδομένου ότι η μεροληψία εντός των τιμών αυτών δεν αναμένεται να αλλάξει, άρα δεν διαρρέει καμία

πληροφορία της ελάχιστης εντροπίας των μυστικών μπιτ [66]. Σε κάθε δείκτη της σειράς απόκρισης, αφού αποθηκευτεί στα βοηθητικά δεδομένα, αλγοριθμικά γίνεται επιλογή των αξιόπιστων μπιτ (ανάλογα την υλοποίηση – για παράδειγμα, σταθερά μπιτ μπορούν να θεωρηθούν μόνο οι άσσοι, ή μαζί ή και χωριστά τα μηδενικά), και στην συνέχεια μειώνεται η πιθανότητα σφάλματος με χρήση αποκωδικοποιητών.

2.4 Ιεραρχεία μη κλωνοποίσημων πηγών

Μια φυσική οντότητα εκτός από τις υποκατηγορίες ταξινόμησης με βάση τα δειγματοληπτικά ζεύγη απόκρισης, υπάρχουν πολλοί παράμετροι που μπορούν να διαχωρίσουν τα έμφυτα συστατικά μιας κατασκευής, τα οποία παράγονται από μια ενσωματωμένη συσκευή με την βοήθεια εξοπλισμού μέτρησης, χρησιμοποιώντας την φυσική ροή - χωρίς την ανάγκη για περαιτέρω επεξεργασίας.

Σε αυτήν την ενότητα, θα συζητηθεί μια σύντομη επισκόπηση, μαζί με παραδείγματα διαφορετικών τύπων πηγών πραγματικής τυχαιότητας, διαμορφώσεων και αποτελεσμάτων απόδοσης.

2.4.1 Παραγωγή μη-αντιγράψημων συναρτήσεων μέσα από μνήμη

Με βάση τον μεγάλο όγκο παραλλαγών μη-κλωνοποίησιμων πηγών [13], η μεγαλύτερη κατηγορία είναι οι συσκευές μνήμης έχοντας ως βάση το πυρίτιο, όπως είναι για παράδειγμα τα D flip-flops και SRAM. Ένα πλεονέκτημα αυτής της κατηγορίας, είναι η ευημερία παροχής αντίστοιχων τιμών σε δυαδική γλώσσα. Συγκεφαλαιώνοντας, προσέχοντας πλεονεκτήματα και αδυναμίες κάθε τεχνολογίας, αυτές αποτελούν μια καλή επιλογή υλοποίησης σε αντιπαράθεση με τις προδιαγραφές ενός συστήματος. Σε αυτή την εργασία θα μας απασχολήσουν μόνο οι μνήμες τύπου SRAM 2.4.1.1.

2.4.1.1 Μνήμη τύπου SRAM

Ένας τύπος μνήμης ημιαγωγών των ηλεκτρονικών συσκευών είναι μια συστοιχία κελιών μνήμης, γνωστή ως στατική μνήμη τυχαίας προσπέλασης (Static random-access memory - SRAM), η οποία συνήθως χρησιμοποιείται σε μικροελεγκτές συσκευών όπως IoT ή γενικά σε ενσωματωμένα συστήματα. Αυτού του είδος μνήμη εάν τροποποηθεί ή και όχι, μπορεί αυτούσια να χρησιμοποιηθεί ως πηγή τυχαιώτητας σε συνεργασία με την ασυμμετρία μεταξύ δύο υπο-αντιστροφών κατά την εκλογή αναγνωριστικού μέσα σε έναν βρόχο -

με αλλά λόγια, η συμπεριφορά αυτή ονομάζεται κατάστασή εκκίνησης 2.4.1.2, στην οποία επιβάλλεται η τιμή(μεταφορά τάσης) στο κελί για την ορθή λειτουργία του ολοκληρωμένου κυκλώματος ASIC. Η προέλευση της πηγής τυχαιότητα έχει επιρροή από την εκκίνηση των δομημένων κελιών της μνήμης SRAM πριν το άνοιγμα της κεντρικής μνήμης, δημιουργώντας έτσι ένα μοναδικό αναγνωριστικό για την συσκευή. Το αναγνωριστικό αυτό, έγκειται ακολουθώντας κάποια κριτήρια τα οποία αναλύονται παρακάτω στο κεφάλαιο 3.0.1. Αυτή η ιδέα προτάθηκε για πρώτη φορά το 2004 από τον Layman [72], και αργότερα από τους Guajardo [60], και παράλληλα σύνθετες παραλλαγές ειπώθηκαν από τον Holcomb [15]. Επομένως, μια θεμελιώδης διαφορά μεταξύ των προτεινόμενων κυκλωμάτων που χρησιμοποιούνται ως πηγή, οι παραλλαγές είναι διαχωρισμένες ανάλογα εάν εκμεταλλεύονται, χωρίς περεταίρω επεξεργασία(του κατασκευαστή), τα εγγενή φαινόμενα, ενώ από την άλλη πλευρά – οκλήρωση παραγωγής γίνεται με διαμόρφωση του κυκλώματος. Άρα, ο διαχωρισμός είναι είτε μοναδικός ζεύγος τιμών μη-κλωνοποίησιμων συναρτήσεων (Single-Challenge PUF ή SCPUF), και σε αυτή τη περίπτωση η μη-αντιγράψημη πηγή είναι αποτέλεσμα bit, γραμμικά ανάλογα με το πλήθος απόκρισης, και από την άλλη μεριά, πολλά ζεύγη τιμών μη-κλωνοποίησιμων συναρτήσεων(Multi-Challenge PUF ή MCPUF) που σε αυτή την σε αυτή την κατηγορία, πολλά χακτηριστικά του κυκλώματος συνδυάζονται μεταξύ τους, όπως είναι αναμιγμένη δειγματοληψία και προσαρμογή του περιβάλλοντος εργασίας. Το πλεονέκτημα αυτής της μεθόδου, είναι διαθεσιμότητα εξοπλισμού, γιατί στα σύγχρονα κυκλώματα προτιμάται ο χειρισμός αυτού του είδους μνήμης. Αντίστροφα, το μεγαλύτερο μειονέκτημα είναι η ευαίσθητοι στις περιβαλλοντικές μεταβολές, ήτοι σε πιθανή μείωση απόδοσης σταθερότητας απόκρισης σε αναλογία με τον χρόνο.

Για την κατανόηση της συμπεριφοράς των μη αντιγράψημων πηγών SRAM στην επόμενη υπο-ενότητα περιγράφεται η γενική δομή των κελιών SRAM, βασικές λειτουργίες και η συμπεριφορά εκκίνησης. Κατά πάγια τακτική, για τη δημιουργία ενός κλειδιού, ένας περιορισμένος αριθμός τιμών της απόκρισης διαθέτοντας για την δημιουργία κλειδιού, αλλά για τη δημιουργία κλειδιού ένας περιορισμένος αριθμός μπιτ απόκρισης είναι καταλυμένος, και οι διαδεδομένοι τρόποι επικύρωσης αποσφαλμάτωσης συμβόλων είναι, με προσομοίωση ενός συνόλου δεδομένου προηγούμενων προσεγγίσεων, έπειτα με μαθηματική επικύρωση ενός καθορισμένου κατωφλίου, και τέλος με εμπειρική προσέγγιση είτε με πεπερασμένο αριθμό δεδομένων, είτε με μηχανική μάθηση.

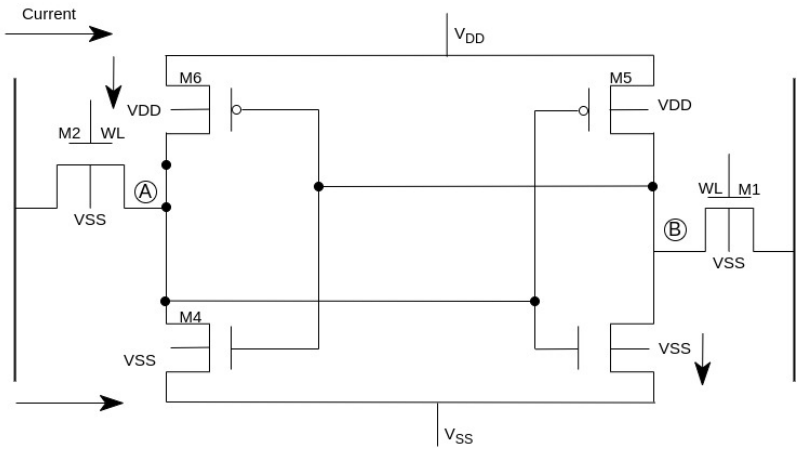

Fig. 2.4 Δομή κελιού 6T SRAM [73, 74].

2.4.1.1.1 Δομή κελιών

Το σημαντικότερο κομμάτι κάθε μνήμης SRAM είναι τα κελία, στα οποία μπορεί να αποθηκευτεί ένα μπιτ δεδομένων. Η πιο συνηθισμένη τοπολογία αποτελείται από 6 τρανζίστορ CMOS που είναι χωρισμένα σε δύο διασυνδεδεμένους μετατροπείς CMOS και δύο τρανζίστορ εισόδου. Η απεικόνιση 2.4 δείχνει τη δομή ενός κελιού SRAM. Το είδος των κελιών του εξοπλισμού χαρακτηρίζεται από έξι τρανζίστορ, και πιο συγκεκριμένα το κάθε κελί μνήμης, κατασκευάζεται χάρις δύο τρανζίστορ πρόσβασης, σε αντιστοιχία με ίδιου πλήθους διασυνδεδεμένων μετατροπέων.

Ειδικότερα, αποτελείται από δύο συνδεδεμένους μετατροπείς και δύο τρανζίστορ εισόδου A και B, τα οποία είναι υπεύθυνα για λειτουργίες ανάγνωσης και καταγραφής στο κελί. Τα τρανζίστορ εισόδου συνδέονται μεταξύ θύρες εισόδου / εξόδου που είναι γνωστές ως bitlines (BL και BL αντίστοιχα) και μετατροπέων. Η ενεργοποίηση των τρανζίστορ εισόδου γίνεται μέσω της γραμμής λέξεων (WL), με αποτελέσματα οι λειτουργίες ανάγνωσης και καταγραφής από τις θύρες BL. Υπάρχουν διάφορες παράμετροι απόδοσης που συνδέονται με τη σταθερότητα και τις καθυστερήσεις που σχετίζονται με διάφορες λειτουργίες.

2.4.1.1.2 Λειτουργία αναμονής

Σε αυτή την κατάσταση το κελί SRAM τα δεδομένα διατηρούνται εφόσον τροφοδοτείται το κελί στον μανδάλου (latch) και τα τρανζίστορ εισόδου απενεργοποιούνται, δηλαδή τα WL στο σχήμα 2.4 είναι ίσα με το μηδέν. Κατά τη διάρκεια της περιόδου αναμονής μπορεί να υπάρξει σημαντική απώλεια ισχύος λόγω των μεγάλων ρευμάτων διαρροής.

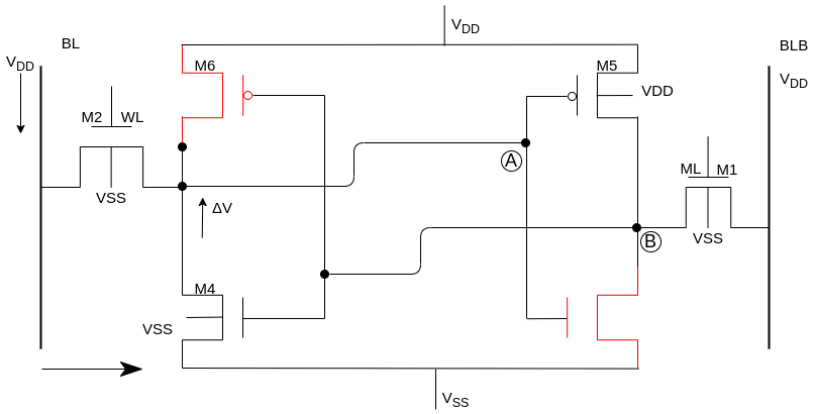

Fig. 2.5 Κατάσταση κελιών κατά την ανάγνωση [73, 74].

Για την αποφυγή υπερβολικών απωλειών ενσωματώνονται ειδικοί αλγόριθμοι καλύτερης διαχείρισης αποκρίσεων και λειτουργείας των κελιών.

2.4.1.1.3 Λειτουργία ανάγνωσης

Στη λειτουργία ανάγνωσης τα τρανζίστορ εισόδου ενεργοποιούνται θέτοντας στις πύλες του WL ίσες με 1. Στο σχήμα παρατηρούμε πως τρανζίστορ, M3 και M6, δεν είναι ενεργά ενώ τα M4 και M5 είναι, αντισταθμίζοντας έτσι ο ρεύμα διαρροής των M3 και M6. Υπό αυτές τις συνθήκες το ρεύμα διαρρέει προς τον κόμβο χαμηλής αποθήκευσης του κελιού, δημιουργώντας έτσι πτώση τάσης σε αυτή τη γραμμή μπιτ ανάλογα με την αντίσταση του τρανζίστορ φορτίου που ανιχνεύεται. Κατά τη διάρκεια της λειτουργίας ανάγνωσης η χαμηλή τάση αποθήκευσης δεν πρέπει να αυξηθεί πάνω από το σημείο ανοχής (trip point) του άλλου μετατροπέα. Τα τρανζίστορ συμπεριφέρονται σαν αντίσταση και τα M2 και M4 σχηματίζουν διαιρέτη τάσης και αυξάνουν την τάση κόμβου A από ΔV. Για να διασφαλιστεί η ορθή λειτουργία της ανάγνωσης, η τάση στην είσοδο του μετατροπέα που έχει έξοδο υψηλή πάνω από την οποία ο μετατροπέας αλλάζει την κατάστασή του το ΔV επιλέγεται έτσι ώστε να μην ενεργοποιεί τον μετατροπέα M5-M3 και ο κόμβος B παραμένει σε VDD καθ'όλη τη διάρκεια επεξεργασίας του κελιού [74].

Στην κατάσταση ανάγνωσης οι γραμμές μπιτ είναι προ-φορτισμένες και η γραμμή λέξης απενεργοποιημένη, και όταν ενεργοποιηθεί η γραμμής λέξης, οι δύο αντιστροφείς παρέχουν ανατροφοδότηση ο ένας στον άλλο, έως ότου οι δύο γραμμές μπιτ (BL και BLB) διαβάσουν την εσωτερική τιμή του κελιού – παράλληλα οι εσωτερικοί κόμβοι έχουν συμπληρωματικές τιμές με βάση τις φυσικές παραμέτρους των αντίστοιχων αντιστροφών. Τελικά, η γραμμή μπιτ που αντιστοιχεί στον απενεργοποιημένο κόμβο, εκφορτίζεται, ενώ η άλλη γραμμή μπιτ θα διατηρήσει την τιμή τάσης μονοπατιού

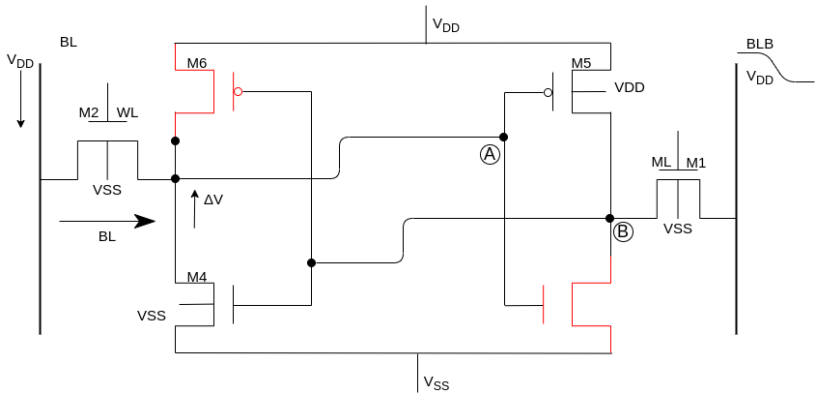

Fig. 2.6 Κατάσταση κελιών κατά την καταγραφή [73, 74].

εκφόρτωσης, και η γραμμή λέξης φορτίζεται, ωστόσο δύο γραμμές προσπαθούν να εκφορτιστούν.

2.4.1.1.4 Λειτουργία καταγραφής

Σε λειτουργία εγγραφής τα τρανζίστορ εισόδου ενεργοποιούνται με την κατάσταση της γραμμής εισόδου WL ίση με VDD, έχοντας τον κόμβο A και B σε κατάσταση VSS και VDD, αντίστοιχα. Η λειτουργία της εγγραφής ολοκληρώνεται μόνο εάν το επίπεδο τάσης στον κόμβο A και B γίνει VDD και VSS, αντίστοιχα. Εάν ο κόμβος αποθήκευσης αποθηκεύει αρχικά VSS και τα δεδομένα στη γραμμή μπιτ είναι VSS, τότε δεν υπάρχει καμία αλλαγή στην κατάσταση του κελιού. Από την άλλη πλευρά, όταν ο κόμβος αποθήκευσης αποθηκεύει αρχικά το VDD και τα δεδομένα στη γραμμή μπιτ είναι VDD, τότε και πάλι δεν υπάρχει καμία αλλαγή στην κατάσταση του κελιού.

Για την εγγραφή (σχήμα 2.6), αρχικά το κελί απομονώνεται από τις γραμμές μπιτ με την απενεργοποίηση της γραμμής λέξης, δηλαδή μηδενίζεται. Οι τιμές που φορτώνονται στα κελιά SRAM των ενεργών γραμμών θα καθορίσουν ποια τρανζίστορ θα χρησιμοποιηθούν τελικά για την αποφόρτιση των γραμμών μπιτ κατά την αξιολόγηση της απόκρισης. Η τιμή του άσσου ορίζεται στο κελί μόνο όταν φορτίσει αρχικά την τη γραμμή bitline, άρα γραμμή bitline (Bit-Line Bar – BLB) αποφορτίζεται. Μόλις ενεργοποιηθεί η γραμμή λέξης, τότε η γραμμή bitline γράφεται μέσα στο κελί. Να σημειωθεί επίσης πως η τιμή ενεργοποίησης του κελιού, μπορεί να χρησιμοποιηθεί και ως τιμή ανάγνωσης μπιτ κελιών, χωρίς προηγούμενη εγγραφή – αξιοσημείωτη παρατήρηση είναι πως αυτή η τιμή ενεργοποίησης είναι μοναδική για τις επιμέρους ασταθείς και συμμετρικούς αντιστροφής, κατά την εκκίνηση χωρίς να έχει αποθηκευτεί κάποια τιμή σε αυτό. Από τεχνικής απόψεως όψη, οι δύο αντιστροφείς δεν είναι ακριβώς ίδιοι και έχουν

διαφορετικές φυσικές παραμέτρους, δηλαδή μήκος και πλάτος, λόγω των μεταβολών της διαδικασίας κατασκευής.

2.4.1.2 Εκκίνηση μνήμης SRAM

Σε μη τροπωμένες SRAM η συμπεριφορά εκκίνησης παίζει πολύ σημαντικό ρόλο για την δημιουργία και ανάλυση μίας PUF συνάρτησης. Κατά την εκκίνηση της SRAM τα κελιά ξεκινάνε ανεξάρτητα κάθε φόρα, ανάλογα τον (σταυροειδώς συνδεδεμένου) αντιστροφέα με τις περισσότερες τιμές [16]. Οι τιμές εκκίνησης των κελιών, γνωστές και ως (Start-up Values – SUV) είναι ευάλωτες σε διαφορετικούς παράγοντες που επηρεάζουν τις τιμές αυτές. Οι λειτουργίες των κελιών SRAM με την ακολουθία εκτέλεσής τους είναι η αναμονή, ανάγνωση και καταγραφή. Επιπλέον, αναταραχή κατά την εκκίνηση της μνήμης μπορεί να γίνει λόγου της ανακατανεμημένης διάταξης της εσωτερικής στοίβας, όταν έχει τεθεί σε λειτουργίας. Ειδικότερα, καθυστερήσεις εγγραφής και ανάγνωσης, είναι παράγοντες θορύβου, που μπορούν να μετρηθούν με την τιμή του περιθώριο στατικού θορύβου (Static noise margin – SNM). Ένα από τα σημαντικότερα προβλήματα των SRAM είναι οι διακυμάνσεις της συχνότητας αποκρίσεων εκκίνησης λόγο των περιβαλλοντικών συνθηκών, και η αστάθεια αυτή θεωρείται μειονέκτημα, καθώς οδηγεί σε σκίασμα του κελιού, δηλαδή σε στατιστική συμπεριφορά εξόδου (μηδέν ή ένα) κάθε κελιού.

Η συμπεριφορά των κελιών κατά την εκκίνηση ταξινομούνται σε τρεις κλάσεις. Πρώτον, χαρακτηρίζεται εν μέρη ακρίβεια των κελιών(partialy-skewed), για τα οποία παρουσιάζεται μικρή αναντιστοιχία μεταξύ δύο αντιστροφών, για παράδειγμα μερικές διευθύνσεις είναι ασταθές για υπό διαφορετικές περιβαλλοντικές συνθήκες. Δεύτερον, με την ίδια λογική η επόμενη κλάση είναι γνωστή ως, μισή αναταραχή (semi-skewed), άρα τα μισά κελία ενδέχονται να αντιμετωπίσουν σχετικά προβλήματα. Τέλος, πλήρες αστάθεια των κελιών (fully-skewed) παρατηρείται όταν τα περισσότερα κελιά να αντιμετωπίσουν αναταραχές τροφοδοσίας, ανεξάρτητα από τις περιβαλλοντικές μεταβολές. Τα παραπάνω φαινόμενα εμφανίζονται σε διαφορετικούς τύπους αστοχίας λειτουργιών της SRAM, και απεικονίζονται συνοπτικά στο σχήμα 2.7. Αρχικά, στην διαταραχή λειτουργίας ανάγνωσης παρατηρείται αύξηση στην γραμμή λέξης τέτοια ώστε το τρανζίστορ pull-down (δίκτυο αλληλουχίας με γείωση) της απέναντι πλευράς ενεργοποείται, και η περίοδος διαταραχής ανάγνωσης μπορεί να εμφανιστεί κατά τη διάρκεια ενός κύκλου εγγραφής – πολλά κελιά στην γραμμή λέξης ενδέχονται να φορτιστούν και αυτά, δημιουργώντας έτσι μια κίνηση αχρησιμοποίητων μπιτ, τα οποία έπρεπε να οδηγούν για εγγραφή. Όταν το ρεύμα ανάγνωσης του κελιού δεν επαρκεί

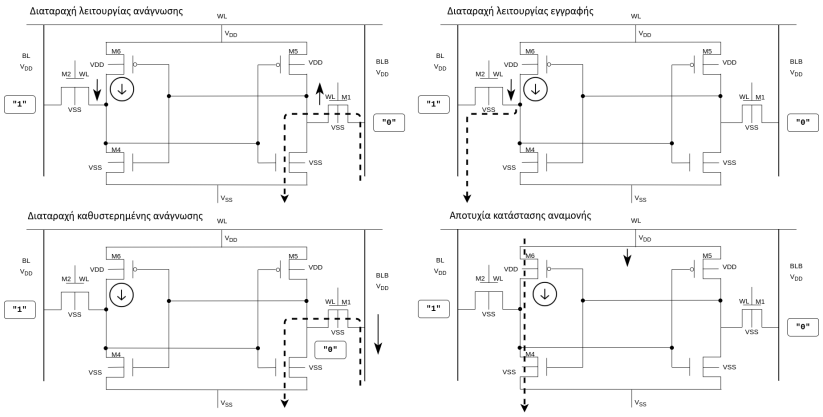

Fig. 2.7 Συνολικά όλες οι περιπτώσεις σφάματος SRAM 6T [2].

για να ικανοποιήσει τις απαιτήσεις χρονισμού του σχεδιασμού, τότε μια γραμμή είναι κατειλημμένη, καθώς η αποτυχία δεν μπορεί πάντα να διαγνωστεί σε διακυμάνσεις εντός του κελιού της επίπεδης μεμονωμένης στήλης, και επίσης ο μετρητής γραμμής μπιτ του ενισχυτή ενδεχομένως να επηρεαστεί, προκαλώντας μετατόπιση αναφερόμενη διεύθυνσης στην είσοδο – αυτό το φαινόμενο ονομάζεται αποτυχία καθυστέρησης ανάγνωσης. Επιπρόσθετα, διαταραχές στην λειτουργία εγγραφής, προκύπτουν το κελί δεν καθαρίζει (διατηρεί την προηγούμενη τιμή των αντιστροφών) κατά της αναμενόμενης συμπεριφοράς, πριν την επιβεβαίωση της γραμμής λέξης. Επίσης, η διαταραχή καθυστέρησης, συμβαίνει όταν ένα κελί χάνει την αποθηκευμένη τιμή του, λόγο αδράνειας για κάποιο συγκεκριμένο χρονικό διάστημα – το φαινόμενο αυτό εμφανίζεται συνήθως λόγο της μείωσης τάσης τροφοδοσίας του κελιού ή η επιρροή θορύβου στους εσωτερικούς κόμβους αποθήκευσης. Όλες αυτές οι κατηγορίες σφαλμάτων επηρεάζουν τις δύο περιπτώσεις αποτυχίας στην δομή των γραμμών λέξεων – συνήθως δεν είναι ούτε ανιχνεύσιμες ούτε διορθώσιμες με κώδικες διόρθωσης σφαλμάτων. Πρώτα από όλα, οι διαταραχές στο μονοπάτι των δεδομένων προκαλεί αδράνεια στα δεδομένα μιας ή περισσότερων στηλών. Αντίστοιχα, η δεύτερη κατηγορία σχετίζεται με τις διαταραχές στο μονοπάτι διευθύνσεων, όπου στις προβληματικές γραμμές λέξεων τα δεδομένα είναι ανεστραμμένα σε σχέση με εκείνα της προοριζόμενης γραμμής λέξης, προκαλώντας αποτυχία ανάγνωση ολόκληρης της λέξης.

2.4.1.3 Καθορισμένη κατάσταση και επαναφορά μνήμης

Όπως καταλαβαίνουμε, οι SRAM έχουν την δυνατότητα να παράγουν ένα μόνο ζεύγος πρόκληση-απόκριση, όπου η απόκριση είναι μια δυαδική ακολουθία. Η προέλευση της απόκρισης είναι είτε οι τιμές εκκίνησης (δες 2.4.1.2), είτε μη αρχικοποιημένες

τιμές της μνήμης – πρώτη εφαρμογή τους στην βιβλιογραφία ήταν η ψηφιακή αυθεντικοποίηση, και ταυτόχρονα ξεχωριστή εφαρμογή για παραγωγή κλειδιών [75, 60]. Η αρχιτεκτονική της SRAM αποτελείται από κελιά (δες 2.4.1.1.1), όπου για κάθε απόκριση ένα κελί αντιπροσωπεύει ένα δυαδικό ψηφίο και σχηματίζεται από δύο παράλληλους συνδεδεμένους αντιστροφείς, και στους αντιστροφείς η είσοδος, αντιστρέφεται μετατρέποντας το ένα σε μηδέν, αντίστροφα. Επομένως, το κελί SRAM μπορεί να υιοθετήσει μόνο κατάσταση και να αποθηκευτεί χάρις τους διασταυρωμένους αντιστροφείς κατά την εκκίνηση, δηλαδή (0, 1) που αντιστοιχεί στην αποθήκευση της τιμής μηδέν, και αντίστοιχα (1, 0) που αντιστοιχεί στην αποθήκευση του άσσου. Ωστόσο, όταν το κύκλωμα επαναφέρεται, η μηχανή καταστάσεων ξεκινά στην κατάσταση μηδέν και τυχόν αποθηκευμένες τιμές χάνονται, οπότε ο άλλος αντιστροφέας οδηγεί τώρα την χαμηλής τάσης έξοδο – οι δύο αντιστροφείς μετατρέπονται είναι σε κατάσταση, με άλλα λόγια (0, 1) ή (1, 0). Η δυαδική τιμή που προκύπτει εξαρτάται τόσο από το θόρυβο όσο και από την πιθανή ανισορροπία μεταξύ των δύο αντιστροφών – το εγγενές χαρακτηριστικό της τυχαιότητας οφείλεται ανισορροπία ανεξέλεγκτων διακυμάνσεων μεταξύ των αντιστροφών είναι απρόβλεπτες και είναι διαφορετικές για κάθε τσιπ.

2.4.1.4 Εκτίμηση των επιμέρους ασταθέων κελιών

Ένας εύχρηστος τρόπος εύρεσης ασταθών κελιών είναι με την χρήση γραμμικού μοντέλου αξιολόγησης πιθανότητας ρυθμού καθυστέρησης ως προς την κατάσταση της διεύθυνσης της τιμής. Ειδικότερα, για ένα διάνυσμα απόκρισης S, και δείκτη R υπολογίζεται το άθροισμα για ένα συγκεκριμένο χρονικό διάστημα – στην περιπτωσή μας ακολουθήσαμε την πρόταση παρόμοιου εξοπλισμού, στον οποίο περιορίστικε το διάνυσμα στις δεκαέξι επαναλήψεις [76]. Το ιδανικότερο είναι το κύκλωμα να ακολουθεί ένα γραμμικό χρονικό μοντέλο, αλλά διάφορα είδη θορύβου, όπως ο θόρυβος και περιβαλλοντικές μεταβολές, προκαλούν μη γραμμικότητα του μοντέλου καθυστέρησης.

$$y_i = \frac{1}{|S|} \sum_{s \in S} R_i(s) \tag{2.11}$$

2.5 Ενσωμάτωση των μη-κλωνοποίσημων πηγών σε εφαρμογές

Οι εγγενείς ιδιότητες των μη αντιγράψγμων συναρτήσεων είναι κατάλληλες για ποικίλες εφαρμογές ασφαλείας, μολονότι ορισμένοι τύποι οχημάτων έχουν εγκριθεί με βάση εθνικά πρότυπα, σε κάθε περίπτωση το ζευγάρι απόκρισης πρέπει να είναι και μη αντιγράψημο. Τα βασικότερα είδη εφαρμογών που μπορούν να υλοποιηθούν βασισμένα σε μη αντιγράψιμες συναρτήσεις είναι η δημιουργία μυστικών κλειδιών [77, 61, 78], πρωτόκολλα κρυπτογράφησης [61] και έλεγχος ταυτότητας [79]. Για αδύναμες μη αντιγράψημες πηγές, χρησιμοποιείται καλύτερα ως κορμός κρπυπτογραφικού σπόρου, και ασφαλής τρόπος αποθήκευσης κλειδιών – ο πεπερασμένος αριθμός των αποκρίσεων δίνει το προβάδισμα σε επιτιθέμενους σε μόνο μία αποκάλυψη κλειδιού για την αποκάλυψη των υπολοίπων. Από την άλλη πλευρά, οι απρόβλεπτες αποκρίσεις των ισχυρών μη κλωνοποιήσημων πηγών λύνουν αυτό το πρόβλημα, ωστόσο έχουν δημοσιευτεί τρόποι μετατροπής αδύναμων μη αντιγράψημων πηγών σε ισχυρές [80, 81].

2.5.1 Αυθεντικοποίηση οντότητας

Τα εγγενείς χαρακτηριστικά των μη κλωνοποιήσιμων πηγών τακτοποιούν την συσκευή ως μοναδική, αποδίδοντας έτσι αναγνωριστικά με εικονικό τρόπο σε οντότητες. Άρα, εξαλείφεται η ανάγκη εξωτερικής δημιουργίας αναγνωριστικών, ειδεμή η εσωτερική μνήμη δεν χρειάζεται να αποθηκεύονται κλειδιά ταυτοποίησης. Μολαταύτα, το σύστημα έχει ωφελήσει κυρίως μείωσης κόστους και πολυπλοκότητα, απαιτείται ανεκτικότητα σε θορυβώδη παράγοντες, όπως είναι για παράδειγμα η απότομη αλλαγή θερμοκρασίας.

2.5.2 Δημιουργία μυστικών κλειδιών

Οι τυπικές σταθερές μνήμες μπορούν να παράγουν μια σειρά από μπιτ η οποία μπορεί να χρησιμοποιηθεί ως μυστικό κλειδί [61]. Σε την ροή των μπιτ δημιουργείται θόρυβος [82] , με αποτέλεσμα να γίνει αναγκαία η χρήση βοηθητικών μπιτ για τον ορθό μετασχηματισμού της αρχικής σειράς δεδομένων. Για την διασφάλιση της ποιότητας των διορθωμένων μπιτ [77] προτάθηκε η μέθοδος ασφαλούς σχεδιασμού (secure sketch), η οποία προτάθηκε από τον Dodis το 2004 [42]. Η δημιουργία μυστικών κλειδιών ελλοχεύει πιθανά προβλήματα ακεραιότητας καθώς οι NVM μνήμες είναι ευάλωτες σε διάφορες επιθέσεις οι οποίες έχουν στόχο να αποκαλύψουν δεδομένα της μνήμης.

2.5.3 Πρωτόκολλα κρυπτογράφικών συστημάτων

Οι μη αντιγράψιμες συναρτήσεις δεν περιορίζονται σε ήδη υπάρχοντα πρωτόκολλα ασφάλειας, αλλά υιοθετούν τα παρόντα κρυπτογραφικά πρωτόκολλα και εφαρμογές, όπως είναι η δημιουργία μυστικών κλειδιών [77, 61, 78], κρυπτογραφικοί αλγόριθμοι όπως είναι ο RSA, για τον οποίο είναι εκτεθειμένα τα ιδιωτικά κλειδιά σε μαθηματική σχετικότητα – οπότε οι σύνθετες και πολύπλοκες ανάγκες ενός σύγχρονου ασυμμετρικού αλγορίθμου κρυπτογράφησης είναι ευνοημένοι με μη κλωνοποίησημες πηγές για την υποστήριξη της ψηφιακής υπογραφής.

Κεφάλαιο 3

Ανάλυση

"*The people being commonly very rude builders, especially inthis speculative way, and more especially still, when actuatedby party-zeal; it is natural to imagine, that their workmanshipmust be a little unshapely, and discover evident marks of thatviolence and hurry, in which it was raised.*"

David Hume, *Essays, moral, political, and literary.*

Σε αυτό το κεφάλαιο, γίνεται αναφορά στο μοντέλο δημιουργίας κλειδιών με χρήση ως μη κλωνοποίησημης πηγής μνήμη τύπου SRAM, τα αποτελέσματα συγκρίνονται με άλλα ερευνητικά έργα στα οποία πραγματοποιήθηκαν παρόμοια πειράματα – δυστυχώς πολλοί συγγραφείς δεν μερολήπτησαν να προσκομίσουν κάποιες μετρήσεις. Μάλιστα, τα αποτελέσματα τους έργου αυτού όχι μόνο διαφέρουν, άλλα είναι καλύτερα σε σχέση με όλες τις συγκεκριμένες δουλειές.

3.0.1 Ιδιότητες και μέτρα αξιολόγησης

Οι μη κλωνομοιήσημες πηγές, εκτός από μια τεράστια γκάμα τρόπων υλοποιήσεων, έχουν προταθεί ορολογίες τυποποίησης για την περιγραφή ιδιοτήτων, μετρήσεων

αποδοτικότητας, ώστε να θεωρηθεί ως πυρήνας εμπιστευτικότητας. Επιπρόσθετα, έχουν δοκιμαστεί διάφοροι τρόποι προσδιορισμού της ποιότητας μίας πηγή, ή και μεθοδολογίας επιτέλεσή τους. Επιπροσθέτως, η ανθεκτικότητα κάθε μη-αντιγράψιμης πηγής, εξαρτάται από συγκεκριμένες ιδιότητες, οι οποίες εν μέρει συνοψίζουν στοιχεία ασφαλείας [83], είτε τρόπους πιστοποίησης κρυπτογραφικών εφαρμογών που παρέχονται από ινστιτούτα και οργανισμούς, όπως είναι για παράδειγμα ο οργανισμός NIST, προκειμένου να επιτραπεί η χρήση τους σε εργασιακό ή παραγωγικό περιβάλλον [84]. Ειδικότερα, ο Maes et al. [54] διατύπωσε και απέδειξε, βασικές ιδιότητες, στις οποίες διαχώρισε σε δύο βασικές κατηγορίες, ανθεκτικές και μη-ανθεκτικές πηγές(strong και weak PUF) [85], ακριβέστερα διακρίθηκαν τα εγγενείς μέσα ανάλογα με το όριο(δυνατότητα) παραγωγής ξεχωριστών μη-κλωνοποιήσιμων τιμών - κατά συνέπεια οι μη-ανθεκτικές πηγές ξεχωρίζουν γιατί το διάνυσμα ζευγαριών είναι περιορισμένο με γραμμική ή πολυώνυμή αύξηση, και σε κάποιες περιπτώσεις κάποιες συσκευές παράγετε μονάχα ένα ζευγάρι τιμών. Έπειτα, κάποια άλλα ποιοτικά χαρακτηριστικά προτάθηκαν, αρχικά καθορίστηκαν από τον Majzoobi τέσσερα κριτήρια [86], τα οποία ορίζουν ένα κατώφλι ανθεκτικότητας σε ευρείες κατηγορίες επιθέσεων - αντίστοιχα οι δοκιμές ήταν η προβλεψιμότητα, αποκωδικοποίηση κώδικα, σύγκρουση, και ευαισθησία. Στην συνέχεια ο Hori [87], πρότειναν σε συνδυασμό με την θεωρία στατικών δοκιμών προσδιορισμού τυχαιότητας και εντροπίας, μέτρο τυχαιότητας αφοσιωμένο για μη-κλωνοποίησημες συναρτήσεις, σταθερότητα, ορθότητα, σταθερότητα, μοναδικότητα, και διάχυση της σειράς, έτσι αντίστοιχα ο Maiti [88], εισήγαγε δείκτες περιβαλλοντικών παραγόντων, δηλαδή ομοιομορφία, μοναδικότητα, αξιοπιστία, και τάση σειράς. Τέλος, ο Danger αντίστοιχα μεταλαμπάδευσε τους προβληματισμούς του για τη μελλοντική τυποποίηση των χαρακτηριστικών παραμέτρων ασφαλείας [89], για τις οποίες οι Habib et al, Su et al και Yamamoto et al, επένδυσαν στην προσαρμογή τους σε ειδικές συσκευές [90–92] που στην συνέχεια δημιουργήθηκε αντίστοιχο πρότυπο [93], και μετά ο Kim διατυπώνοντας τις παραπάνω μετρήσεις σε προσεγμένη λεπτομέρεια, ομαδοποιήθηκαν κατάλληλες μετρήσεις για κάθε φυσικό μέσο [94]. Στις παρακάτω υπο-ενότητες αναγράφονται κατάλογοι ιδιοτήτων μη-κλωνοποίσημων πηγών, καθώς και οι ιδανικές συνθήκες.

3.0.2 Ακεραιότητα

Το κυριότερο χαρακτηριστικό μιας μη κλωνοποίσημης πηγής είναι η ακεραιότητα(γνωστό στην βιβλιογραφία ως uniqueness ή inter-chip Hamming Distance), καθώς η αυθεντικοποίηση από ένα ζευγάρι παραγμένο από μια πηγή, πρέπει σε κάθε περίπτωση να

είναι μοναδική, εάν και μόνο, δεν μπορεί να βρεθεί ομοιότητα μεταξύ των συστατικών που την απαρτίζουν [95]. Ωστόσο, ο συγκεκριμένος τρόπος ανάκτησης, έχει την ιδιαιτερότητα πως, κάθε κύκλωμα παραγωγής μη κλωνοποίσημου συστήματος, εξαρτάται από εξωτερικούς και εσωτερικούς παράγοντες, του φυσικού επιπέδου. Με άλλα λόγια, μια PUF χαρακτηρίζεται ως μοναδική, εάν η σειρά των μπιτ είναι τελείως διαφορετική με μια άλλη [95, 96], η οποία όπως θα δούμε στην συνεχεία, είτε θα είναι από διαφορετικό ολοκληρωμένο κύκλωμα, είτε από το ίδιο, αλλά με δύο ή παραπάνω αυθαίρετα επιλεγμένες συσκευές - διαφορετικές μεταξύ τους (στην περίπτωσή μας, τσιπ μνήμης). Παράλληλα, οι παράμετροι σύγκρισης για την ικανοποίηση της πρότασης είναι πως η πιθανότητα μοναδικότητας κάθε ζευγαριού στο ίδιο κύκλωμα (αλλά με ίδιες θέσεις μνήμης), να είναι μεταξύ τους ανόμοιες, δηλαδή αυτό σημαίνει ότι η απόσταση Χάμινγκ στην ιδανική περίπτωση είναι ίση με 50% (τομή των δύο συνόλων μπιτ), πράγμα που σημαίνει ότι, οι μισές απαντήσεις που παράγονται από δύο PUF πρέπει να είναι διαφορετικές μεταξύ τους. Ως επί των πλείστων, μια ομάδα φυσικών μέσων $N_{devices}$ παράγονται ίδιου μήκους σειρές r_i και r_j, από τις θέσεις τιμών i, και j αντίστοιχα [97].

$$Uniqueness = \frac{2}{N_c(N_c-1)} \sum_{i=1}^{N_c-1} \sum_{j=i+1}^{N_c} r_i \bigoplus r_j \times 100\% \tag{3.1}$$

3.0.3 Μη-προβλεψιμότητα

Ένα κριτήριο ζωτικού ρόλου σε μη κλωνοποιήσιμα συστήματα, είναι η δυνατότητα αποκάλυψης κάποιου μυστικού, ακόμη σε και σε περίπτωση που αποκαλυφθεί κάποιο κομμάτι του κλειδιού ή κάποιας άλλης πληροφορίας, σε σύγκρισή με κάποιο εύλογο διάστημα, το οποίο κάποιος επιτιθέμενος έχει στην διάθεσή του. Σε διάφορα μοντέλα ασφαλείας, στα οποία εφαρμόζονται, αυθεντικοποίηση και κρυπτογράφηση, σημαντικό στοιχείο είναι η ακεραιότητας της τυχαιότητας, η οποία όπως είδαμε παραπάνω, εξαρτάται από την ελάχιστη εντροπία (δες 2.3).

Για την ερμηνεία αυτού του διχασμένου ορισμού, πρέπει να επιθεωρηθούν πρώτα, το βάρος Χάμινγκ σε συνδυασμό με την στατιστική σχετικότητα, επικυρώνοντας τα αποτελέσματα με τις στατιστικές δοκιμές και θεωρητική κριτική ανάλυση τυχαιότητας, όπως είναι οργανισμός NIST (FIPS 140 [84] και SP 800-22 B [7]) και AIS.31 της BSI [98]. Από αυτό σημπεραίνουμε ότι, κάθε σειρά τιμών αποτελείται αμερόληπτα από ισορροπημένη και τυχαία ταυτόχρονα, χωρίς βέβαια να παρατηρηθεί κάποιο

επαναλαμβανόμενο αλγοριθμικό μοτίβο. Πρέπει να έχουμε κατά νου ότι ο παραπάνω κανόνας, είναι πρακτικά δύσκολο να τηρηθεί σε κάθε στιγμιότυπο ιδανική τυχαιότητα, γιατί δεν επαρκεί να αποδειχθεί ότι η εφαρμογή ή συσκευή ανάλογα, είναι καλή για χρήση στον πραγματικό κόσμο.

3.0.4 Σχετικότητα

Εγγενή χαρακτηριστικό των μη-κλωνοποίσημων πηγών, είναι η ανομοιογένεια του ίδιου κυκλώματος, λόγο της παρασκευής – κατά την αναπαράσταση των μπιτοσερών από τα αντίστοιχα κελία του αντιστροφέα. Οι τεχνικές συσχέτισης είναι αναμφισβήτητα μια από τις πιο συχνά χρησιμοποιούμενες στατιστικές διαδικασίες για την διερεύνηση ποιοτικών χαρακτηριστικών μιας πηγής τυχαιότητας. Ένας από τους γνωστότερους αλγορίθμους συσχέτισης είναι του Pearson, στον οποίο ανοιχνεύεται συνδιακύμανση των δύο μεταβλητών που κανονικοποιούνται, πολλαπλασιάζοντας τις τυπικές αποκλείσεις τιμών i και j [99].

$$Correlation = \frac{cov(i,j)}{SD_i \times SD_j} \tag{3.2}$$

3.0.5 Αξιοπιστία

Με το όρο αξιοπιστία (ή αλλιώς reliability ή μέτρο intra-chip Hamming Distance), αναφερόμαστε στο μέτρο αξιολόγησης του κυκλώματος ως προς την σταθερότητα απόκρισης των δεδομένων, είτε για μικρό ή μεγάλο χρονικό διάστημα - έτσι ποσοτικοποιείται η ανθεκτικότητα της συσκευής έναντι του φαινομένου γήρανσης του εξοπλισμού ή άλλων παρεμβολών [100]. Τώρα, σε περίπτωση που αποτύχει η σταθερή παραγωγή τιμών, τότε το κύκλωμα θεωρείται αναξιόπιστο και απαιτείτε διόρθωση σφαλμάτων. Η αποσκοπούσα περίπτωση είναι όταν ο θόρυβος είναι ανύπαρκτος, άρα ο λόγος δεδομένων προς σφάλμα είναι ίσος με μηδέν - αντίστοιχα όσο πιο κοντά στο 100% βρίσκεται η αξιοπιστία, τόσο το καλύτερο [97].

$$Reliability = [100 - \frac{2}{N_{cktcrp}(N_{cktcrp}-1)} \sum_{i=1}^{N_{cktcrp}-1} \sum_{ji=i+1}^{N_{cktcrp}} r_i \bigoplus r_j i] \times 100\% \tag{3.3}$$

Όπου $cktcrp$ μετριέται η απόκριση σειράς μπιτ σε κάποια συσκευή. Να σημειωθεί ότι, ο παραπάνω ορισμός είναι ισοδύναμος με την διαφορετική του συνόλου με BER

$$BER = \frac{1}{\binom{crp}{2}} \sum_{i=1}^{crp-1} \sum_{j=i+1}^{crp} \frac{HD(r_i, r_j)}{V} \times 100\% \tag{3.4}$$

Απότοκο αυτού είναι, το ποσοστού θορύβου σε μη-κλωνοποίσημες πηγές ορίζεται ως HD προβλέπεται η απόσταση Χάμινγκ (Hamming Distance) , V το μέγεθος της σειράς, crp σύνολο δειγματοληψίας.

3.0.6 Ομοιομορφία

Μια άλλη στατιστική μέτρηση απόδοσης είναι η ομοιομορφία, γνωστή και ως uniformity, στην οποία αντιπροσωπεύεται η ικανότητα δημιουργίας ισορροπημένης απόκρισης σειράς, σαφέστερα διακρίνεται η αναλογία 0 και 1 σε ολόκληρο το σύνολο τιμών - αβίαστα, λοιπόν, συνάγεται το συμπέρασμα πως όσο πιο κοντά στο 50% βρίσκεται το αποτέλεσμα της απόστασης Χάμινγκ κάθε θέσης μπιτ μιας τιμής σε σχέση με την συσκευή της, είναι το ιδανικότερο. Γιατί με χαμηλή ομοιομορφία ελλοχεύει η αύξηση της πιθανότητας μείωσης χώρου συνδυασμών από εισβολείς. Πιο συγκεκριμένα, μεροληπτείτε ο υπολογισμός της απόστασης Χάμινγκ για ένα σύνολο τιμών $crps$ για κάθε δείγμα c.

$$Uniformity = \frac{1}{crps} \sum_{c=1}^{crps} r_c \times 100\% \tag{3.5}$$

Σκόπιμο είναι να αναφερθεί πως μπορεί να αξιολογηθεί μέσα από την στατιστική σουίτα NIST [7], όπως θα δούμε και παρακάτω. Επιπλέον, μια γνωστή λύση στην ισοβάθμηση της ομοιομορφίας, γίνεται με τον μετατροπέα Von Neumann [101], για τον οποίο έχει αποδειχθεί πως έχει αποτέλεσμα καλύτερες διακυμάνσεις ισοβάθμησης μίας θορυβώδεις πηγής [102, 103].

3.0.7 Τάση σειράς

Η συλλογή των τιμών εκκίνησης μίας μνήμης, μετά από κάποιο εύλογο χρονικό διάστημα, λόγω του θορύβου στα κελιά, ενδέχεται κάποιες προσκομήσουσες σειρές μπιτοσειρών να τηρούν κάποιους στατιστικούς κανόνες - ανάλογα με περιβάλλον που λαμβάνει χώρα η δειγματοληψία, και προτιμήσεις σε διευθύνσεις(τάση τιμής 0 ή 1 αντίστοιχα). Γι' αυτό τον λόγο, η μέτρηση της απόστασης Χάμινγκ των μπιτ απόκρισης δείγματος $crps$, το οποίο αποτελείται από c αντίστοιχες τιμές. Η τιμή που είναι ιδανική, είναι η κοντινότερη στο 50% [102].

$$Bit - aliasing = \frac{1}{N_c} \sum_{c=1}^{crps} r_{crp,c} \times 100\% \tag{3.6}$$

Οπότε, η εκτίμηση διάκρισης μέλλων μιας σειράς, $Bit - Bias$, είναι η άθροιση του βάρους Χάμινγκ του κάθε ζευγαριού απόκρισης, ως προς μήκος των αξιολογούμενων μπιτ. Με την ίδια λογική, το ποσοστό ευαισθησίας μεταβλητότητας των μπιτ, $Bit-Flips$, είναι ο έλεγχος τιμών δειγματοληψίας από μια αρχική κατάσταση σε συνδυασμό με αποτελέσματα περαμάτων υπό διαφορετικές περιβαλλοντικές συνθήκες.

Ειδικότερα, κατευθυντήριο κριτήριο είναι r_c, και από την άλλη πλευρά, r'_c αντιπροσωπεύεται η συσσώρευση δειγμάτων ανόμοιων βιότοπων [102].

$$Bit - Flips = HW[\frac{1}{N_c} \sum_{i=1}^{N_c} \frac{HD(r_c, r'_c)}{N_c}] \times 100\% \tag{3.7}$$

3.1 Ανάλυση τρόπων διεύρυνσης της έρευνας

Πρώτού ξεκινήσει η ανάλυση, σκόπιμο είναι η αναφορά προηγούμενων υλοποιήσεων της βιβλιογραφίας, και έπειτα η περιγραφή της μεθοδολογίας που τηρήθηκε.

3.1.1 Σχετική έρευνα και υλοποίησεις μη-αντιγράψιμων πηγών SRAM

Οι συσκευές SRAM εκτός ότι μπορούν να χρησιμοποιηθούν ως μη κλωνοποίσημες πηγές, υπάρχουν πολλά πρακτικά προβλήματα, τα οποία αντιμετωπίστηκαν σε διάφορα ερευνητές εργασίες. Αρχικά, για την επίλυση του θορύβου στα δεδομένα απόκρισης μιας SRAM, μελετήθηκαν αλγόριθμοι βοηθητικών δεδομένων (δες 2.3.4) εξαγωγής κλειδιών [62]. Ωστόσο, η πρόταση ήταν βασισμένη σε κώδικες ασφαλούς σχεδίου σε εξειδικευμένες συσκευές FPGA – η διαδικασία της ανακατασκευής του κλειδιού συγκεκριμένης απόκρισης, η οποία εκχωρήθηκε ως τελικό μπλοκ δημιουργίας κρυπτογραφικών κλειδιών. Έπειτα, οι αλγόριθμοι βοηθητικών δεδομένων χρησιμοποίησαν για αμοιβαίο έλεγχο ταυτότητας, σε μια σχεδίαση στην οποία η επιλογή του κώδικα διόρθωσης σφαλμάτων μείωσε τον πληθυσμό των διαθέσιμων κυττάρων της SRAM – στόχος του σχήματος ήταν η μείωση του αριθμού των αναξιόπιστων μπιτ σε σχέση με την εξάρτηση πολυπλοκότητας του αλγορίθμων διόρθωσης σφαλμάτων [17]. Στη συνέχεια, μια νέα διερεύνηση έγινε στην προ-επεξεργασίας ταξινόμησης ζευγαριών σε συστάδες αξιόπιστων κελιών της SRAM με βάση την αναντιστοιχία τάσης κατωφλίου μεταξύ των συνδεδεμένων τρανζίστορ, με βάσι κατώφλι απόρριψης υποψηφίων κελιών – τα μειονεκτήματα αυτής της τεχνικής ήταν το υπολογιστικό κόστος και επιβάρυνση τοπικής περιοχής της τεχνικής κωδικοποιητή γραμμής λέξεων [18]. Ένας καινοτόμος αλγόριθμος ήταν ο MECCA (MEmory Cell Characterization based Authentication), ο οποίος με χρήση της διαφορετικής διάρκειας του παλμού της γραμμής λέξης για τη δημιουργία μοναδικών υπογραφών, παραλείποντας τη χρήση της διάρκειας παλμού ως κρίσιμης παραμέτρου στην αξιολόγηση του μυστικού κλειδιού, συνδέοντας ένα προγραμματιζόμενο μπλοκ καθυστέρησης με τον αποκωδικοποιητή σειράς για τον έλεγχο της διάρκειας του παλμού – έτσι η ευαισθησία στις περιβαλλοντικές συνθήκες και η επιβάρυνση της επιφάνειας μπορεί να είναι δύο περιοριστικοί παράγοντες για αυτή την τεχνική [104]. Αργότερα, μια νέα προσέγγιση δημιουργίας μυστικού κλειδιού ή και αναγνωριστικού, η μέθοδος της εξαγωγής μοναδικού δακτυλικού ακέριάς αντιπροσωπίας (Memory Built-In Self-Test) εκμεταλλεύτηκε τυχαία μπιτ που δεν ανταποκρινόντουσαν στην δοκιμή αυτής της στρατηγικής. Η συλλογή αυτών των μπιτ που δεν ανταποκρίνονται στο τεστ, είναι στην πραγματικότητα σταθερές τιμές κατωφλίου κελιών σε συγκεκριμένο φάσμα, οπότε η μέθοδος προκαλεί αυτό το φαινόμενο – κύριο μειονέκτημα αυτής της τεχνικής είναι ο χρόνος μετατροπής που απαιτείται για τη δημιουργία ασφαλούς αναγνωριστικού, και η πιθανότητα γήρανσης του εξοπλισμού έχοντας σαν αποτέλεσμα αλλαγής της συστάδας [105]. Μια άλλη καινούρια μέθοδος

αυθεντικοποίησης αναγνωριστικού πυριτίου, διατηρώντας την πληροφορία στα κελιά με κατάλληλη σύγκριση τροφοδοσίας της SRAM – η μόνη ανησυχία πρακτικότητας είναι η χρόνο-καθυστέρηση [106]. Ακόμα, λόγω της επίδρασης των διακυμάνσεων διεργασιών αυξάνεται με τη μείωση των μεγεθών των τρανζίστορ – παρατηρείται καθυστέρηση, επηρεάζοντας την απόδοση. Έτσι, τεχνικές αξιοποίησης των αυξανόμενων παραλλαγών διεργασίας όπως είναι ο αλγόριθμος διαχρονικού πλειοψηφικής εκλογής, στον οποίο χωρίζονται τα σταθερά κελία υπό κάποιες συνθήκες [107]. Τέλος τα πιο πρόσφατα σχήματα έρχονται να αντιμέτωπα με τις υπολογιστικές δυνάμεις των κβαντικών συστημάτων, και εξωτικές αντιλήψεις αυστηρών περιορισμών, όπως είναι για παράδειγμα ιατρικά δεδομένα [108, 109].

3.1.2 Διαδικασία αρχικοποίησης μη-αντιγράψιμης πηγής

Η αξιολόγηση της επίδρασης διαφόρων περιβαλλοντικών παραγόντων σε μια SRAM ή επίδειξη της σημασίας σταθερότητας σε κάθε απόκριση. Η στρατηγική που ακολουθήσε για την παρούσα έρευνα, είναι η ακόλουθη. Πρώτα από όλα, η συλλογή δειγμάτων βασίστηκε στα εγγενή χαρακτηριστικά χωρίς επεξεργασία πριν ή μετά τον ορισμό των ζευγαριών τιμών. Ύστερα, για την αντιμετώπισή του θορύβου, επιλεκτικέ ένας από τους πιο διαδεδομένους τρόπους διόρθωσης σφαλμάτων, BCH, σε συνδυασμό την ανάκτηση της ασαφούς επιλογής. Τα αποτελέσματα της δειγματοληψίας αναμένονται να είναι τυχαία, δεδομένου ότι το μοτίβο εκκίνησης είναι τυχαίο, καθώς η πρόβλεψη των κεκλιμένων κελιών είναι δύσκολη, όπως και το κύκλωμα ακολουθεί τυχαία συμπεριφορά. Οι περιβαλλοντικές μεταβολές μπορούν επίσης να οδηγήσουν σε διαταραχές των χρονισμών της τάσης εκκίνησης SRAM, και προσομοίωση αυτού του φαινομένου μπορεί να γίνει με ανάλυση εργαλείων του Monte Carlo [110]. Σχετικές μετρήσεις σε μη κλωνοποίησημες πηγές SRAM αποδεικνύουν πως το μοτίβο της ακολουθίας εκκίνησης είναι τυχαίο, ακόμη και αν η μέση τιμή διακύμανσης είναι ίδια, ταυτόχρονα και η μοτίβο διακύμανσης εξόδου είναι εντελώς τυχαίο [111].

Όταν οι εφαρμογές μη-αντιγράψιμων πηγών απαιτούν αναπαραγωγικές απαντήσεις με τις ίδιες προκλήσεις, η αποθήκευση CRPS είναι μια άμεση, υψηλής κόστους και μη ασφαλής μέθοδος αποθήκευσης. Εάν λάβουμε υπόψη το χαρακτηριστικό αστάθεια, το οποίο χρειάζεται ένα ισχυρό ECC για μετα-επεξεργασία, η όλη λύση γίνεται περισσότερο χρονοβόρα και η σπατάλη μνήμης. Σε αυτή την ενότητα, παρέχουμε μια απλή αλλά πρακτική δομή δεδομένων για να καταγράψουμε τα χρήσιμα χαρακτηριστικά του PUFS,

η οποία θεωρείται ως ένα θεμελιώδες στοιχείο της βελτίωσης της αποτελεσματικότητας επιλογής μπιτ και της σταθερότητας PUF.

Algorithm 1: Δειγματοληψία αποκρίσεων ανοιγοκλεισιματος ρεύματος

Data: N(χρόνος αναμονής), a(αρχή θέσης μνήμης), b(τέλος θέσης μνήμης), SUV(πίνακας CRP τιμών)

Result: CRP από την διεύιηση μνήμης a έως b

```
ορισμός του μήκους απόκρισης;
if καθυστέρηση then
    κλείσε τροφοδοσία;
    καθυστέρηση(N);
    άνοιξε τροφοδοσία;
else
    for i = a; i < b; i++ do
        κλείσε τροφοδοσία;
        άνοιξε τροφοδοσία;
        SUV[i] = διάβασεμνήμη(i);
    end
end
```

Μια παρατήρηση ζωτικής σημασίας είναι η ποιοτική διαφορά μεταξύ των κωδικοποιημένων δεδομένων εισόδου, με των δυαδικών. Οι κωδικοποιημένες σειρές είναι δυαδικό αποτέλεσμα της πράξης XOR από την απόκριση μιας μη κλωνοποιήσιμης πηγής, και αποθηκεύεται ως παράμετρος των βοηθητικών δεδομένων. Κατά την αποκατάσταση του κλειδιού, τα βοηθητικά δεδομένα επιτρέπουν την επιστροφή μιας κωδικοποιημένης θορυβώδους απόκριση, σε μορφή όπου μπορεί να εφαρμοστεί αποκωδικοποίηση διόρθωση σφαλμάτων. Στην πραγματικότητα, η μη κλωνοποιήσιμη πηγή χρησιμοποιείται για την αποθήκευση των βασικών συστατικών του κλειδιού, χρησιμοποιώντας για μία μοναδική παραλλαγή κατασκευή – όπου η τιμή του κλειδιού μπορεί να κατακερματιστεί σε ένα κλειδί, άρα οι κωδικοποιημένες λέξεις είναι αποτελούμενες από δυαδικές τιμές, και οι δυαδικές τιμές είναι σύμβολα κάποιας γραμματικής.

3.1.3 Μοντέλο συστήματος και το ασαφές σύστημα δέσμευσης

Σε ένα σύστημα με βοηθητικών δεδομένα έχουμε δύο φάσεις. Φάση εγγραφής, που εκτελείται μόνο μία φορά κατά την οποία παράγεται το κλειδί και τα βοηθητικά δεδομένα, και η φάση ανακατασκευής, στην οποία ανακατασκευάζεται το κλειδί, και μπορεί να

επαναληφθεί πολλές φορές. Κατά την εγγραφή, το διάνυσμα απόκαρσης της SRAM $x \in 0, 1$ μπορεί να χρησιμοποιηθεί για την εξαγωγή εντροπίας. Αντίστοιχα, το κλειδί αντιπροσωπεύει την παράμετρο $k \in K$ – όπου K σύνολο των πιθανών κλειδιών και $|K|$ η πληθικότητά του, με βοηθητικά δεδομένα $h \in H$, με H είναι το σύνολο όλων των πιθανών βοηθητικών δεδομένων, Το n το μήκος του διανύσματος απόκρισης x.

$$(k, h) = E(x^n) \tag{3.8}$$

Από την άλλη πλευρά, στην φάση ανακατασκευής το δυαδικό διάνυσμα θούβου ορίζεται ως $y \in (0, 1)$, ισχύει $y^n = x^n \oplus e^n$, και το διάνυσμα σφάλματος ορίζεται ως e και η αποκωδικοποιημένη ανακατασκευή γίνεται με εκτίμηση του κλειδιού $\hat{k}$, και το θορυβώδες διάνυσμα y – επιτυχία ανακατασκευής είναι όταν το αρχικό κλειδί είναι στην έξοδο, δηλαδή $\hat{k} = k$.

$$\hat{k} = D(h, y^n) \tag{3.9}$$

Η διαδικασία της ασαφούς ανάκτησης αποτελείται από δύο μέρη, κωδικοποίηση με αντίστοιχους αλγορίθμους διόρθωσης σφαλμάτων, και ενίσχυση της ιδιωτικότητας – η αντιμετώπιση διαρροής πληροφορίας, εξάγοντας ένα κλειδί πλήρους εντροπίας από το ανακατασκευασμένο κλειδί που έχει αποκαλυφθεί ένα κομμάτι του, όπως κατανέμονται τα βοηθητικά δεδομένα.(δες σχήμα 3.1) [67]. Ειδικότερα, για ένα γραμμικό κώδικα διόρθωσης σφαλμάτων δυαδικού πίνακα γεννήτριας G διαστάσεων kxn, επίσης ορίζεται ως σειρά δυαδικών τιμών κάθε απόκρισης $m^k \in (0, 1)^k$ μήκους k, και δυαδικών τιμών απόκρισης ορίζεται αντίστοιχα $c \in (0, 1)^n$.

$$\hat{m}^l = D(h, y^n) \tag{3.10}$$

Η συνάρτηση κωδικοποίησης για έναν συγκεκριμένο αλγόριθμο κωδικοποίησης E, μιας απόκρισης S:

$$c^n = m^k G = c^n \oplus E(S) \tag{3.11}$$

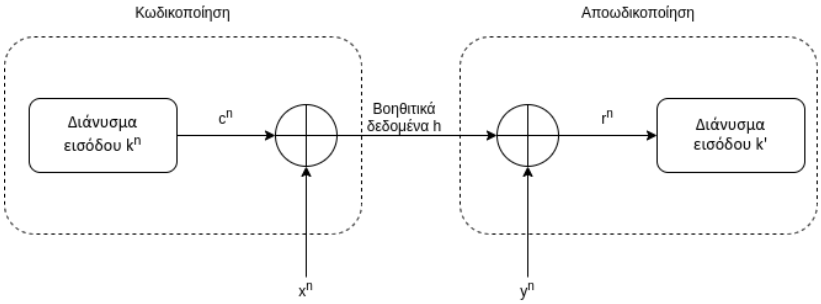

Fig. 3.1 Σχήμα ασαφούς δέσμευσης

Η συνάρτηση αποκωδικοποίησης ορίζεται ως:

$$\hat{m}^k = D(c^n \oplus e^n) \tag{3.12}$$

3.2 Απαιτήσεις εφαρμογής

Ο απώτερος στόχος των μη-αντιγράψιμων συναρτήσεων είναι η επίτευξη ενιαίας αυθεντικοποίησης σε επίπεδο συσκευής, στην οποία στερούσε υπολογιστικές δυνατότητες. Για τον σκοπό αυτό, ο σχεδιασμός αρχιτεκτονικής παρατίθεται εξάρτηση σε ένα σύνολο απαιτήσεων στο επίπεδο της εφαρμογής.

3.2.1 Στοιχεία προϋποθέσεων αναγκών ασφαλούς συστήματος

Η αυθεντικοποίησης της μνήμης SRAM δεν αφορά μόνο θεμελιώδες κομμάτι του υλικού κατασκευής, αλλά το κλειδί που προκύπτει πρέπει να χρησιμοποιείται ως ραχοκοκαλιά εμπιστοσύνης (root-of-trust) ως κοινή ερμηνευτική καθοδήγηση των εγγενών χαρακτηριστικών. Πέρα από την αυθεντικοποίηση, το επιθυμητό επίπεδο ασφαλείας ενός κρυπτογραφικού κλειδιού πρέπει να υλοποιηθεί έτσι ώστε να εγγυώνται συμμόρφωση με πρότυπα προστασίας ευαίσθητων πληροφοριών [112]. Επιπρόσθετα, όλες οι απαραίτητες λειτουργίες ενδεχόμενος να χρησιμοποιούν έμμεσα την μνήμη για τον διακανονισμό επικουρικών κωδικών διόρθωσης σφαλμάτων, επομένως στην αρχιτεκτονική συνιστάται η πρόβλεψη με επαρκή βαθμό πιθανότητας επιθέσεων ανάκτησης μνήμης. Ακόμα, η διενέργεια μηχανισμό ελέγχου ταυτότητας προβλέπει

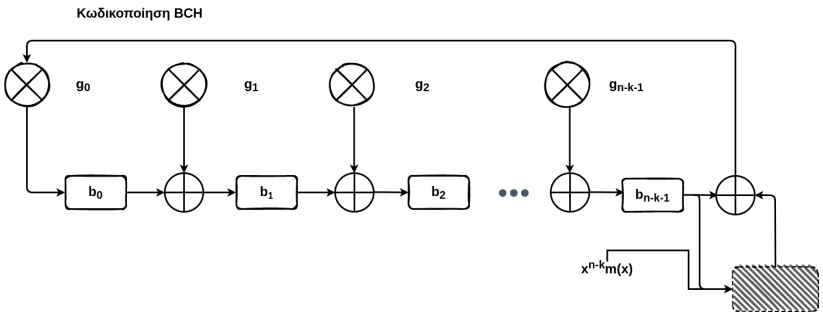

Fig. 3.2 Σχεδιασμός των κωδικών διορθώεθωσης σφαλμάτων BCH, όπου $m(x)$ το πολυώνυμο των δυαδικών τιμών εισόδου, γεννήτριας πολυωνύμου $g(x)$ [3, 4].

κατάλληλα αντίμετρα, και για την διατήρηση διαβίβασης των εμπιστευτικών δεδομένων με εξουσιοδότηση, είναι απαραίτητο η επικοινωνία να είναι κρυπτογραφημένη.

3.2.2 Αρχιτεκτονική κωδικών BCH

Ο αλγόριθμος ασφαλούς σκίτσου, όπως παρουσιάστηκε στην ενότητα 2.3.1, χρησιμοποιεί έναν ενιαίο γραμμικό κώδικα διόρθωσης σφαλμάτων για την επιδιόρθωση σφαλμάτων στις αποκρίσεις μιας μη-αντιγράψιμης πηγής. Ωστόσο, ο συνδυασμός με κώδικες διόρθωσης, προσφέρουν σημαντικά πλεονεκτήματα ασφαλείας – η υπολογιστική κατανάλωση είναι υψηλή, δηλαδή δεν είναι κατάλληλη για συγκεκριμένες περιπτώσεις όπου η ενέργεια και χωρητικότητα λαμβάνονται υπόψη. Η φιλοσοφία του αλγορίθμου Berlekamp συνίσταται στην επίλυση του συνόλου των συμμετρικών αθροιστικών συναρτήσεων δυνάμεων (δες σχεδιάγραμμα σχήμα 3.2) [3, 4] – το πιο υπολογιστικά σπάταλο βήμα είναι η αναζήτηση του πολυωνύμου εντοπισμού σφάλματος.

Εκτός του ότι οι κώδικες BCH έχουν αποκωδικοποιητή χαμηλής πολυπλοκότητας, έχουν αυστηρή αλγεβρική δομή. Συνεπώς, είναι απλοί στη χρήση τόσο στην κωδικοποίηση όσο και στην αποκωδικοποίηση. Στους κώδικες BCH, οι κώδικες λέξεις δημιουργούνται διαιρώντας ένα πολυώνυμο m(x) που αντιπροσωπεύει τα δεδομένα (δυαδικά δεδομένα) με ένα πολυώνυμο γεννήτριας g(x) και λαμβάνοντας το υπόλοιπο, το

οποίο θα παρουσιαστεί ως μπιτ ελέγχου ισοτιμίας r(x). Τα χαρακτηριστικά του κώδικα καθορίζονται από το επιλεγμένο πολυώνυμο γεννήτριας g(x).

Algorithm 2: Βήματα αποκωδικοποίησης του αλγορίθμου BCH [4, 113, 3].

Data: v(λέξη εισόδου με το πολύ t σφάματα με κώδικα σχεδιασμένης απόστασης $d \geq 2t + 1$)

Result: w(μεταδιδόμενη λέξη), e(σφάλματα λέξης)

1 Προσδιορισμός συνόδου της ληφθείσας δυαδικής σειράς v ;
2 Προσδιορίστε τον μέγιστο αριθμό $r \leq t$ ώστε το σύστημα εξισώσεων ;
3 Το αρχιό μύνημα μετατρέπεται σε άρθροισμα του αρχικού μυνήματος και ορίζεται ένα διάνυσμα σφαλμάτων;
4 Επίλυση συνδρόμου ανιχνεύοντας τις θέσεις σφάλματος;
5 Προσδιορισμός και διόρθωση σφαλμάτων, και εύρεση μεταβαλόμενων δυασικών λέξεων;
6 Επιστροφή των w και e;

Συνοψίζοντας, οι κώδικές BCH δεν είναι πανάκεια για σφάλματα που ακολουθούν διαφορετική συνεχόμενη ακολουθία συμβόλων, και για συγκεκριμένο αριθμό σφαλμάτων t, γιατί δεν είναι δυνατόν να ανιχνευθεί αν έχει ξεπεραστεί η δυνατότητα διόρθωσης – η απόδοση του αλγορίθμου Berlekamp–Massey είναι ικανοποιητικές σε σχέση με άλλους αλγορίθμους όπως ο Reed-Solomon [114].

3.2.3 Μηδενισμός κλειδιών

Ο μηδενισμός της μνήμης αποτελεί όχι μόνο ένα μηχανισμό ασφαλείας, διαγράφοντας ορισμένα κλειδιά σε μια μνήμη, αλλά με αυτό τον τρόπο μπορούν να διαχωριστούν τα σταθερά μπιτ με τα ασταθή. Αυτό μπορεί να συμβεί με την αντικατάσταση ολόκληρης της τιμής του κλειδιού που εξέρχεται είτε με μηδενικά είτε με μια τυχαία συμβολοσειρά, άλλα για τον προσδιορισμό της αστάθειας ακολουθείτε η εξής διαδικασία. Για να χαρακτηριστούν τα κελιά της μνήμης, αρχικά η διεύθυνση μνήμης διαγράφεται τελείως γεμίζοντας τη με άσσους. Έπειτα, με την ίδια λογική η διεύθυνση προγραμματίζεται, δηλαδή γεμίζει με μηδενικά. Πριν από την εκτέλεση κάθε λειτουργίας μερικής διαγραφής, το τμήμα του κελιού προγραμματίζεται έτσι ώστε η επόμενη λειτουργία μερικής διαγραφής να εκτελείται με όλα τα κελιά στην προγραμματισμένη κατάσταση. Στη

συνέχεια, εκτελείται μια λειτουργία μερικής διαγραφής για έναν παραμετροποιημένο αριθμό ανιχνεύοντας έτσι ποια κελιά είναι σταθερά ή ασταθή.

Algorithm 3: Συνάρτηση διαγραφής μνήμης και χαρακτηρισμός σταθερών μπιτ

```
Data: a(αρχή θέσης μνήμης), b(τέλος θέσης μνήμης)
1 while καθορισμένος χρόνος do
2     Πλήρης διαγραφή τμήματος          ▷ γέμισμα με 0xFF;
3     Πλήρης διαγραφή σχήματος          ▷ γέμισμα με 0x00;
4     Μερικώς διαγραφή κατάστασης       ▷ γέμισμα τυχαία με 0x00 και 0xFF;
5     for i = a; i < b; i++ do
6         σταθερά1(i)                   ▷ άθροισμα σταθερών άσσων;
7         σταθερά0(i)                   ▷ άθροισμα σταθερών μηδενικών;
8     end
9 end
```

Να σημειωθεί πως στην βιβλιογραφία υπάροχυν αρκετοί τρόποι φιλτραρίσματος που βελτιώνουν την αποδοτικότητα και ασφάλεια του κυκλώματος [76].

3.2.4 Εργαστηριακός εφοδιασμός

Πρώτα από όλα, η υλοποίησή όλων των πειραμάτων πραγματοποιήθηκαν πάνω σε μικροεπεξεργαστές ATmega2560 (ταχύτητα ρολογιού 16Mhz και εσωτερική SRAM 8kB) [1] της πλακέτας ανάπτηξης της Arduino, και ο συνολικός αριθμός ήταν δύο. Αναλυτικότερα, στο αναφερθέντα εργαλείο επανδρώθηκαν οι μνήμες τύπου SRAM, δύο συνολικά 23LC1024 [2], δύο 23K256 [3], και ένα CY62256 [4]. Η απόφαση εγκρίθηκε σύμφωνα με την απαίτηση δοκιμών σε SRAM CMOS μνήμες οι οποίες, πρώτων ήταν προσιτές ως προς το οικονομικό κομμάτι, και δεύτερον, η διαθεσιμότητα ήδη υπάρχουσας βιβλιογραφίας. Εντούτοις, η ραχοκοκαλιά της μη κλωνοποίησής πηγής είναι ο μικροεπεξεργαστής του ATMEGA 256[5], για τον οποίο παρότι συνεχίζεται ραγδαία ο ανταγωνισμός στους επεξεργαστές υλοποίησης, αποτελεί ρεαλιστική προσέγγιση σε πειραματική συσσώρευση πειραμάτων [115, 116, 111, 117], όσο και σε βιομηχανικό επίπεδο προστασίας της εχεμύθειας που παρέχουν τα εγγενή χαρακτηριστικά.

[1] https://docs.arduino.cc/hardware/mega-2560 (Accessed May 26 2021)
[2] https://www.microchip.com/wwwproducts/en/23LC1024 (Accessed May 26 2021)
[3] https://www.microchip.com/wwwproducts/en/23K256 (Accessed May 26 2021)
[4] https://www.manualslib.com/products/Cypress-Cy62256-6986949.html (Accessed May 26 2021)
[5] https://www.microchip.com/wwwproducts/en/ATmega2560

Έπειτα, η γλώσσα προγραμματισμού αφενός ήταν εξ ορισμού C του επίσημου προϊόν, αφετέρου πραγματοποιήθηκε προκαταρκτική υλοποίησή σε σύγχρονη και ασφαλή γλώσσα σε αναπτυξιακό περιβάλλον ενσωματωμένων συσκευών Rust[6], αυτό οφείλεται στις παροχές ασφαλείας, λόγου χάρη η εγγύηση μηδενισμού με ασφάλειας της μνήμης με την βοήθεια της βιβλιοθήκη zeroize[7]. Ωστόσο, μια καλή πρακτική είναι η ανάπτυξη κώδικα ακολουθώντας τους κανόνες και συστάσεις του οργανισμού CERT[8].

3.2.5 Επαλήθευση και την επικύρωση ταυτοποίησης του κυκλώματος

Στο πρώτο στάδιο επιθεώρησης τυχαιότητας της πηγής παρέχεται η επιστημονική αιτιολόγηση, πρώτον υποστήριξης μοναδικότητας σε σύγκρισή με ίδιο εξοπλισμό (τσιπ SRAM), και δεύτερον πραγματοποίηση ίδιας μέτρησης διαφορετικών επεξεργαστών(ίδιου τύπου). Η μμέθοδος αναφοράς συνίσταται στον προσδιορισμό αυξομείωσης του θορύβου και των ασταθών κελιών. Αξιοσημείωτη παρατήρηση είναι η συζήτηση σχετικά με την ασφάλεια που παρέχει το σύστημα, μολονότι στους περισσότερους σχετικούς ορισμούς, η ασφάλεια ποσοτικοποιείται με τη χρήση των μέτρων τυχαιότητας, και του χρόνου εκτέλεσης ή την παρατήρησης ανάλυσης κωδικών μετατροπής των αποκρίσεων. Ακόμα κι έτσι, στη παρούσα αναφορά ενδείκνυται να ληφθεί μέριμνα παράκαμψης ποσοτικοποίησης της ασφάλειας και αντ' αυτού επίκεντρο γίνεται σε παρακολούθηση υποκατάστατων παραμέτρων για λόγους διαφάνειας και σφαιρικότητας. Η αναλογία των δυαδικών τιμών, κυμαινόταν μεταξύ 55% και 58% πλήθους των άσσων – η δειγματοληψία έλαβε χώρα σε θερμοκρασία δωματίου, δηλαδή °25C ... °30C (°77 ... 86F), και τάση εύρους 1.5V μέχρι 4.5V.

3.2.6 Τυχαιότητα απόκρησης

Τυχαίοτητα των αποκρίσεων μιας μη κλωνοποιήσης πηγής εκτιμάται με διάφορες παραμέτρους όπως εξηγήθηκε παραπάνω 3.0.3. Για να παράγει μια πηγή (συσκευή) τυχαίες τιμές, αρχικά πρέπει να εξασφαλιστεί η εγγενής τυχαιότητα, με την σύγκριση μια απόκρισης, ίδιων διευθύνσεων, αλλά με διαφορετικές συσκευές. Μετά, η δειγματοληψία ελέγχεται σε μια πληθώρα στατιστικών δοκιμών. Τα περισσότερα τεστ περιγράφονται αναλυτικά στο παράρτημα της αναφοράς .1.

[6]https://github.com/avr-rust
[7]https://docs.rs/zeroize/1.3.0/zeroize/index.html
[8]https://wiki.sei.cmu.edu/confluence/display/c/SEI+CERT+C+Coding+Standard

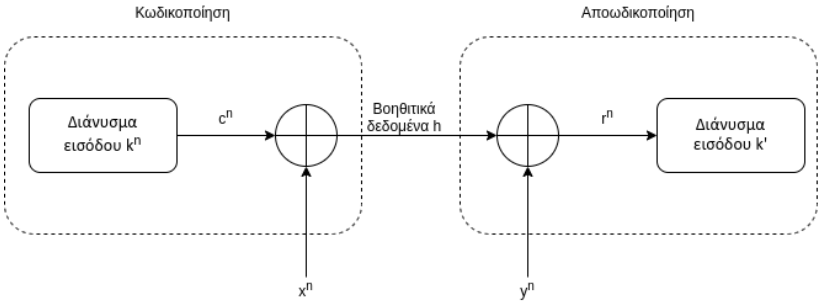

Fig. 3.3 Γράφημα ιστογράμματος .

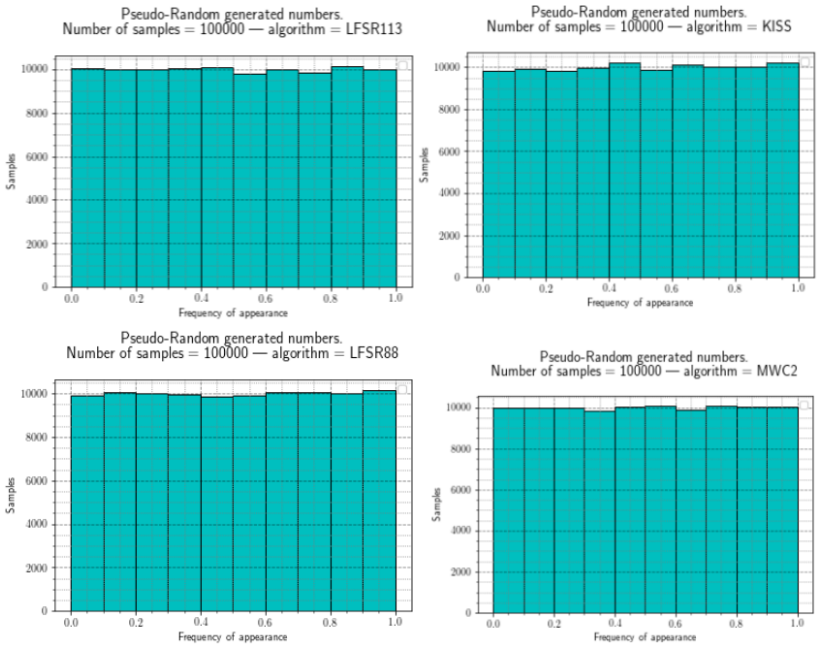

Fig. 3.4 Γράφημα ιστογράμματος τεσσάρων αλγορίθμων ψευδοτυχαίων αριθμών, δείγματος 1000 τιμών. Παρατηρούμε πως τυχαίες οι μεταβλητές αντιπροσωπευόνται από απόλυτα επίπεδο ιστόγραμμα σε σχέση με τις πραγματικά τυχαίες συναρτήσεις.

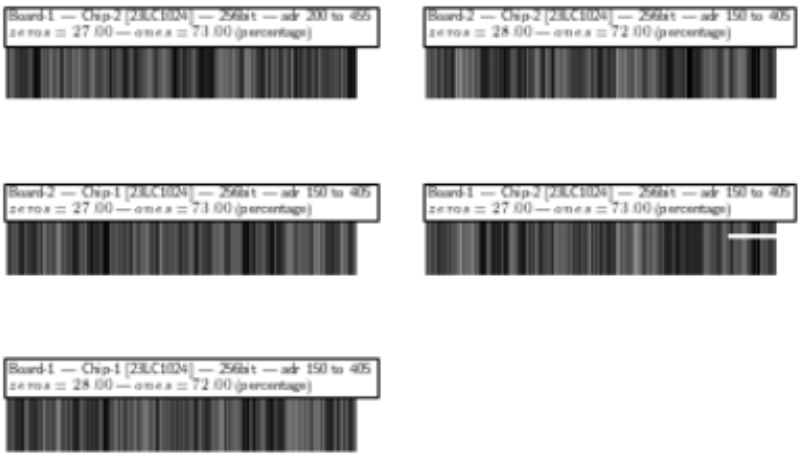

Fig. 3.5 Βάρος Χάμινγκ σε πέντε διαφορετικές περιπτώσεις δείγματος 500 τιμών. Σε κάθε δέκα χιλιάδες δείγματα υπάρχει το πολύ 4% δείγματος 128 μπιτ μεταβάλεται, και μεταβάλονται από 5 έως 9 διευθήνσεις τιμών.

Για την εγγύηση επαρκούς παραλλαγής μεταξύ των αποκρίσεων δύο ίδιων τσιπ(διαφορετικά), πρέπει να εξεταστεί ένα σετ αποκρίσεις ίδιων διευθύνσεων μνήμης, αλλά διαφορετικών συσκευών. Η διακύμανση μεταξύ των δύο κυκλωμάτων είναι παρόμοια με την παραλλαγή την εσωτερικής απόστασης Χάμινγκ. Έτσι, καταλήγουμε στο συμπέρασμα ότι υπάρχει επαρκής ποσοστό διαφοράς μεταξύ των δύο πηγών, σε βάρος Χάμινγκ και απόσταση μεταξύ διαφορετικών συσκευών. Με αυτή την μέθοδο ανιχνεύτηκε και η πιο ευαίσθητη συσκευή(θορυβώδες), η οποία στην συνέχεια χρησιμοποιήθηκε σαν σημείο αναφοράς για άλλα πειράματα. Σε σύγκριση με τις ψευδοτυχαίες γεννήτριες αριθμών, στις οποίες πηγή τυχαιότητας είναι κάποιο ασταθές γραμμικό στοιχείο (πχ. η τρέχουσα ώρα), παρατηρείται σχήμα 3.4 το δείγμα για διαφορετικούς αλγορίθμους η απόσταση Χάμινγκ, όσο και το βάρος δεν ικανοποιούν τις συνθήκες πραγματικής τυχαιότητας.

Κατασκευή μια απόκρισης σε συγκεκριμένες θέσεις μνήμης, είχε σαν αποτέλεσμα στις μνήμες 23LC1024 αναλογία περίπου 67% με 68% άσσων, κάτι που δεν είναι δεκτό σε ένα μη-αντιγράψιμο σύστημα. Ωστόσο, σε παρόμοια έρευνα το δείγμα διαχωρίστηκε σε όρια με τις ποιο σταθερές διευθύνσεις. Σε όλες τις μνήμες SRAM(τσιπ), όταν η δειγματοληψία διάβαζε όλη τις πιθανές θέσεις μνήμης, τότε η αναλογία βελτιωνόταν δραματικά, με νέα αναλογία κοντά 50%. Εάν και μη πρακτική μεθοδολογία, η επιλογή των πιο σταθερών κελιών είχε επίδραση στη σειρά μέχρι και 55% άσσων.

Το φαινόμενο γήρανσης σε 1000 δείγματα, εάν και λίγα, παρουσιάζεται σε λίγες περιπτώσεις είναι η τάση ευαίσθητη για μικρές μεταβολές.

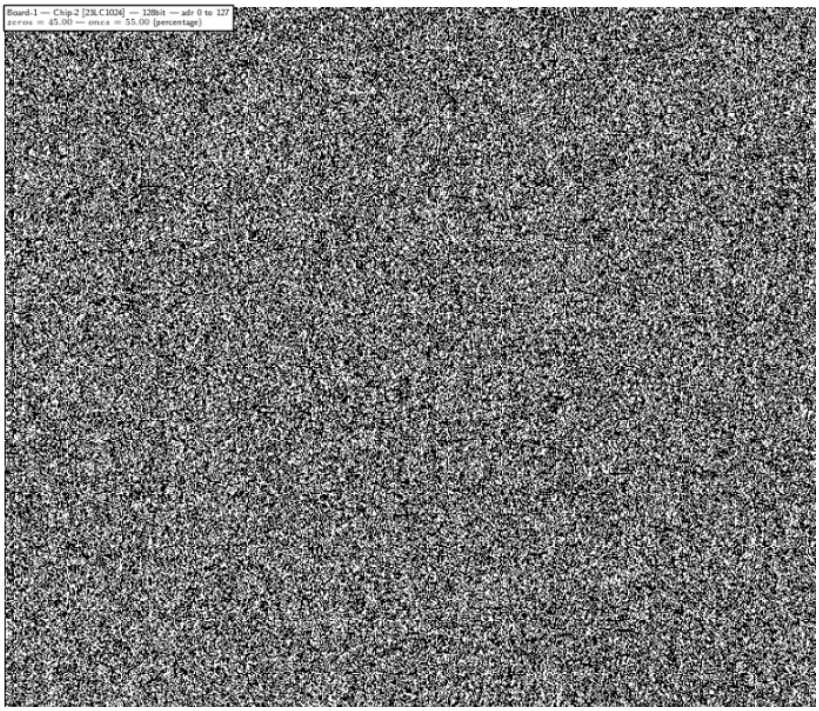

Fig. 3.6 Βάρος Χάμινγκ για ένα κύκλωμα 128 μπιτ δείγματος 1000 τιμών. 55% είανι άσσοι, και 45% μηδενικά.

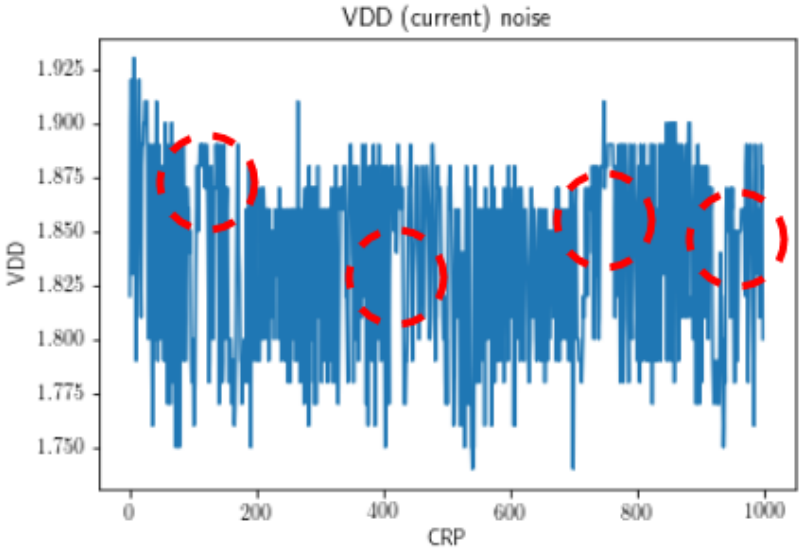

Fig. 3.7 Μικρές παρεμβολές τάσεις δείγματος 1000 τιμών.

Με την βοήθεια της σουίτας Dieharder, και NIST, επαληθεύτηκε η τυχαιότητα του κυκλώματος σε δείγμα διάστασης ενός εκατομμυρίου αποκρίσεων.

Η ακατέργαστη έξοδος των μνημών SRAM είναι μεροληπτική και μη-ομοιόμορφα κατανεμημένη. Ωστόσο, δεν υπάρχει τυπική τεχνική που λαμβάνει υπόψη τη δυνατότητα συσχετίσεων μεταξύ δειγμάτων, για την αξιολόγηση της εντροπίας φυσικών πηγών. Ως εκ τούτου, η σουίτα στατιστικών δοκιμών της NIST και DieHarder, εφαρμόζονται για την αξιολόγηση της καταλληλότητας του παραγόμενου βασικού υλικού. Μια καλή πρακτική καλύτερης ακρίβειας των δοκιμών, είναι η συλλογή των τιμών P, για δύο λόγους. Εάν η διαδικασία, για οποιοδήποτε λόγο διακοπεί, τότε η δοκιμή δεν χάνει το ιστορικό των προηγούμενων τιμών και η επόμενη λύψη . Επιπλέον, πολλές δοκιμές, όπως η (θεωριτικό υπόβαθμο εδώ .4.7) μπορεί να παρουσίαζαν μη φανερά αποτελέσμα (weak), δηλαδή περιρετέρο επεξεργασία ήταν απαραίτητη.

Η αναγνώριση του στατιστικού μοτίβου σταθερότητας των αποκρίσεων, γνωστό ως False Acceptance Rate (FAR) και False Rejection Rate (FRR) αντίστοιχα, και για την ταυτοποίηση της στατιστικής τάσης ελέγχεται το ποσό δειγματοληψίας της απόστασης Χάμινγκ για δύο περιπτώσεις. Πρώτα, με έλεγχο επικάλυψης δειγμάτων σε σύγκριση με το ίδιο κύκλωμα ή και με διαφορετικές διευθύνσεις (βλέπε σχήμα 3.10), και σε συνδυασμό με διαφορετικό ίδιου τύπου εξοπλισμού (τσιπ) [6]. Ωστόσο, η μέθοδος ελέγχου σταθερών μπιτ είναι πιο αποτελεσματική μέθοδος αναγνώρισης σφαλμάτων, τα μέτρα αναγνώρισης στατιστικών μοτίβων, FAR και FRR συνιστώνται για έλεγχο σε διαφορετικές περιβαλλοντικές συνθήκες.

3.2.7 Σχολιασμός αποτελεσμάτων

Το πρώτο αναμενόμενο αποτέλεσμα της δειγματοληψίας είναι η πραγματική τυχαιότητα, με άλλο λόγια πρέπει να ισχύουν δύο συνθήκες. Για μια συγκεκριμένη συσκευή, οι συγκεκριμένες διευθύνσεις(εγγενή) μνήμης πρέπει να έχουν διαφορετικά αποτελέσματα για διαφορετικό εύρος φάσματος, και προβλέπεται ένα ισορροπημένο βάρος Χάμινγκ. Ωστόσο, όπως και στα έργα της βιβλιογραφίας, τα επιλεγμένα τσιπ SRAM, δεν είναι αποδοτικότητα για συγκεκριμένο μήκος δειγματοληψίας. Έπειτα, η ομοιομορφία μεταξύ των δύο ίδιων τσιπ(SRAM), η οποία αναμένεται να έχουμε υψηλή ανομοιότητα, και με τα αποτελέσματα αυτό επαληθεύεται έστω και για δύο διαθέσιμες συσκευές μονάχα.

Το ιδανικότερο είναι $\sigma = 0.0442$ και $\mu = 0.5$ για πλήρες τυχαιότητα. Για τον ρυθμό σφάλματος μπιτ σε κάθε δείγμα, υπολογίστηκε στο τέλος της δειγματοληψίας, για περίπου χίλιες αποκρίσεις σε κάθε περίπτωση.

test_name	ntup	tsamples	psamples	p-value	Assessment
diehard_birthdays	0	100	100	0.65833713	PASSED
diehard_operm5	0	1000000	100	0.73447973	PASSED
diehard_rank_32x32	0	40000	100	0.13532425	PASSED
diehard_rank_6x8	0	100000	100	0.67334174	PASSED
diehard_bitstream	0	2097152	100	0.76933379	PASSED
diehard_opso	0	2097152	100	0.75339079	PASSED
diehard_oqso	0	2097152	100	0.51982961	PASSED
diehard_dna	0	2097152	100	0.24459837	PASSED
diehard_count_1s_str	0	256000	100	0.26348943	PASSED
diehard_count_1s_byt	0	256000	100	0.31463149	PASSED
diehard_parking_lot	0	12000	100	0.32092307	PASSED
diehard_2dsphere	2	8000	100	0.97350879	PASSED
diehard_3dsphere	3	4000	100	0.24078371	PASSED
diehard_squeeze	0	100000	100	0.59375	PASSED
diehard_sums	0	100	100	0.11152722	PASSED
diehard_runs	0	100000	100	0.11565658	PASSED
diehard_runs	0	100000	100	0.2676741	PASSED
diehard_craps	0	200000	100	0.32045037	PASSED
diehard_craps	0	200000	100	0.96787572	PASSED
marsaglia_tsang_gcd	0	10000000	100	0.76404136	PASSED
marsaglia_tsang_gcd	0	10000000	100	0.48110595	PASSED
sts_monobit	1	100000	100	0.89067256	PASSED
sts_runs	2	100000	100	0.09679602	PASSED
sts_serial	1	100000	100	0.98979275	PASSED
sts_serial	2	100000	100	0.38294337	PASSED
sts_serial	3	100000	100	0.24047207	PASSED
sts_serial	3	100000	100	0.29228199	PASSED
sts_serial	4	100000	100	0.48745071	PASSED
sts_serial	4	100000	100	0.48780004	PASSED
sts_serial	5	100000	100	0.45855356	PASSED
sts_serial	5	100000	100	0.07524926	PASSED
sts_serial	6	100000	100	0.50052161	PASSED
sts_serial	6	100000	100	0.37479638	PASSED
sts_serial	7	100000	100	0.71387648	PASSED
sts_serial	7	100000	100	0.82322663	PASSED
sts_serial	8	100000	100	0.76922365	PASSED
sts_serial	8	100000	100	0.85034347	PASSED
sts_serial	9	100000	100	0.23982013	PASSED
sts_serial	9	100000	100	0.68887988	PASSED
sts_serial	10	100000	100	0.68784177	PASSED
sts_serial	10	100000	100	0.86684024	PASSED
sts_serial	11	100000	100	0.32673337	PASSED
sts_serial	11	100000	100	0.43558266	PASSED
sts_serial	12	100000	100	0.83836166	PASSED
sts_serial	12	100000	100	0.68260588	PASSED
sts_serial	13	100000	100	0.66839913	PASSED
sts_serial	13	100000	100	0.6917886	PASSED
sts_serial	14	100000	100	0.59017905	PASSED
sts_serial	14	100000	100	0.4043428	PASSED
sts_serial	15	100000	100	0.28218027	PASSED
sts_serial	15	100000	100	0.3909433	PASSED
sts_serial	16	100000	100	0.19985545	PASSED
sts_serial	16	100000	100	0.41791429	PASSED
rgb_bitdist	1	100000	100	0.71089255	PASSED
rgb_bitdist	2	100000	100	0.98522809	PASSED
rgb_bitdist	3	100000	100	0.34077962	PASSED
rgb_bitdist	4	100000	100	0.15725554	PASSED
rgb_bitdist	5	100000	100	0.55860965	PASSED
rgb_bitdist	6	100000	100	0.36394184	PASSED
rgb_bitdist	7	100000	100	0.6503176	PASSED
rgb_bitdist	8	100000	100	0.64822266	PASSED
rgb_bitdist	9	100000	100	0.97054624	PASSED
rgb_bitdist	10	100000	100	0.47673586	PASSED
rgb_bitdist	11	100000	100	0.99262257	PASSED
rgb_bitdist	12	100000	100	0.80876763	PASSED
rgb_minimum_distance	2	10000	1000	0.39631494	PASSED
rgb_minimum_distance	3	10000	1000	0.73721093	PASSED
rgb_minimum_distance	4	10000	1000	0.63317962	PASSED
rgb_minimum_distance	5	10000	1000	0.26255031	PASSED
rgb_permutations	2	100000	100	0.82743915	PASSED
rgb_permutations	3	100000	100	0.51446359	PASSED
rgb_permutations	4	100000	100	0.99799891	WEAK
rgb_permutations	5	100000	100	0.7414606	PASSED
rgb_lagged_sum	0	1000000	100	0.55436316	PASSED
rgb_lagged_sum	1	1000000	100	0.82076868	PASSED
rgb_lagged_sum	2	1000000	100	0.34237766	PASSED
rgb_lagged_sum	3	1000000	100	0.31696315	PASSED
rgb_lagged_sum	4	1000000	100	0.04469651	PASSED
rgb_lagged_sum	5	1000000	100	0.98009164	PASSED
rgb_lagged_sum	6	1000000	100	0.05006724	PASSED
rgb_lagged_sum	7	1000000	100	0.87038618	PASSED
rgb_lagged_sum	8	1000000	100	0.79961094	PASSED
rgb_lagged_sum	9	1000000	100	0.79899877	PASSED
rgb_lagged_sum	10	1000000	100	0.89041014	PASSED
rgb_lagged_sum	11	1000000	100	0.65076604	PASSED
rgb_lagged_sum	12	1000000	100	0.38243426	PASSED
rgb_lagged_sum	13	1000000	100	0.11294708	PASSED
rgb_lagged_sum	14	1000000	100	0.96180847	PASSED
rgb_lagged_sum	15	1000000	100	0.54007105	PASSED
rgb_lagged_sum	16	1000000	100	0.98385455	PASSED
rgb_lagged_sum	17	1000000	100	0.23418633	PASSED
rgb_lagged_sum	18	1000000	100	0.72651693	PASSED
rgb_lagged_sum	19	1000000	100	0.04645434	PASSED
rgb_lagged_sum	20	1000000	100	0.77177094	PASSED
rgb_lagged_sum	21	1000000	100	0.37196652	PASSED
rgb_lagged_sum	22	1000000	100	0.97894002	PASSED
rgb_lagged_sum	23	1000000	100	0.88219901	PASSED
rgb_lagged_sum	24	1000000	100	0.95288858	PASSED
rgb_lagged_sum	25	1000000	100	0.17097275	PASSED
rgb_lagged_sum	26	1000000	100	0.94822619	PASSED
rgb_lagged_sum	27	1000000	100	0.98469817	PASSED
rgb_lagged_sum	28	1000000	100	0.43748068	PASSED
rgb_lagged_sum	29	1000000	100	0.51911714	PASSED
rgb_lagged_sum	30	1000000	100	0.67593179	PASSED
rgb_lagged_sum	31	1000000	100	0.93962304	PASSED
rgb_lagged_sum	32	1000000	100	0.63027538	PASSED
rgb_kstest_test	0	10000	1000	0.64720296	PASSED
dab_bytedistrib	0	51200000	1	0.80357631	PASSED
dab_dct	256	50000	1	0.08154249	PASSED
dab_filltree	32	15000000	1	0.04006625	PASSED
dab_filltree	32	15000000	1	0.29572706	PASSED
dab_filltree2	0	5000000	1	0.22489276	PASSED
dab_filltree2	1	5000000	1	0.21929544	PASSED
dab_monobit2	12	65000000	1	0.87486528	PASSED

SRAM: 23LC1024 - Chip: #1 - Board: #1 - 16 bit - Memory address: 49 to 65

Fig. 3.8 Αναλυτικός πίνακας αποτελεσμάτων δοκιμών Dieharder της απόκρισης μήκους 16 μπιτ της SRAM 23LC1024 – στο διάνυσμα δεν πραγματοποιήθηκε επεξεργασία πρίν ή μετά της δειγματολειψίας.

Test	Status
The Frequency (Monobit) Test	PASS
Frequency Test within a Block	PASS
The Runs Tests	PASS
Test for the Longest-Run-of-Ones in a Block	PASS
The Binary Matrix Rank Test	PASS
The Discrete Fourier Transform (Spectral) Test	PASS
The Non-overlapping Template Matching Test	PASS
The Overlapping Template Matching Test	PASS
Maurer's "Universal Statistical" Test	PASS
The Lempel-Ziv Compression Test	PASS
The linear Complexity Test	PASS
The Serial Test	PASS
The approximate Entropy Test	PASS
The Cumulative Sums (Cusums) Test	PASS
The Random Excursion Test	PASS
The Random Excursion Variant Test	PASS

Fig. 3.9 Αναλυτικός πίνακας αποτελεσμάτων δοκιμών πλατφόμας NIST [5], σε ένα εκκατομύριο δείγματα (1.4 εκκατομύρια) και ένα εκκατομύριο για καλύτερη ακρίβεια.

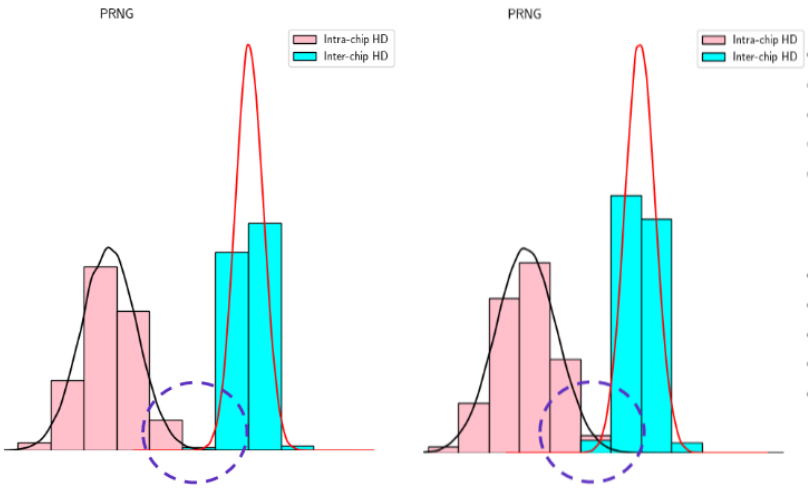

Fig. 3.10 Η απόσταση Χάμινγκ ίδιας συσκευής, αλλά διαφορετικού τσιπ πρέπει όσο το δυνατότερο διαφορετική , προκειμένου να μην υπάρχει ομοιομορφία μεταξύ των κλάσεων. Στα αριστερά είναι ευανάγνωστα φαναιρό ότι οι δύο σείρες έχουν πολλές ομοιότητες, δηλαδή όσο μεγαλύτερη απόσταση του έρους απόστασης Χάμινγκ, τόσο ποιο ανομοιόμορφο είναι το κύκλωμα [6].

Μοντέλο SRAM	Απόσταση Χάμινγκ#1	Απόσταση Χάμινγκ#2	Ομοιομορφία	μ	σ
23LC1024	46	45.5	42	0.73	0.45
23K256	42	43.2	39	0.79	0.39

Table 3.1 Αποτελέσματα δύο κλάσεων SRAM για δύο συσκευές σε δείγμα δέκα χιλιάδων αποκρίσεων.

Μοντέλο SRAM	Βάρος Χάμινγκ	Κλασματική απόσταση Χάμινγκ
23LC1024	55%	58%
CY62256	69%	61%
23K256	72%	65%

Table 3.2 Αποτελέσματα όλων των διαφορετικών τύπων SRAM για τις καλύτερες περιπτώσεις. Το πλήθος του δείγματος ήταν περίπου δέκα χιλιάδες για κάθε τσιπ ξεχωριστά.

Βελτίωση στο βάρος Χάμινγκ πραγματοποιήθηκε σε όλα τα τσιπ όταν το μέγεθος της απόκρισης αυξανόταν, ή ακολουθούσε εκλογή των σταθερών μπιτ της μνήμης SRAM. Επίσης, για τον αβυσσαλέο ρυθμό παραγωγής(μηδέν ή ένα) των κελιών, μας ενδιαφέρει το συνολικό εφικτό ποσοστό(ποιοτικό χαρακτηριστικό). Εφόσον οι αποκρίσεις ενός κελιού είναι ανεξάρτητες και ταυτόσημες κατανεμημένες, οι καταστάσεις των κελιών καθορίζονται από τυχαίες μεταβλητές με κάποια συνάρτηση πυκνότητας πιθανότητας. Κάθε απόκριση 128 μπιτ, χρειάζεται περίπου 50 ns για να παραχθεί, πρακτικά είναι επαρκώς γρήγορο για τις περισσότερες εφαρμογές, αλλά ενδέχεται έως και τριπλασιασμός του χρόνου όταν επεξεργαστεί η απόκριση με αλγόριθμο διόρθωσης σφαλμάτων. Οπότε, ορίζοντας προτεραιότητα στα χαρακτηριστικά που αναφερθήκαμε προηγούμενος, οι μνήμες SRAM συνίστανται προ-επεξεργασία του κυκλώματος για διόρθωση σφαλμάτων ή βελτίωσης των αποκρίσεων.

Κεφάλαιο 4

Μετρήσεις και αποτελέσματα

"*The disincentive to replicate, the incentive to engage in questionable practices, and the inability to verify when the rare replication is done, combine to form what is often referred to as a replication crisis...*"

Pagell M., *Replication without repeating ourselves: Addressing thereplication crisis in operations and supply chainmanagement research*

Για να δείξουμε τις δυνατότητες της ρύθμισης μέτρησης σε αυτό το κεφάλαιο παρουσιάζονται τα αποτελέσματα μέτρησης για συγκεκριμένο εξοπλισμό. Το κεφάλαιο ξεκινά με μια σύντομη περίληψη του σκεπτικού οργάνωσης του έργου, την προοπτική τοποθέτησης μέτρησης και μια περιγραφή των συνθηκών δοκιμής σε σύγκριση, μαζί με τα τελικά αποτελέσματα.

4.1 Σχέδιο και συζήτηση της πρότασής μας

Σε σχέση με τα ίδη υπάρχοντα σχήματα αυθεντικοποίησης, υπάρχουν τρία κριτήρια που έχουν σημασία. Πρώτα, η δυνατότητα αποφυγής αποθήκευσης ευάλωτων στοιχείων στην απροστάτευτη μνήμη, μετά είναι η αξιοπιστεία του συστήματος σε ακραίες

περιβαλλοντικές συνθήκες, και τέλος, η ανθεκτηκότητα ενάντιας σε επιθέσεις μηχανικής μάθησης. Τα πειράματα παραγωγής κλειδιών με χρήση εγγενών χαρακτηριστικών χωρίς κώδικες διόρθωσης σφαλμάτων, προκειμένου να μειωθεί περαιτέρω το ποσοστό αποτυχίας οι ρυθμήσεις του BCH ιναοποιούσαν μέχι $t = 15$, στη δυαδική συμβολοσειρά λόγο περιοριμένης υπολογιτικής δύναμης του Arduino. Ένα άλλο ενδιαφέρον φαινομένο ήταν η βελτίωση των αποτελεσμάτων μετά τον καθαρισμό της μνήμης πρίν την λειτουργία αποσύνδεσης τροφοδοσίας, ωστόσο αυτή η παράμετρος δεν μελετήθηκε περεταίρω – το μόνο αρνητικό όμως είναι η καθυστέριση επανακκίνησης του κυκλωμάτος λόγω υπερφόρτωσης ενδιάμεσων διαδικασιών.

4.1.1 Στρατιγική υλοποίησης

Τα μη αντιγράψιμα συστήμα παράγουν μονδαδικές και μη-αντιγράψημες αποκρίσεις με βάση τις εγγενείς ιδιότητες του πυριτίου, για τις οποίες το ζεύγος εισόδου-εξόδου εξασφαλίζεται ότι η αλληλεπίδραση μεταξύ τους είναι εντελώς τυχαία και δύσκολα αντιγράψιμη. Υπάρχουν δύο σημαντικές έννοιες που σχετίζονται με την ασφάλεια, δηλαδή η αξιοπιστεία και ομοιομορφία, που ορίζεται ως η ισορροπία κατανομής δυαδικών τιμών(μηδέν ή άσσος), και για να εκπληρωθεί ευρωστία υψηλής εντροπίας πρέπει να παραμείνει όσο το δυνατό υψηλή. Ουδόλως η πρακτική αυτή περιορίζεται στην έρευση σταθερών κελιών, για ένα περιορισμένο εύρος αποκρίσεων οι κώδικές διόρθωσης αντιμετωπίζουν επαρκώς το ζήτημα αυτό. Εκτός από την ασφάλεια, οι μνήμες SRAM αναμένεται αναπόφευκτη σκάρτα συμπεριφορά του κυκλώματος (φαινομένο γήρανσης), η ελλατωματικότητα της πηγής έχει σαν αποτέλεσμα κυκλωματικών περιβαλλοντικών διακυμάνσεων, αλλά το υψηλό ποσοτό τυχαιότητας παραμένει ικανοποιητικό. Μεταξύ των συστημάτων διαχείρισης κλειδιών, η κατάσταση της εντροπίας έχοντας ικανοποιτικά ποσοστά όχι μόνο μπορεί να χρησιμοποιηθεί ως πηγή τυχαιότητας (seed) γεννητριών ψευδοτυχαίων αριθμών, αλλά και σαν οικονομική λύση παραμέτρων κρυπτογραφικών αλγορίθμων.

Αρχικά, με βάση τις προαναφερόμενες επιδιώξεις και με πλήρη συμμόρφωση με το πρότυπο [14], οι καθορισμένοι βραχυπρόθεσμοι στόχοι είναι πρώτων, η τυχαιότητα σε κάθε διάθασμα(γνωστό στην βιβλιογραφία ως challenge) να διαφέρει η τιμή εξόδου (ή response) με ίδιο κατασκευαστικά κυκλώματα – στη δική μας περίπτωση, η μνήμη τύπου SRAM. Δευτερεύον χαρακτηριστικό , μεταξύ άλλων, για μνήμες SRAM, η δειγματοληψία έχοντας προσκομίσει αποδείξεις σχετικά με την τυχαιότητα, τα σχετικά συμπεράσματα παρατίθενται λεπτομερέστατα στον κανόνα αξιοπιστίας του εσωτερικού περιβαλλοντικού συστήματός σε όρους ακρίβειας και ευαισθησίας. Κατόπιν

της αναθεώρησης των εν λόγω κριτήριων, καταλαβαίνουμε πως υπάρχει έλλειψη ομοιομορφίας στα εξεταζόμενα τσιπ. Στις περισσότερες περιπτώσεις, η επίθεση μοντελοποίησης μπορεί να επιτύχει σχεδόν πλήρες ακρίβεια με ένα μικρό αριθμό CRPs κάτω από ένα σταθερό περιβάλλον δοκιμών, ειδικά με τη βοήθεια της ενεργής μάθησης [118].

4.1.2 Συνθήκες και προοπτικές

Η ακαδημαϊκή μελέτη των φυσικών μη κλωνοποίησιμων συστημάτων αποτελεί βασικό θεμέλιο αποκλειστικά στον τομέα της ασφάλειας υλικού. Τέλος, η προσφεύγουσα σύνοψη υποστηρίζει, επίσης, ότι η καθείς εκτίμησης όσον αφορά τις περιβαλλοντικές συνθήκες και την ποιότητα των μεθόδων δειγματοληψίας για τη συνολική διαχείριση των συμπερασμάτων. Ο πίνακας που ακολουθεί παρέχει πληροφορίες των χαρακτηριστικά γνωρίσματα που καθορίζουν την ομοιομορφία των αποκρίσεων σε σχέση με τον θόρυβο.

Απόσταση Χάμινγκ επεξεργασμένων τιμών*	
[119]	12.7%
(Μετρήσεις μας)	10.8%

Table 4.1 Σύγκριση αποτελεσμάτων με 23LC1024. * Ποστοστό βελτίωσης απόστασης Χάμινγκ μετά την βελτίωσης σφαλμάτων με τον αλγόριθμο BCH.

Αφού εξετάσουμε το νέο σχέδιο επιλογής σταθερών κελιών, καταλήγουμε στο συμπέρασμα ότι για συγκεκριμένο εύρος αριθμό διόρθωσης, ο αλγόριθμος BCH, είναι αρκετά αποτελεσματικός, και τα αποτελέσματα ικανοποιητικά.

4.1.3 Η έννοια του προτεινόμενου μηχανισμού ασφαλείας

Η δικιά μας εισαγόμενη μέθοδος αποσκοπεί στην ανάλυση και την πειραματική επικύρωση της χρήσης λειτουργιών που βασίζονται σε κρυπτογραφικά πρωτόκολλα που αποτελούν αναπόσπαστο κομμάτι της ασφάλειας έξυπνων συσκευών με ελάχιστο κόστος όσον αφορά τους πόρους υλικού που απαιτούνται για την συνθήκη ελέγχων διασφαλίσεων μεταξύ των οντοτήτων.

4.1.4 Υποβάθμιση εντροπίας κατά την ανάκτηση των βοηθητικών δεδομένων

Τα βοηθητικά δεδομένα είναι απαραίτητη πληροφορία για την ορθή λειτουργία του ασφαλούς σχεδίου, και για την διαδικασία αναπαραγωγής του κλειδιού. Ωστόσο, λόγο της γραμμικής φύσεως των κωδικών διόρθωσης σφαλμάτων, τα βοηθητικά δεδομένα περιέχουν σχετικές πληροφορίες με την απόκριση του κυκλώματος. Ειδικότερα, εάν το υπόλοιπο της διαφοράς του μήκους προς την διάσταση της πολυώνυμής γεννήτριας, τότε η υπόλοιπη εντροπία είναι μηδέν. Με άλλα λόγια, πρωτόκολλα όπως του αντίστροφου ασαφούς εξαγωγής το αποτέλεσμα απόκρισης μεταφέρεται δημόσια [120] – οπότε παραλείποντας την σοβαρότητα της εντροπίας είναι μια θεωρητικού επιπέδου ευπάθεια, μολονότι η μείωση της εντροπίας δεν ισχύει μόνο για την ασφαλή κατασκευή σχεδίου, αλλά επηρεάζεται σε κάθε εφαρμογή όπου συστατικά αποκρίσεων είναι δημόσια πληροφορία.

4.1.5 Επιθέσεις ενάντιας μη-κλωνοποίησιμων πηγών

Οι μη-κλωνοποιήσιμες πηγές SRAM, βασίζονται σε συμβατικά πρωτεύοντα στοιχεία ασφάλειας για την διατήρηση του κλειδιού με ασφάλεια, όσο το τσιπ τροφοδοτείται με ρεύμα. Κατά συνέπεια, οποιαδήποτε δευτερεύοντα κανάλια ή ευπάθειες στον κρυπτογραφικού σχεδιασμού, αποτελούν απειλή για το μυστικό κλειδί που εξάγεται από τα εγγενή χαρακτηριστικά του κυκλώματος. Επιπλέον, δεδομένου ότι οι αποκρίσεις του συστήματος δεν συσχετίζονται άμεσα με το μυστικό κλειδί, τότε η μοντελοποίηση επιθέσεων των ισχυρών μη-αντιγράψιμων πηγών είναι αδύνατη, εφόσον βέβαια οι σχέσεις εισόδου-εξόδου είναι κρυφές. Ωστόσο, υπάρχουν και άλλοι τρόποι στην βιβλιογραφία, οι οποίοι εξαρτώνται από το επίπεδο πρόσβασης που έχει κάποιος στη συσκευή, εξαρτώνται από το επίπεδο πρόσβασης που έχει κάποιος στη συσκευή, πιο συγκεκριμένα όταν επιτραπεί το δικαίωμα εγγραφής στην SRAM τότε μπορούν να αξιοποιηθούν μοτίβα περιβαλλοντικών παραμέτρων, όπως είναι η θερμοκρασία αποκαλύπτοντας προτιμήσεις των ασύστολα μεταβαλλόμενων μπιτ. Ακόμα, με την τροποποίηση της θερμοκρασίας, ενδεχομένως κάποιες αποκρίσεις ή και κυψέλες να μην είναι σε διαθεσιμότητα, εφόσον το κύκλωμα λειτουργεί εκτός της περιοχής σχεδιασμού του. Άρα, με την μεταβολή της τάσης, ή και θερμοκρασίας επηρεάζει άμεσα την αστάθεια των μπιτ [75]. Μια άλλη τακτική με χρήση υπέρυθρου παρατηρώντας την λειτουργία εκκίνησης, μετρώντας έτσι σημαντικά κομμάτια μοτίβων της απόκρισης [121]. Επίσης, τα δεδομένα των περισσότερων SRAM δεν διαγράφονται αμέσως κατά την απενεργοποίηση,

αλλά παραμένουν αποθηκευμένα στα κελιά τους για ένα ορισμένο σύντομο χρονικό διάστημα μετά την απενεργοποίηση της μνήμης – μόνη λύση σε αυτό το πρόβλημα είναι η χρήση ασφαλούς διαγραφής δεδομένων από τη στερεάς κατάστασης μνήμη [122]. Στο χαμηλότερο επίπεδο υλοποίησης, διερευνώνται οι αριθμητικοί υπολογισμοί, μολονότι είναι δύσκολο να προσδιοριστεί λύση σε ευρύ πεδίο εφαρμογής. Ως εκ τούτου, διερευνώνται τα επιμέρους συστατικά και ενδιάμεσα συστατικά της συνολικής αρχιτεκτονικής.

Μια πληθώρα επιθέσεων έχει αναφερθεί στη βιβλιογραφία, όπου οι περισσότερες είναι εξειδικευμένες για συγκεκριμένα αρχιτεκτονική μη-αντιγράψιμων πηγών. Ορισμένες δημοφιλείς επιθέσεις περιλαμβάνουν επιθέσεις μοντελοποίησης, επιθέσεις σφάλματος, και άλλα σχήματα τα οποία χρησιμοποιούνται για ισχυρές μη αντιγράψημες πηγές, γιατί η άλλη κλάση μη κλωνοποίησιμων πηγών έχει περιορισμένο αριθμό αποκρίσεων. Οι επιθέσεις μπορούν γενικά να ταξινομηθούν σε επεμβατικές, μισο-επεμβατικές και μη επεμβατικές. Οι επιθέσεις τύπου ενεργής παρέμβασης εκμεταλλεύονται και τροποποιώντας τη δομή του κυκλώματος – οπότε η υλοποίηση είναι σχετικά δύσκολη και χρονοβόρα. Αντιθέτως, στις μισο-επεμβατικές επιθέσεις εκμεταλλεύονται την πρακτικότητα των εξωτερικών φυσικών προβλημάτων, τα οποία μειώνουν την αποδοτικότητα ενός κυκλώματος, και ταυτόχρονα με στατιστική σχετικότητα μπορούν να οδηγήσουν σε κάποια συμπεράσματα. Οι επιθέσεις χρησιμοποιούν την εγγενή θορυβώδη αστάθεια στις αποκρίσεις, όπως είναι η αντίδραση σε άλλη περιβαλλοντικές συνθήκες θερμοκρασίας. Τέλος, στις μη-επεμβατικές επιθέσεις βασίζονται στην φιλοσοφία είτε των επιθέσεων με μηχανική μάθηση, είτε επιθέσεις πλάγιου μονοπατιού(side-channel attacks), και χρησιμοποιούνται για εκτεταμένες δοκιμές στην δομή του πρωτόκολλο ασφαλείας που έχει υλοποιηθεί και τυχόν λανθασμένες διαμορφώσεις του. Εργαλεία ανοικτού κώδικα και για τα τρία είδη υπάρχουν διαθέσιμα, αλλά για τις μετρήσεις μας χρησιμοποιήθηκε η βιβλιοθήκη pypuf [123, 124], και [125].

4.2 Μοντέλα υλοποιησης

Οι αλγόριθμοι μηχανικής μάθησης χρησιμοποιούνται στο σχεδιασμό μοντέλων μακροπρόθεσμων και βραχυπρόθεσμων προβλέψεων, και με αυτή την λογική πραγματοποιείται δυναμικός έλεγχος των εγγενών χαρακτηριστικών, με σύνολο δεδομένων ένα μικρό μέρος του πραγματικού δείγματος ή ενός τυχαίου. Η θεμελιώδες αρχή των επιθέσεων μηχανικής μάθησης βασίζεται στη λογική την πρόβλεψη μοτίβου απόκρισης, και η μάθηση γίνεται με δύο τρόπους. Το μοντέλο μπορεί να υλοποιηθεί με

ένα σύνολο δεδομένων μεγέθους δέκα χιλιάδων τυχαίων τιμών μήκους 128 μπιτ. Το μέγεθος των δεδομένων εκπαίδευσης συνήθως σχετίζεται με την ακρίβεια του μοντέλου πρόβλεψης, δηλαδή όσο μεγαλύτερο είναι το σύνολο δεδομένων που συλλέγονται, τόσο μεγαλύτερη είναι η ακρίβεια πρόβλεψης. Όσον αφορά την μεθοδολογία της επίθεσης, αρχικά με ψευδοτυχαίο τρόπο ανακατεύεται το σύνολο δεδομένων μάθησης, και ο διαχωρισμός το σύνολο κατάρτισης καταλαμβάνει το εβδομήντα τις εκατό, σε αντίθεση με το υπόλοιπο τριάντα του συνόλου δοκιμών από συνολικά δείγματα μήκους δέκα χιλιάδων τιμών. Μετά την εκπαίδευση του μοντέλου στο παρεχόμενο σύνολο δεδομένων, δοκιμάζεται για επικύρωση σε άγνωστα δεδομένα που έχουν ανακατευτεί τυχαία με βάση ένα σπόρο(seed) της τρέχουσας χρονικής σήμανσης. Στις παρακάτω υποενότητες γίνεται αναφορά στα μοντέλα μηχανικής μάθησης που χρησιμοποιήθηκαν για τον πειραματισμό επιθέσεων σε μη ισορροπημένα δεδομένα, και κλείνει με τα αποτελέσματα.

4.2.1 Αλγόριθμος Μηχανών Υποστίριξης Διανυσμάτων (Support Vector Machine)

Ένας διαδεδομένος αλγόριθμος μηχανικής μάθησης είναι ο αλγόριθμος Μηχανών Υποστίριξης Διανυσμάτων (Support Vector Machine), για τον οποίο η δημοφιλότητά του οφείλεται στην υψηλή απόδοση σε μικρές έως μεσαίες σειρές δεδομένων ταξινόμησης. Ωστόσο η απόδοση είναι χαμηλότερη όταν εφαρμόζεται σε πολύ μεγάλα σύνολα δεδομένων, καθώς οι μαθηματικοί υπολογισμοί αυξάνονται. Ο αλγόριθμος διαχωρίζει δυο κλάσεις αναλόγως κάποια κριτήρια, τα οποία ταξηνομούν τα πλησιέστερα σημεία μεταξύ των τάξεων σε ένα διαχωριστικό υπερπλάνο. Η εκμάθηση των κοντινότερων σημείων στο αεροπλάνο (βοηθητικά διανύσματα), επηρεάζονται άμμεσα από τις αλλαγές των εσωτερικών λειτουριών χαρτογράφησης(πυρήνες). Το καταλληλότερο σχήμα πυρήνα για ανίχνευση δυαδικών μοτίβων είναι η λειτουργία ακτινικής βάσης(radial basis function), και σε αυτή την περίπτωση σκιαγραφίζονται μη γραμμικά δείγματα σε μεγαλήτερες διαστάσεις και έτσι αξιολογείται μια σχέση μεταξύ των καρτελών τάξης(labels) [126].

4.2.2 Λογιστική παλινδρόμηση (Logistic Regression)

Η λογική του προγνωστικού μοντέλου λογιστικής παλινδρόμησης (Logistic Regression) υποστηρίζει ένα σύνολο δεδομένων που οι τιμές μπορούν να είναι μηδέν ή ένα, το οποίο προσδιορίζει μια δυαδική σειρά ποσοτικοποιόντας τη σχέση μεταξύ

της διχοτόμου εξαρτώμενης μεταβλητής και των αναμενόμενων ζευγαριών που χρησιμοποιούν αναλογικές τιμές. Σε αυτή τη μελέτη η αναλογία αποδόσεων είναι η πιθανότητα ότι η τιμή του δυαδικού μοτίβου θα εκτιμάται σε σχέση όλης της σειράς, διαιρούμενη με την πιθανότητα ότι η τιμή της δυαδικού μοτίβου δεν θα εκτιμήσει στην σειρά [127].

4.2.3 Δέντρα απόφασης (Decision Tree)

Τα μοντέλα δέντρων απόφασης (Decision Tree) δεν βασίζονται σε μη πεπερασμένες τακτικές, ωστόσο είναι ικανά να αντιμετωπίσουν πιο σύνθετα μη γραμμικά πρότυπα και αλληλεπιδράσεις χαρακτηριστικών χάρις την κατασκευή ενός δέντρου, για οποίο οι μεταβλητές εισόδου αντιπροσωπεύονται στα κλαδιά και οι τιμές εξόδου στα φύλλα αντίστοιχα, και ο αλγόριθμος απόφασης επιλέγει ένα χαρακτηριστικό σε κάθε βήμα που δίνει την καλύτερη διάσπαση του συνόλου δεδομένων, σε σχέση με τις αλλαγές των μεταβλητών. Το κέρδος χαρακτηριστικών, υπολογίζεται από το υπόλοιπο των κόμβων μείον το επιβαρημένο άθροισμα των υπολοίπων των δύο νέων παιδιών που θα δημιουργηθούν από τη διάσπαση.που θα δημιουργηθούν από τη διάσπαση. [128].

4.2.4 Τυχαία δάση (Random Forest)

Τα Τυχαία Δάση(Random Forest) είναι ένας αλγόριθμος που βασίζεται στα δέντρα απόφασης 4.2.3, όπου το δέντρο απόφασης αποτελεί ένα ένα κατευθυνόμενο γράφημα, και κάθε διαδρομή είναι διαχωρισμένη σε κλάδους, αναλόγος κάποιους κανόνες απόφασης για την χαρτογράφηση του επιθυμιτού αποτελέσματος. Η αρχιτεκτονική ενός δέντρου απόφασης εξαρτάται κυρίως από τα δεδομένα εκπαίδευσης, τα οποία οριστηκοποιούν τους κανόνες απόφασης και το μονοπάτι των κλάδων – αλλά υπό την υπόθεση ότι κάποιες τυχαίες τιμές των κατασκευασμένων δέντρων αποφάσεων, μπορεί να είναι ικανά για καλύτερη πρόβλεψη από την διαδικασία της εκλογής της οντότητας με μικρότερη τιμή [129].

4.2.5 Κ-κοντινότεροι γείτονες(K-Nearest Neighbors)

Οι κ-κοντινότεροι γείτονες (K-Nearest Neighbors), αποτελούν έναν αλγόριθμο εκμάθησης που ταξινομεί νέες περιπτώσεις με βάση κάποια μέτρα ομοιότητας και χρησιμοποειίται για την ανύχνευση όλων των διαθέσιμων περιπτώσεων με βάση τον τρόπο ταξινόμησης

των γειτόνων δεδομένων. Ένα πλεονέκτημα του αλγορίθμου είναι η ανίχνευση μοτίβων ή στατιστικών φαινομένων, δηλαδή τα δεδομένα ταξυνομούνται με βάση τον τρόπο ταξινόμησης των γειτόνων του [130].

4.2.6 Ταξινομητής Μπέυζ (Bayes Classifier)

Ο Ταξινομητής Μπέυζ (Bayes Classifier) από την άλλη πλευρά, είναι ένας πιθανοτικός ταξινομητής που βασίζεται στο θεώρημα του Μπέυζ. Ο αλγόριθμος είναι αρκετά αποτελεσματικός όταν τα δεδομένα ταξινόμησης έχουν συγκεκριμένα χαρακτηριστικά, καθώς οι πιθανότητες χαρακτηριστικών προσδιορίζονται εύκολα μετρώντας απλώς την εμφάνηση τους, στο σύνολο εκπαίδευσης – η πρόβλεψη γίνεται αφότου η αναδρομική υπόθεση του συνόλου δεδομένων αποδείξει την ταξινόμηση μέγιστης πιθανότητας, που συχνά αναφέρεται ως μέγιστη εκ των υστέρων [131].

4.2.7 Απόδοση μοντέλων

Η απόδοση των μοντέλων μηχανικής μάθησης αναλύεται εκπαιδεύοντάς το σε διαφορετικών μεγεθών εκπαίδευσης που κυμαίνονται σε 70% και 80% του συνόλου δεδομένων, και το σύνολο δεδομένων απαρτίζεται μόνο από αποκρίσεις (challenge). Στον συνοπτικό πίνακα αποτελεσμάτων παρατηρούμε ότι η πρόβλεψη μοτίβου σε μια σείρα με υψηλή εντροπία είναι δύσκολο έργο, και η χαμηλή ακρίβεια σχετίζεται άμεσα με τον αριθμό των κλάσεων.

Μοντέλο μηχανικής μάθησης	Ακρίβεια δεδομένων εκπαίδευσης	Ακρίβεια δεδομένων ελέγχου
Support Vector Machines	15%	14%
K-Nearest Neighbors	18%	13%
Random Forest	14%	12%
Logistic Regression	15%	12%
Decision Tree	5%	8%
Bayes Classifier	12%	15%

Table 4.2 Αποτελέσματα επιθέσεων μηχανικής μάθησης σε σύνολο δεδομένων δέκα χιλιάδων τιμών.

Κεφάλαιο 5

Αναφορά αποτελεσμάτων

> "*The late majority adopt new ideas just after the average member of a social system. Adoption may be both an economic necessity and the answer to increasing network pressures.*"
>
> Everett M., *Diffusion of Innovations.*

Η διατριβή αυτή αποσκοπεί σε μια επισκόπηση των τρεχουσών μεθόδων που χρησιμοποιούνται στον τομέα των μη-αντιγράψιμων στις ενσωματομένες συσκευές και στον καθορισμό ορισμένων ενδιαφέρον προβληματισμών για περαιτέρω έρευνα. Στα πρώτα κεφάλαια εισήχθη το θεωρητικό υπόβαθρο και τρόποι αξιολόγησης, στην συνέχεια τα ποιοτικά χαρακτηριστικά των πειραμάτων οργανώθηκαν και σχολιάστηκαν. Στο τελευταία κεφάλαια γίνεται μια γενική σύνοψη όλων των παραπάνω, η γνώση που αποκτήθηκε και κλείνει με την επισήμανση των μελλοντικών δυνατοτήτων του έργου.

5.0.1 Συμπεράσματα μελέτης

Σε γενικές γραμμές, υπάρχουν τρεις κύριες συνεισφορές της παρούσας διατριβής. Αρχικά, η εξερεύνηση των εγγενών χαρακτηριστικών μνημών τύπου SRAM, ως προς την τυχαιότητα και μοναδικότητα. Μελετήθηκε ο τρόπος με τον οποίο παράγεται η υψηλή εντροπία σε αποκρίσεις μιας μνήμης SRAM. Αξιολογήθηκαν δύο μέθοδοι εξαγωγής

τυχαιότητας, πρώτα με σειριακή ανάγνωση χωρίς επεξεργασία, και μετά με αλγόριθμο εύρεσης σταθερών κελιών έχοντας μια προ-απαιτούμενη κλίμακα αξιολόγησης. Όμως οι τυχαίοι αριθμοί που εξάγονται με αυτόν τον τρόπο είναι προκατειλημμένοι ανάλογα με την τροφοδοσία λειτουργίας του κυκλώματος, και δραματική βελτίωση παρατηρήθηκε σε σχετική δειγματοληψία. Έπειτα, τονίστηκε η θεμελιώδες αρχή των κωδικών διόρθωσης σφαλμάτων, περιεγράφηκαν και δοκιμάστηκαν επιθέσεις τεχνικής νοημοσύνης, κλείνοντας με συζήτηση μεταξύ των προβληματισμών μας. Συνεπώς, τα μη κλωνοποίησημα συστήματα δεν είναι πανάκεια για όλες τις πτυχές μοντέλων εκτίμησης απειλών, αλλά σε συστήνεται η εφαρμογή του υπό κάποιες συνθήκες. Σε καμία περίπτωση δεν προτείνεται η χρήση μη-αντιγράψιμων πηγών τύπου SRAM σε στρατιωτικό ή ιατρικό εξοπλισμό, αντίθετα η συσκευή μπορεί να χρησιμοποιεί για την αποθήκευση κλειδιών με ασφάλεια, χωρίς βέβαια να είναι εκτεθημένη. Όπως είδαμε προηγούμενος, η σταθερότητα μνήμων τύπου SRAM πετυχαίνετε με προ-επεξεργασία των εγγενών αποκρίσεων.

5.1 Μελλοντική έρευνα

Αφού με λεπτομέρεια αναφερθήκαμε στα αποτελέσματα της εργασίας, σκόπιμο είναι να παραχωρηθούν οι νέες ιδέες και προβληματισμοί που προέκυψαν. Πρώτον, ενδελεχής ανάλυση κυκλώματος με αποδοτικές γεννήτριες ψευδοτυχαίας συσχέτισης [132, 133], συνοδευόμενο με μοντέρνες εκδώσεις κρυπτανάλυσης [134], και κατάλληλους κρυπτογραφικούς αλγόριθμους για ενσωματωμένες συσκευές και βελτίωσης ασφαλείας βοηθητικών δεδομένων [135, 136], αποτελούν προκλήσεις οι οποίες όχι μόνο έχουν κεντρίσει το ενδιαφέρον μας, αλλά ένα μεγάλο εύρος ερευνητικών και εμπορικών δυνατοτήτων, χάρις την επάνδρωση του πληροφοριακού συστήματος. Δεύτερον, στην ερευνητική κοινότητα υπάρχουν πολλές ενδόμυχες σκέψεις και προκαταλήψεις σχετικά με την εξασφάλιση αξιοπιστίας και ανθεκτικότητας των μη-αντιγράψιμων πηγών, πράγμα που υπόκειται σε μέτρα αξιολόγησης, για παράδειγμα το φαινόμενο της γήρανσης έχει αμφισβητήσει ο τρόπος μέτρησης, είτε έχει δοκιμαστεί σε περιορισμένα είδη συσκευών, είτε έχει γίνει ανάλυση βασισμένη σε σύστημα μοντελοποίησης. Άρα, η περίπλοκη του ζητήματος καθιστά ευεπίφορη σε συγχύσεως μεταξύ των αρθρογράφων, και μια πρακτική λύση μπορούσε να είναι η κοινή συνεισφορά αποτελεσμάτων σε κοινόχρηστο σύστημα για λόγους διαφάνειας. Τρίτον, η ενσωμάτωση των μη-αντιγράψιμων πηγών στην εξωτική έννοια της ομομορφικής κρυπτογραφίας έχει ενσαρκωθεί σε αρχιτεκτονικές απόδειξης χωρίς προηγούμενη γνώση (zero-knowledge-proofs), η εν λόγω εφεύρεση

παραμερίζεται σε θέματα ασφαλείας παραβίασης δεδομένων ανταλλαγής ευπαθών παραμέτρων – το σχήμα zk SNARK αντιμετωπίζει αυτά τα προβλήματα έχοντας κρυπτογραμένη πληροφορία μεταξύ του επαληθευτή και τη προοριζόμενη οντότητα [137]. Τέταρτον, τα τελευταία χρόνια έχουν γίνει πολλές προσπάθειας για την διαχείριση κόστος αποθήκευσης και αποθήκευσης αρχείων, ωστόσο η επερχόμενη λύση σε αυτό το πρόβλημα είναι το πρωτόκολλο IPFS, το οποίο βασίζεται σε κατανεμημένη διαχείριση κατακερματισμένων οντοτήτων, πάνω στην τεχνολογία Blockchain [138]. Αυτή η πλατφόρμα έχει πρόσφατα προταθεί για χρήση σε αμυντικές εφαρμογές [139], ως εκ τούτου οι δυνατότητες του μπορούν να εκμεταλλευτούν σε κρυπτογραφικά συστηματικά υψηλής ακρίβειας – σε συνδυασμό με τα μη-αντιγράψιμα συστήματα, η κατανεμημένη διαχείριση δημόσιων δεδομένων, όπως είναι τα δημόσια κλειδιά ασυμμετρικής κρυπτογράφησης ή βοηθητικών δεδομένων για την κατασκευή κλειδιών, μπορούν να τοποθετηθούν αλώβητα σε ένα ανοικτό αποκεντρωμένο δίκτυο.

5.1.1 Τεχνικά εμπόδια

Δεδομένου του καινοφανή χαρακτήρα στον κλάδο των μη-αντιγράψιμων συναρτήσεων, είναι θεμιτό θεωρητικές έννοιες να αλλάζουν ασύστολα ανάλογα το είδος εξοπλισμού και ευρηματικότητας. Μολονότι η περιεκτικότητα των δωρεάν διαθέσιμων πόρων της κοινότητας του Arduino, επικαλύπτει όλες τις βασικές πτυχές ανάπτυξης ενός ερασιτεχνικού έργου ενσωματωμένων συσκευών, η ορθότητα των πηγών σε εξεζητημένες εμπορικές συσκευές, όπως είναι οι μνήμες SRAM, είτε υπάρχουν προβλήματα στις βιβλιοθήκες ανοικτού κώδικα, είτε δεν είναι ολοκληρωμένες. Τα μεγαλύτερα ζητήματα σχετίζονται με τα πνευματικά δικαιώματα και ζητήματα ασφαλείας του ανοικτού κώδικα σχετικών ιστότοπων (ερωτήσεων και απαντήσεων) [140]. Λόγω των περιστάσεων, ελλοχεύει ο κίνδυνος στη σχετική βιβλιογραφία την λανθάνουσας ή ελλείπεις σύγκρισης με τα ήδη υπάρχοντα ευρήματα άλλων ερευνητών.

Χαρακτηριστικό πρόβλημα στην σχετική επιστημονική κοινότητα είναι η αποφυγή, ή και συσκότιση λάθος, πριν τα τελικά αποτελέσματα, μειώνοντας την αναφορά διαδικασίας σκέψεις – που σε καμία περίπτωση δεν είναι αλάνθαστη. Στην πραγματικότητα, οι ερευνητές όχι μόνο έχουν συστηματικά, αποτυχίες, αλλά αυτά βοήθησαν στην εκπλήρωση στόχων. Σε αυτή την εργασία, ένα από τα σημαντικότερα λάθη ήταν ο τρόπος δειγματοληψίας, για δύο λόγους. Αρχικά η συλλογή απόκρισης εκτός ότι πρέπει να γίνει σε ένα εύλογο χρονικό διάστημα, η καλύτερη κατανόηση των συστάδων αναλύονται ακριβέστερα όταν διαχωριστούν τα σταθερά κελία. Επίσης, οι πειραματισμοί χωρίζονται είτε σε δυαδικά δεδομένα (δηλαδή, μηδέν και ένα),

ή σε μπιτοσειρές (0 μέχρι 255) – με όλο τον σεβασμό, σε πολλές διπλωματικές εργασίες, αρκετοί φοιτητές απέρριψαν την επεξήγηση ή προσδιορισμό αυτή της σημείωσης δημιουργώντας έτσι μια συνήχηση στον αναγνώστη. Ένα άλλο πρόβλημα που παρατηρήθηκε στην σχετική βιβλιογραφία, ήταν πως σε μεγάλο βαθμό πολλοί ερευνητές και αρθρογράφοι, παρέλειπαν τον προσδιορισμό εμποδίων στην υλοποίησή (για αποφυγή ανακύκλωσης), καθώς η έλλειψη αποτυχιών είναι σχεδόν αδύνατη.

5.1.2 Συστάσεις και συμβουλές

Η παρουσία των πολυσχιδή προκλήσεων αποτελεί ταυτόχρονα, αποθάρρυνση στους μελλοντικούς αναγνώστες, και ρηξικέλευθο βήμα δημιουργίας κατάλληλης στρατηγικής. Το προτεινόμενο πλάνο οργάνωσης σχετικής έρευνας είναι αρχικά ο ορισμός του κυκλώματος μη-αντιγράψιμων πηγών, η επιλογή ποικίλη σε σκαπανέες μεθοδολογίες και αλγορίθμους προς υλοποίησή. Ιδιαίτερη προσοχή χρειάζεται στον τρόπο αξιολόγησης του διαλεγμένου συστήματος, καθώς η εκλεκτικότητα είναι ζωτικής σημασίας για την απόδειξη των αποτελεσμάτων. Ένα άλλο ποιητικό χαρακτηριστικό διεξαγωγής έρευνας είναι η δομή της αναφοράς και παρουσίασης των ευρημάτων – υπάρχει πακτωλό βιβλιογραφίας στο ζητήματα αυτό [141, 142]. Μια άλλη τεχνική φύσεως παρατήρηση είναι το μέγεθος και μήκος της δειγματοληψίας, γιατί στην απόσταση Χάμινγκ το μήκος της δυαδικής λέξης να είναι ίδιο, και οι στατιστικές σουίτες που χρησιμοποιήθηκαν είχαν διαφορετικές ιδιοτροπίες μεταξύ τους – κάθε πλατφόρμα ανάλυσης έχει χτιστεί με διαφορετική γλώσσα προγραμματισμού, δηλαδή C, C++, και άλλες, οπότε το όριο κάθε μεταβλητής αλλάζει κάθε φορά.

Αναφορές

[1] N. A. Christakis, *Apollo's Arrow: The Profound and Enduring Impact of Coronavirus on the Way We Live*. Little, Brown Spark, 2020.

[2] K. Ishibashi and K. Osada, *Low power and reliable SRAM memory cell and array design*, vol. 31. Springer Science & Business Media, 2011.

[3] R. Lidl and H. Niederreiter, *Finite fields*. No. 20, Cambridge university press, 1997.

[4] T. K. Moon, *Error correction coding: mathematical methods and algorithms*. John Wiley & Sons, 2020.

[5] J. Kelsey and E. Barker, "Recommendation for random number generation using deterministic random bit generators," *NIST, Gaithersburg, MD, USA, Tech. Rep. SP*, 2015.

[6] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security*, pp. 3–37, Springer, 2010.

[7] M. S. Turan, E. Barker, J. Kelsey, K. A. McKay, M. L. Baish, and M. Boyle, "Recommendation for the entropy sources used for random bit generation," *NIST Special Publication*, vol. 800, no. 90B, 2018.

[8] M. Faundez-Zanuy, "On the vulnerability of biometric security systems," *IEEE Aerospace and Electronic Systems Magazine*, vol. 19, no. 6, pp. 3–8, 2004.

[9] D. Bauder, "An anti-counterfeiting concept for currency systems," *Sandia National Labs, Albuquerque, NM, Tech. Rep. PTK-11990*, 1983.

[10] G. J. Simmons, "Identification of data, devices, documents and individuals," in *Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on Security technology*, pp. 197–218, IEEE, 1991.

[11] R. Pappu, "Physical one-way functions: Phd thesis in media arts and sciences," 2001.

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

[13] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "A puf taxonomy," *Applied Physics Reviews*, vol. 6, no. 1, p. 011303, 2019.

[14] I. ISO, "Information security, cybersecurity and privacy protection — physically unclonable functions — part 1: Security requirements," *International Standard*, 2020. https://www.iso.org/standard/76353.html, visited 2020-12-09.

[15] D. E. Holcomb, W. P. Burleson, K. Fu, *et al.*, "Initial sram state as a fingerprint and source of true random numbers for rfid tags," in *Proceedings of the Conference on RFID Security*, vol. 7, p. 01, 2007.

[16] M. Cortez, A. Dargar, S. Hamdioui, and G.-J. Schrijen, "Modeling sram start-up behavior for physical unclonable functions," in *2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, pp. 1–6, IEEE, 2012.

[17] R. Maes, P. Tuyls, and I. Verbauwhede, "A soft decision helper data algorithm for sram pufs," in *2009 IEEE international symposium on information theory*, pp. 2101–2105, IEEE, 2009.

[18] M. Hofer and C. Boehm, "An alternative to error correction for sram-like pufs," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 335–350, Springer, Berlin, Heidelberg, 2010.

[19] R. Maes, P. Tuyls, and I. Verbauwhede, "Low-overhead implementation of a soft decision helper data algorithm for sram pufs," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 332–347, Springer, 2009.

[20] S. Eiroa, J. Castro, M. C. Martínez-Rodríguez, E. Tena, P. Brox, and I. Baturone, "Reducing bit flipping problems in sram physical unclonable functions for chip identification," in *2012 19th IEEE International Conference on Electronics, Circuits, and Systems (ICECS 2012)*, pp. 392–395, IEEE, 2012.

[21] A. Hosey, M. T. Rahman, K. Xiao, D. Forte, and M. Tehranipoor, "Advanced analysis of cell stability for reliable sram pufs," in *2014 IEEE 23rd Asian Test Symposium*, pp. 348–353, IEEE, 2014.

[22] A. Narayanan and E. W. Felten, "No silver bullet: De-identification still doesn't work," *White Paper*, pp. 1–8, 2014.

[23] W. Hu, C. H. Chang, A. Sengupta, S. Bhunia, R. Kastner, and H. Li, "An overview of hardware security and trust: Threats, countermeasures and design tools," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, pp. 1–1, 2020.

[24] J. Delvaux, "Security analysis of puf-based key generation and entity authentication," *Ph. D. dissertation*, 2017.

[25] H. Balinsky, S. J. Simske, and D. S. Perez, "Data leak prevention systems and methods," Dec. 22 2015. https://lens.org/017-826-417-715-81X, visited 2021-03-07.

[26] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "Emerging physical unclonable functions with nanotechnology," *IEEE access*, vol. 4, pp. 61–80, 2016.

[27] B. Halak, "Authentication of embedded devices," 2021.

[28] S. Ghosh, M. Zaman, G. Sakauye, and S. Sampalli, "An intrusion resistant scada framework based on quantum and post-quantum scheme," *Applied Sciences*, vol. 11, no. 5, p. 2082, 2021.

[29] H. Weng, C. Zhang, P. Chen, R. Chen, J. Xu, Y. Liao, Z. Liang, D. Shen, L. Zhou, and J. Ke, "A quantum chaotic image cryptosystem and its application in iot secure communication," *IEEE Access*, vol. 9, pp. 20481–20492, 2021.

[30] P. Campisi, *Security and privacy in biometrics*, vol. 24. Springer, 2013.

[31] A. K. Jain, R. Bolle, and S. Pankanti, *Biometrics: personal identification in networked society*, vol. 479. Springer Science & Business Media, 2006.

[32] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "Stealing keys from pcs using a radio: Cheap electromagnetic attacks on windowed exponentiation," in *International workshop on cryptographic hardware and embedded systems*, pp. 207–228, Springer, 2015.

[33] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?," in *Proceedings of the 3rd ACM workshop on Cloud computing security workshop*, pp. 113–124, 2011.

[34] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby, "A pseudorandom generator from any one-way function," *SIAM Journal on Computing*, vol. 28, no. 4, pp. 1364–1396, 1999.

[35] C. E. Shannon, "A mathematical theory of communication," *The Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.

[36] R. Hamming, "Error detecting and error correcting codes bell syst," 1950.

[37] I. S. Reed, "A class of multiple-error-correcting codes and the decoding scheme," tech. rep., Massachusetts Inst of Tech Lexington Lincoln Lab, 1953.

[38] D. E. Muller, "Application of boolean algebra to switching circuit design and to error detection," *Transactions of the IRE professional group on electronic computers*, no. 3, pp. 6–12, 1954.

[39] A. Rényi *et al.*, "On measures of entropy and information," in *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*, The Regents of the University of California, 1961.

[40] T. M. Cover and J. A. Thomas, *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. 2006.

[41] R. W. Hamming, "Error detecting and error correcting codes," *The Bell system technical journal*, vol. 29, no. 2, pp. 147–160, 1950.

[42] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *International conference on the theory and applications of cryptographic techniques*, pp. 523–540, Springer, 2004.

[43] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. Nickel, C. Donahue, and C. G. Peterson, "Fast, efficient error reconciliation for quantum cryptography," *Physical Review A*, vol. 67, no. 5, p. 052303, 2003.

[44] Q. Li, Y. Sutcu, and N. Memon, "Secure sketch for biometric templates," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 99–113, Springer, Berlin, Heidelberg, 2006.

[45] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric templates with sketch: Theory and practice," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 503–512, 2007.

[46] J. Bringer, H. Chabanne, and B. Kindarji, "The best of both worlds: Applying secure sketches to cancelable biometrics," *Science of Computer Programming*, vol. 74, no. 1-2, pp. 43–51, 2008.

[47] A. K. Jain and K. Nandakumar, "Biometric authentication: System security and user privacy.," *IEEE Computer*, vol. 45, no. 11, pp. 87–92, 2012.

[48] Q. Li and E.-C. Chang, "Robust, short and sensitive authentication tags using secure sketch," in *Proceedings of the 8th workshop on Multimedia and security*, pp. 56–61, 2006.

[49] Y. Sutcu, Q. Li, and N. Memon, "How to protect biometric templates," in *Security, Steganography, and Watermarking of Multimedia Contents IX*, vol. 6505, p. 650514, International Society for Optics and Photonics, 2007.

[50] M. Zhang, J. Zhang, and W.-R. Tan, "A secure sketch-based authentication scheme for telecare medicine information systems.," *J. Inf. Sci. Eng.*, vol. 32, no. 2, pp. 389–402, 2016.

[51] T. Scheidat, C. Vielhauer, and J. Dittmann, "Biometric hash generation and user authentication based on handwriting using secure sketches," in *2009 Proceedings of 6th International Symposium on Image and Signal Processing and Analysis*, pp. 89–94, IEEE, 2009.

[52] P. H. Nguyen, D. P. Sahoo, C. Jin, K. Mahmood, U. Rührmair, and M. van Dijk, "The interpose puf: Secure puf design against state-of-the-art machine learning attacks," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 243–290, 2019.

[53] A. S. Patil, R. Hamza, H. Yan, A. Hassan, and J. Li, "Blockchain-puf-based secure authentication protocol for internet of things," in *International Conference on Algorithms and Architectures for Parallel Processing*, pp. 331–338, Springer, 2019.

[54] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "Pmsec: Physical unclonable function-based robust and lightweight authentication in the internet of medical things," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 388–397, 2019.

[55] E. Mattox, "Medical devices and patient safety," *Critical care nurse*, vol. 32, no. 4, pp. 60–68, 2012.

[56] J. U. Obogo, "Security and privacy challenges in healthcare iot devices for patient treatment and monitoring," 2020.

[57] N. V. Boulgouris, K. N. Plataniotis, and E. Micheli-Tzanakou, *Biometrics: theory, methods, and applications*, vol. 9. John Wiley & Sons, 2009.

[58] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*. Springer Science & Business Media, 2009.

[59] I. Buhan, J. Doumen, P. Hartel, and R. Veldhuis, "Fuzzy extractors for continuous distributions," in *Proceedings of the 2nd ACM symposium on Information, computer and communications security*, pp. 353–355, 2007.

[60] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "Fpga intrinsic pufs and their use for ip protection," in *International workshop on cryptographic hardware and embedded systems*, pp. 63–80, Springer, 2007.

[61] R. Maes, A. Van Herrewege, and I. Verbauwhede, "Pufky: A fully functional puf-based cryptographic key generator," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 302–319, Springer, 2012.

[62] C. BÖSCH, J. Guajardo, A.-R. Sadeghi, J. Shokrollahi, and P. Tuyls, "Efficient helper data key extractor on fpgas," in *International workshop on cryptographic hardware and embedded systems*, pp. 181–197, Springer, 2008.

[63] M. Hiller, D. Merli, F. Stumpf, and G. Sigl, "Complementary ibs: Application specific error correction for pufs," in *2012 IEEE International Symposium on Hardware-Oriented Security and Trust*, pp. 1–6, IEEE, 2012.

[64] V. Van der Leest, B. Preneel, and E. Van der Sluis, "Soft decision error correction for compact memory-based pufs using a single enrollment," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 268–282, Springer, 2012.

[65] M.-D. Yu, R. Sowell, A. Singh, D. M'Raïhi, and S. Devadas, "Performance metrics and empirical results of a puf cryptographic key generation asic," in *2012 IEEE International Symposium on Hardware-Oriented Security and Trust*, pp. 108–115, IEEE, 2012.

[66] M.-D. Yu and S. Devadas, "Secure and robust error correction for physical unclonable functions," *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 48–65, 2010.

[67] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proceedings of the 6th ACM conference on Computer and communications security*, pp. 28–36, 1999.

[68] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes and Cryptography*, vol. 38, no. 2, pp. 237–257, 2006.

[69] M. Hiller, L. Kürzinger, and G. Sigl, "Review of error correction for pufs and evaluation on state-of-the-art fpgas," *Journal of Cryptographic Engineering*, vol. 10, pp. 229–247, 2020.

[70] S. Puchinger, S. Müelich, M. Bossert, M. Hiller, and G. Sigl, "On error correction for physical unclonable functions," in *SCC 2015; 10th International ITG Conference on Systems, Communications and Coding*, pp. 1–6, VDE, 2015.

[71] Z. Paral and S. Devadas, "Reliable and efficient puf-based key generation using pattern matching," in *2011 IEEE international symposium on hardware-oriented security and trust*, pp. 128–133, IEEE, 2011.

[72] P. A. Layman, S. Chaudhry, J. G. Norman, and J. R. Thomson, "Electronic fingerprinting of semiconductor integrated circuits," May 18 2004. US Patent 6,738,294.

[73] G. Chen, D. Sylvester, D. Blaauw, and T. Mudge, "Yield-driven near-threshold sram design," *IEEE transactions on very large scale integration (VLSI) systems*, vol. 18, no. 11, pp. 1590–1598, 2009.

[74] M. Sharifkhani, "Design and analysis of low-power srams," 2006.

[75] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-up sram state as an identifying fingerprint and source of true random numbers," *IEEE Transactions on Computers*, vol. 58, no. 9, pp. 1198–1210, 2008.

[76] Z.-W. Lai and K.-J. Lee, "Using unstable sram bits for physical unclonable function applications on off-the-shelf sram," in *2019 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, pp. 41–44, IEEE, 2019.

[77] J. Delvaux, D. Gu, D. Schellekens, and I. Verbauwhede, "Helper data algorithms for puf-based key generation: Overview and analysis," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 6, pp. 889–902, 2014.

[78] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conference*, pp. 9–14, IEEE, 2007.

[79] B. Gassend, M. Van Dijk, D. Clarke, and S. Devadas, "Controlled physical random functions," in *Security with Noisy Data*, pp. 235–253, Springer, 2007.

[80] R. Liu, H. Wu, Y. Pang, H. Qian, and S. Yu, "Extending 1kb rram array from weak puf to strong puf by employment of sha module," in *2017 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, pp. 67–72, IEEE, 2017.

[81] L. Santiago, V. C. Patil, C. B. Prado, T. A. Alves, L. A. Marzulo, F. M. França, and S. Kundu, "Realizing strong puf from weak puf via neural computing," in *2017 IEEE international symposium on defect and fault tolerance in VLSI and nanotechnology systems (DFT)*, pp. 1–6, IEEE, 2017.

[82] G. E. Suh, C. W. O'Donnell, and S. Devadas, "Aegis: A single-chip secure processor," *IEEE Design & Test of Computers*, vol. 24, no. 6, pp. 570–580, 2007.

[83] M. Yu, D. M'Raïhi, S. Devadas, and I. Verbauwhede, "Security and reliability properties of syndrome coding techniques used in puf key generation," in *Government Microcircuit Applications & Critical Technology Conference, GOMACTech*, pp. 1–4, 2013.

[84] S. Weingart and S. R. White, "Mind the gap: Updating fips 140," in *at FIPS Physical Security Workshop, Hawaii*, 2005.

[85] M. Roel, "Physically unclonable functions: Constructions, properties and applications," *Katholieke Universiteit Leuven, Belgium*, 2012.

[86] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Testing techniques for hardware security," in *2008 IEEE International Test Conference*, pp. 1–10, IEEE, 2008.

[87] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, "Quantitative and statistical performance evaluation of arbiter physical unclonable functions on fpgas," in *2010 International Conference on Reconfigurable Computing and FPGAs*, pp. 298–303, IEEE, 2010.

[88] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A large scale characterization of ro-puf," in *2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pp. 94–99, IEEE, 2010.

[89] J.-L. Danger, S. Guilley, P. Nguyen, and O. Rioul, "Pufs: Standardization and evaluation," in *2016 Mobile System Technologies Workshop (MST)*, pp. 12–18, IEEE, 2016.

[90] B. Habib and K. Gaj, "A comprehensive set of schemes for puf response generation," *Microprocessors and Microsystems*, vol. 51, pp. 239–251, 2017.

[91] Y. Su, J. Holleman, and B. P. Otis, "A digital 1.6 pj/bit chip identification circuit using process variations," *IEEE Journal of Solid-State Circuits*, vol. 43, no. 1, pp. 69–77, 2008.

[92] D. Yamamoto, K. Sakiyama, M. Iwamoto, K. Ohta, T. Ochiai, M. Takenaka, and K. Itoh, "Uniqueness enhancement of puf responses based on the locations of random outputting rs latches," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 390–406, Springer, 2011.

[93] "Information security, cybersecurity and privacy protection – Physically unclonable functions – Part 2: Test and evaluation methods," standard, International Organization for Standardization, Mar. 2021.

[94] J. Kim, T. Ahmed, H. Nili, J. Yang, D. S. Jeong, P. Beckett, S. Sriram, D. C. Ranasinghe, and O. Kavehei, "A physical unclonable function with redox-based nanoionic resistive memory," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 437–448, 2017.

[95] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[96] A. Maiti and P. Schaumont, "Improving the quality of a physical unclonable function using configurable ring oscillators," in *2009 International Conference on Field Programmable Logic and Applications*, pp. 703–707, IEEE, 2009.

[97] A. Maiti and P. Schaumont, "Improved ring oscillator puf: An fpga-friendly secure primitive," *Journal of cryptology*, vol. 24, no. 2, pp. 375–397, 2011.

[98] W. Killmann and W. Schindler, "A proposal for: Functionality classes for random number generators," *ser. BDI, Bonn*, 2011.

[99] G. E. Box, G. M. Jenkins, G. C. Reinsel, and G. M. Ljung, *Time series analysis: forecasting and control*. John Wiley & Sons, 2015.

[100] A. Garg and T. T. Kim, "Design of sram puf with improved uniformity and reliability utilizing device aging effect," in *2014 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1941–1944, IEEE, 2014.

[101] B. Jun and P. Kocher, "The intel random number generator," *Cryptography Research Inc. white paper*, vol. 27, pp. 1–8, 1999.

[102] A. Degada and H. Thapliyal, "An integrated trng-puf architecture based on photovoltaic solar cells," *IEEE Consumer Electronics Magazine*, 2020.

[103] S. K. Satpathy, S. K. Mathew, R. Kumar, V. Suresh, M. A. Anders, H. Kaul, A. Agarwal, S. Hsu, R. K. Krishnamurthy, and V. De, "An all-digital unified physically unclonable function and true random number generator featuring self-calibrating hierarchical von neumann extraction in 14-nm tri-gate cmos," *IEEE Journal of Solid-State Circuits*, vol. 54, no. 4, pp. 1074–1085, 2019.

[104] A. R. Krishna, S. Narasimhan, X. Wang, and S. Bhunia, "Mecca: A robust low-overhead puf using embedded memory array," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 407–420, Springer, 2011.

[105] H. Fujiwara, M. Yabuuchi, H. Nakano, H. Kawai, K. Nii, and K. Arimoto, "A chip-id generating circuit for dependable lsi using random address errors on embedded sram and on-chip memory bist," in *2011 Symposium on VLSI circuits-digest of technical papers*, pp. 76–77, IEEE, 2011.

[106] D. E. Holcomb, A. Rahmati, M. Salajegheh, W. P. Burleson, and K. Fu, "Drv-fingerprinting: Using data retention voltage of sram cells for chip identification," in *International Workshop on Radio Frequency Identification: Security and Privacy Issues*, pp. 165–179, Springer, 2012.

[107] S. K. Mathew, S. K. Satpathy, M. A. Anders, H. Kaul, S. K. Hsu, A. Agarwal, G. K. Chen, R. J. Parker, R. K. Krishnamurthy, and V. De, "16.2 a 0.19 pj/b pvt-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22nm cmos," in *2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC)*, pp. 278–279, IEEE, 2014.

[108] W. Barker, W. Polk, and M. Souppaya, "Getting ready for post-quantum cryptography: Exploring challenges associated with adopting and using post-quantum cryptographic algorithms," tech. rep., National Institute of Standards and Technology, 2021.

[109] H. Akhundov, E. van der Sluis, S. Hamdioui, and M. Taouil, "Public-key based authentication architecture for iot devices using puf," *arXiv preprint arXiv:2002.01277*, 2020.

[110] B. Raj, A. Saxena, and S. Dasgupta, "Nanoscale finfet based sram cell design: Analysis of performance metric, process variation, underlapped finfet, and temperature effect," *IEEE Circuits and Systems Magazine*, vol. 11, no. 3, pp. 38–50, 2011.

[111] H. Ramanna, "A study on controlling power supply ramp-up time in sram pufs," 2019.

[112] E. Barker and A. Roginsky, "Transitioning the use of cryptographic algorithms and key lengths," tech. rep., National Institute of Standards and Technology, 2018.

[113] R. Micheloni, A. Marelli, and R. Ravasio, *Error correction codes for non-volatile memories*. Springer Science & Business Media, 2008.

[114] Y. Wu, "New list decoding algorithms for reed–solomon and bch codes," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3611–3630, 2008.

[115] C. Lipps, A. Weinand, D. Krummacker, C. Fischer, and H. D. Schotten, "Proof of concept for iot device authentication based on sram pufs using atmega 2560-mcu," in *2018 1st International Conference on Data Intelligence and Security (ICDIS)*, pp. 36–42, IEEE, 2018.

[116] G. Vaidya, A. Nambi, T. Prabhakar, S. Sudhakara, *et al.*, "Iot-id: A novel device-specific identifier based on unique hardware fingerprints," in *2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pp. 189–202, IEEE, 2020.

[117] P. Urien, "Innovative atmega8 microcontroler static authentication based on sram puf," in *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1–2, IEEE, 2020.

[118] Y. Wen and Y. Lao, "Puf modeling attack using active learning," in *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1–5, IEEE, 2018.

[119] A. Setyawan Sajim, "Open-source software-based sram-puf for secure data and key storage using off-the-shelf sram," 2018.

[120] A. Van Herrewege, S. Katzenbeisser, R. Maes, R. Peeters, A.-R. Sadeghi, I. Verbauwhede, and C. Wachsmann, "Reverse fuzzy extractors: Enabling lightweight mutual authentication for puf-enabled rfids," in *International Conference on Financial Cryptography and Data Security*, pp. 374–389, Springer, 2012.

[121] C. Helfmeier, C. Boit, D. Nedospasov, and J.-P. Seifert, "Cloning physically unclonable functions," in *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pp. 1–6, IEEE, 2013.

[122] M. Liu, C. Zhou, Q. Tang, K. K. Parhi, and C. H. Kim, "A data remanence based approach to generate 100% stable keys from an sram physical unclonable function," in *2017 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED)*, pp. 1–6, IEEE, 2017.

[123] Nils and Christoph, "pypuf: Cryptanalysis of Physically Unclonable Functions," 2021.

[124] N. Wisiol, C. Gräbnitz, C. Mühl, B. Zengin, T. Soroceanu, N. Pirnay, and K. T. Mursi, "pypuf: Cryptanalysis of Physically Unclonable Functions," 2021.

[125] H. Nichols and M. R. Guthaus, "Puffery: An Open-Source Benchmark Tool for PUFs," 2019.

[126] W. S. Noble, "What is a support vector machine?," *Nature biotechnology*, vol. 24, no. 12, pp. 1565–1567, 2006.

[127] D. W. Hosmer Jr, S. Lemeshow, and R. X. Sturdivant, *Applied logistic regression*, vol. 398. John Wiley & Sons, 2013.

[128] T. G. Dietterich and E. B. Kong, "Machine learning bias, statistical bias, and statistical variance of decision tree algorithms," tech. rep., Citeseer, 1995.

[129] T. K. Ho, "The random subspace method for constructing decision forests," *IEEE transactions on pattern analysis and machine intelligence*, vol. 20, no. 8, pp. 832–844, 1998.

[130] K. Fukunaga and P. M. Narendra, "A branch and bound algorithm for computing k-nearest neighbors," *IEEE transactions on computers*, vol. 100, no. 7, pp. 750–753, 1975.

[131] D. M. Tax and R. P. Duin, "Using two-class classifiers for multiclass classification," in *Object recognition supported by user interaction for service robots*, vol. 2, pp. 124–127, IEEE, 2002.

[132] M. E. O'Neill, "Pcg: A family of simple fast space-efficient statistically good algorithms for random number generation," Tech. Rep. HMC-CS-2014-0905, Harvey Mudd College, Claremont, CA, Sept. 2014. https://www.cs.hmc.edu/tr/hmc-cs-2014-0905.pdf visited 2014-03-20.

[133] E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, L. Kohl, and P. Scholl, "Efficient pseudorandom correlation generators: Silent ot extension and more," in *Annual International Cryptology Conference*, pp. 489–518, Springer, 2019.

[134] T. Cui, S. Chen, K. Fu, M. Wang, and K. Jia, "New automatic tool for finding impossible differentials and zero-correlation linear approximations," *SCIENCE CHINA-INFORMATION SCIENCES*, vol. 64, no. 2, 2021.

[135] K. McKay, L. Bassham, M. Sönmez Turan, and N. Mouha, "Report on lightweight cryptography," tech. rep., National Institute of Standards and Technology, 2016.

[136] M. Á. Prada-Delgado, I. Baturone, G. Dittmann, J. Jelitto, and A. Kind, "Puf-derived iot identities in a zero-knowledge protocol for blockchain," *Internet of Things*, vol. 9, p. 100057, 2020.

[137] M. Petkus, "Why and how zk-snark works," *arXiv preprint arXiv:1906.07221*, 2019.

[138] J. Benet, "Ipfs-content addressed, versioned, p2p file system," *arXiv preprint arXiv:1407.3561*, 2014.

[139] R. W. Ahmad, H. Hasan, I. Yaqoob, K. Salah, R. Jayaraman, and M. Omar, "Blockchain for aerospace and defense: Opportunities and open research challenges," *Computers & Industrial Engineering*, vol. 151, p. 106982, 2021.

[140] S. Baltes, C. Treude, and S. Diehl, "Sotorrent: Studying the origin, evolution, and usage of stack overflow code snippets," in *2019 IEEE/ACM 16th International Conference on Mining Software Repositories (MSR)*, pp. 191–194, IEEE, 2019.

[141] P. Oliver, *Writing your thesis*. Sage, 2013.

[142] R. Murray, "Ebook: How to write a thesis," 2017.

[143] D. F. DiCarlo, "Random number generation: Types and techniques," 2012.

[144] G. Marsaglia, "Random numbers for c," *MC93*, p. 218, 1999.

[145] G. Marsaglia *et al.*, "Xorshift rngs," *Journal of Statistical Software*, vol. 8, no. 14, pp. 1–6, 2003.

[146] G. G. Rose, "Kiss: A bit too simple," *Cryptography and Communications*, vol. 10, no. 1, pp. 123–137, 2018.

[147] R. T. Kneusel, "Generating uniform random numbers," in *Random Numbers and Computers*, pp. 27–80, Springer, 2018.

[148] P. L'Ecuyer, "Tables of maximally equidistributed combined lfsr generators," *Mathematics of computation*, vol. 68, no. 225, pp. 261–269, 1999.

[149] P. L'ecuyer, "Maximally equidistributed combined tausworthe generators," *Mathematics of computation*, vol. 65, no. 213, pp. 203–213, 1996.

[150] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," tech. rep., Booz-allen and hamilton inc mclean va, 2001.

[151] R. G. Brown, D. Eddelbuettel, and D. Bauer, "Dieharder: A random number test suite," *Open Source software library, under development*, 2013.

[152] M. J. Cooper and K. B. Schaffer, "Security requirements for cryptographic modules," 2019.

[153] J. Kelsey and E. Barker, "Recommendation for random bit generator (rbg) constructions (sp 800-90c)," in *Second Draft*, National Institute of Standards and Technology, US Department of Commerce, 2016. https://csrc.nist.gov/publications/detail/sp/800-90c/draft, visited 2016-13-06.

[154] K. McKay, "Users guide to running the draft nist sp 800-90b entropy estimation suite," *NIST, Gaithersburg, MD, USA, Tech. Rep. SP*, 2016.

Πλατφόρμες δοκιμών τυχαίων αριθμών

"*The theoretical inquiries to come will have to take into account the time evolution of the phenomenon and the aging of the radiating particles to better connect the light curves and spectra.*"

G.Trap, *Soft gamma-ray constraints on a bright flare from the Galactic Center supermassive black hole*

Σε αυτό το σημείο της αναφοράς θα αναφερθούν τα θεμελιώδες ιδιότητες των Ψευδοτυχαίες Γεννήτριων Αριθμών, καθώς και οι πλατφόρμες που χρησιμοποιήθηκαν για κάποια πειράματα, μαζί με μία σήντομη περιγραφή των μεθοδολογιών διασφάλησης της ποιότητας αυτής. Όλες οι επίσημες τεμηριώσεις των σουίτων είναι αρκετά περίπλοκες, προϋποθέτουν πολλές προαπετούμενες γνώσεις για να γίνουν κατανοητές, οπότε για χάρη της απλότητας, σε αυτό το παράτημα απαρτίζονται όλες οι δοκιμές που λάμβανε χώρα στην ανάλυση των πειραμάτων.

.1 Ψευδοτυχαία γεννήτρια αριθμών

Ο κλάδος της επιστήμης των πληροφορικών συστημάτων, κρυπτογραφία, όχι μόνο χρησιμοποείται σε κάθε σύγχρονο σύστημα, αλλά αποσπεί ένα βασικό κομμάτι λειτουργίας μιας εφαρμογής. Οι γεννήτριες τυχαίων αριθμών (RNGs), αποτελούν τον

πυρήνα δημιουργίας κρυπτογραφικών κλειδιών, αλλά χρησιμεύουν και σαν βοήθημα πρόσθετης ασφαλείας, από επιθέσεις πλευρικών καναλιών(side channel attacks). Οι ψευδοτυχέες γεννήτριες αριθμών, γνωστές και ως PRNG (Pseudorandom Number Generator), έχουν την δυνατότητα παραγωγής μίας ντετερμινιστικής ακολουθίας αριθμών, δηλαδή το αποτέλεσμα εξαρτάται μόνο από την εσωτερική κατάσταση και δομή - η σειρά χαρακτηρίζεται από την απροβλεψημότητα, ανεξαρτησία και ομοιομορφιμότητα των αριθμών που την απαρτήζουν [143]. Κάθε σχετικός αλγόριθμος, έχοντας σημείο αναφοράς κάποιο σημείο πηγής (seed), το οποίο είτε μπορεί να σχηματιστεί από το χρήστη ή να δημιουργηθεί από διαφορετικές παραμέτρους ενός πληροφοριακού συστήματος, συμπεριλαμβανομένου του αναγνωριστικού χρόνου και διαδικασίας. Συνήθως, οι τυχαίοι αριθμοί που λαμβάνονται κατευθείαν από το σύστημα, έχουν κλίση στατιστικής ομοιγέννειας, και περετέρο επεξεργασία αντιστάθμισης αυτής της ευπάθειας. Γιαυτό τον λόγο, ο διορθωτής Von Neumann, απαλήφει από μια ακολουθία αριθμών, την στατιστική προτήμιση, και αντίστοιχα επιστρέφει μια νέα σειρά, στην οποία τα μέλη της σταθμίζονται εξίσου [101]. Αναφορικά, οι ποιό διαδεδομένοι αλγόριθμοι είναι, του George Marsaglia [144, 145], αλγόριμος KISS [146, 147], LFSR113 [148], LFSR88 [149], kneusel2018generating,manssen2012random .(TODO more detailed description) Στο πλαίσιο εφαρμογής στατιστικών δοκιμών, κάθε πειραματικό κριτήριο αξιολόγησης βασίζεται σε μια υπολογισμένη στατιστική τιμή, γνωστή ως P_value , η οποία συνοψίζει την ισχύ των αποδεικτικών στοιχείων δείγματος έναντι της υπόθεσης ιδανικής τυχαιότητας. Με άλλα λόγια, το P είναι η πιθανότητα παραγωγής ακολουθίας που αξιολογείται σε σχέση ενός καθορισμένου (από τον χρήστη) άξονα - και σε περίπτωση που είναι ίση με ένα, τότε η ακολουθία έχει υψηλή τυχαιότητα, καθώς το αντίθετο ισχύ όταν η τιμή πλησιάζει στο μηδέν(οι τιμές των δοκιμών κυμαίνονται από όριο 0.01 έως 0.001). Τα ποιό γνωστά πρώτηπα γεννητριών ψευδοτυχέών αριθμών, για τα οποία ο πηγαίος κώδικας είναι δημόσιος, είναι η σειρά εκδώσεων NIST SP 800-22 1a [150], Dieharder [151], PCG [], FIPS 140-3 [152]

.2 Σύνολο στατιστικών ελέγχνων NIST

Μια από τις πιο δημοφηλή σουίτες στατιστικών ελέγχνων, μια προσφορά του διεθνή οργανισμού NIST(National Institute of Standards show sources), είναι η ειδική δημοσίευση SP 800-22 1a [150]. Μετά την πρώτη κυκλωφορία της πρώτης έκδωσης, κυκλοφόρησε μια εμπλουτισμένη επέκταση SP 800-90 A έως C [5, 153, 7], στις οποίες παρέχουν προτάσεις για την ορθή σχεδίαση παραγωγών τυχαίων αριθμών,με αντίστοιχο οδηγό χρήσης [154].

Για τα πειράματα της παρούσας έρευνας, η εκδοχή της σουίτας περιείχε 15 είδη δοκιμών, αποτελούμενο από πολλαπλές υπο-παραλλαγές με συνολικό αριθμό 188, και για την πραγματοποίηση των πειραμάτων δοκημάστηκαν δύο λογισμικά ανοικτού κώδικα, δηλαδή η επίσημη συνησφορά από την NIST(υλοποίσηση μαύρου καυτιού), καθώς και ένα πειραματική ανάπτυξη του αρχικού προτύπου με επιπλέον δυνατότητες(εφεδρική αρχιτεκτονική) [123]. Η τυπική κανονική κατανομή χρησιμοποιείται ως αναφορά για τη σύγκριση της τιμής του στατιστικού ελέγχου που λαμβάνεται από τις δοκιμές, υπό την υπόθεση της τυχαιότητας. Στις παρακάτω ύπο-ενότητες θα καλυφθούν επιγραμματικά ο στόχος των δοκιμών.

.2.1 Δοκιμή συχνότητας δυαδικών τιμών

Όπως αναλύθηκαν σε προηγούμενα κεφάλαια, τα χαρακτηριστικά όπως της μοναδικότητας (κεφ. 3.0.2) και τυχαιότητας (κεφ. 3.0.3), μια τυχαίας πηγής, τηρούνται κάποιοι κακνόνες. Η στατιστή δοκιμή monobit, εστιάζει σε μια ιδιότητα συχνότητας, δηλαδή το ποσοστό διαδικών τιμών (0 ή 1) μιας ακολουθίας με την βοήθεια του μετρητή S, και απώτερος σκοπός είναι ο προσδιορισμός ισότιμης ισορροπίας μεταξύ των δύο επιλογών - οπότε αξιολογείται μόνο η συνολική επανάλληψη, και όχι η μέριμνα θέση ή κάποιας άλλης δημογραφικής τάσης. Ιδανική τιμή αυτής της ανάλυσης είναι το 50

$$(P_{value}) = erfc(S_{obs}/\sqrt{2}) \tag{1}$$

.2.2 Δοκιμές συχνότητας

Με την δοκιμή συχνότητας αναλύεται η αναλογία μηδενικών και μονάδων σε μια ακολουθία, και ο απότερος σκόπος αυτής της δοκιμής είναι να προσδιοριστεί αν ο αριθμός των μονάδων και των μηδενικών είναι περίπου ο ίδιος με αυτόν που θα αναμενόταν για μια πραγματικά τυχαία σειρά X. Αυτό επιτυγχάνεται αξιολογόντας την σχετικότητα των άσσων στην μέση της διάταξης μεγέθους Z, μετατρέποντας τα bit 0 και 1 σε -1 και $+1$, αντίστοιχα. Η συμπληρωματική συνάρτηση σφάλματος που ορίζεται ως $erfc$. Εάν το αποτέλεσμα της υπολογιζόμενης τιμής P είναι μεγαλύτερη από το 0,01, τότε συμπεράνετε ότι η ακολουθία συμπεράνετε ότι η ακολουθία. Επομένος, όταν οι θετικές

υπερισχύουν, καταλαβαίνουμε ότι έχουμε πολλούς άσσους, και αντίστροφα ισχύει το ανάποδο με την ίδια λογική.

$$(P_{value}) = erfc(s/\sqrt{2}) \tag{2}$$

$$erfc(y) = \frac{2}{\sqrt{\pi}} \int_{y}^{\infty} e^{u^2}\, du \tag{3}$$

.2.3 Δοκιμή συχνότητας σε ένα μπλοκ

Το αποτέλεσμα αυτού του τεστ είναι ο προσδιορισμός της συχνότητας άσσων σε ένα μπλοκ M bit είναι περίπου το μισό (απόδειξη τυχαιότητας), ενώ η εξεταζόμενη δειγματοληψία χωρίζεται σε πολλαπλά μπλοκ, καθένα από τα οποία έχει μήκος M, και τα υπόλοιπα τμήματα σε περίπτωση που υπάρχουν, απορρίπτονται. Όταν το αποτέλεσμα είναι μικρότερο του 0,01, τότε υπάρχει μεγάλη ή ίση αναλογία άσσων και μηδενικών σε τουλάχιστον ένα από τα μπλοκ, και ιδανική τιμή είναι αντίστοιχα (0.01, 0.99). Ειδικά, ελέγχεται η συχνότητα των διαδρομών σε μια ροή και αν τα bits σε μια δοκιμασμένη ροή αλλάζουν πολύ γρήγορα ή πολύ αργά σε σύγκριση με πραγματικά τυχαίες ροές. Απόρροια μεγάλου δείγματος σε κάθε μπλοκ, είναι η τιμή P να μηδενιστεί.

$$(P_{value}) = igamc(\frac{n}{2}, \frac{\rho}{2}) \tag{4}$$

$$igamc = \frac{\Gamma(a,b)}{\Gamma(a)} = \frac{1}{\Gamma(a)} \int_{b}^{\infty} e^{-t} t^{a-1}\, dt \tag{5}$$

.2.4 Δοκιμή εκτέλεσης

Σε αυτή την περίπτωση, επιθεωρείται εάν τα επόμενα bit είναι αναμενόμενα για μια τυχαία ακολουθία, καθώς ερμηνεύεται ως ”διαδρομών” μια αδιάσπαστη ακολουθία πανομοιότυπων bits, και αποτελείται από ακριβώς k πανομοιότυπα bits και περιορίζεται

πριν και μετά με ένα bit της αντίθετης τιμής. Συμπερασματικά, εάν η τιμή του R είναι μεγάλη, τότε η εναλλαγή δυαδικού αριθμού (δηλαδή, από μηδέν σε ένα, ή και αντίστροφα) δεν είναι συχνή, και με την ίδια λογική ισχύει το ανάποδο. Πέρα από αυτό, μια μπιτοσειρά με λίγες αναστροφές έχει λιγότερη δράση βρόχου από όσα θα αναμένονταν σε μια τυχαία ακολουθία.

$$(P_{value}) = erfc(\frac{|R - 2Z\pi(1-\pi)|}{2\sqrt{2Z}\pi(1-\pi)}) \tag{6}$$

.2.5 Δοκιμή για τη μεγαλύτερη σειρά μονάδων σε ένα μπλοκ

Αυτή η δοκιμή μελετά την παρουσία συστάδων σε υποσύνολα της ακολουθίας – σειράς μονάδων ή μηδενικών, εντός της εξεταζόμενης ακολουθίας εάν είναι ισοδύναμο με το μήκος της μεγαλύτερης σειράς μονάδων που θα αναμενόταν σε μια τυχαία ακολουθία. Η εκτέλεση προυποθέτει αρχικοποιημένο διαμειρασμό τιμών της ακολουθίας σε μπλοκ M μπιτ, και η συχνότητες της μεγαλύτερης σειράς μονάδων σε κάθε μπλοκ τοποθετούνται σε κατηγορίες. Για κάθε μπλοκ με μήκος M, η δοκιμή θα εκτελεστεί περισσότερες από συγκεκριμένες επαναλήψεις, στη συνέχεια θα καταγραφούν οι μεγαλύτερες διαδρομές των άσσων και θα χρησιμοποιηθεί στατιστική για την αξιολόγηση της τιμής P, οπότε το μήκος της σειράς πρέπει να είναι πολύ μεγαλύτερο από το μέγεθος του μπλοκ. Η τυχαία ακολουθία bit εισόδου έχοντας χωριστεί σε N μπλοκ των M μπιτ, κάθε μπλοκ σαρώνεται και επιστρέφει μια τιμή ίση με τη μέγιστη συνεχόμενη τιμή της διαδικής τιμής, και τελικά σε αυτή τη διαμόρφωση το αποτέλεσμα τους διανύσμος, μπορεί να μετράει διαφορετικούς τύπους εύρους συχνοτήτων, ανάλογα την ρύθμιση του χειριστή. Τέλος, εάν η τιμή P είναι μικρότερη του 0,01, τότε συμπεραίνετε ότι η ακολουθία δεν είναι τυχαία.

$$(P_{value}) = igamc(\frac{K}{2}, \frac{x^2}{2}) \tag{7}$$

.2.6 Δοκιμή κατάταξης δυαδικού πίνακα

Σε αυτή την δοκιμή διερευνάται η γραμμική εξάρτηση μεταξύ υποσυνόλων τυχαίου bit χρησιμοποιώντας για δείκτη την τάξη του πίνακα. Για την ακρίβεια, η ροή των δεδομένων, διαιρείται σε μπλοκ των οποίων η τάξη ενός τετραγωνικού πίνακα nxn

είναι ο αριθμός των γραμμικά ανεξάρτητων στηλών, και γραμμών, καθορίζεται από τους υποπίνακες με ελάχιστη τάξη το μηδέν, και αντίστοιχα μέγιστη το n. Ακόμη, σε κάθε πίνακα υπολογίζεται μια αναγνωριστική αξιολόγησης, για την οποία ταξινομείτε η συσχέτιση γραμμικότητας – επομένος αποθηκεύεται η κατάταξη σε τρισδιάστατο διάνυσμα. Χρησιμοποιώντας την προεπιλεγμένη διάσταση, $32x32$ που καθορίζεται ανωτέρω, όταν πολλοί υποπίνακες έχουν μικρή τάξη, συμπεραίνεται ότι το δείγμα έχει γραμμική ανεξαρτησία και θα αποτύχει σε αυτή τη δοκιμή. Κατά συνέπεια, σε περίπτωση που η τιμή P εάν είναι μικρότερη του 0.01, τότε ότι η ακολουθία δεν είναι τυχαία – εντούτοις πραγματική τυχαιότητα πετυχαίνεται για λίγες γραμμικές συσχετίσεις μεταξύ των υπο-ακολουθιών.

$$(P_{value}) = igamc(1, \frac{x^2(obs)}{2}) = e^{\frac{-x^2(obs)}{2}} \tag{8}$$

.2.7 Διακριτός μετασχηματισμός Fourier (φασματική) δοκιμή

Σε αυτή την δοκιμή ανιχνεύεται περιοδικότητα μοτίβων στην σαρωμένη ακολουθία. Με την βοήθει του διακριτού μετασχηματισμού Fourier, διαχωρίζεται η κανονικοποιημένη διαφορά μεταξύ του παρατηρούμενου και του αναμενόμενου αριθμού συνιστωσών συχνότητας(αριθμός των κορυφών) που υπερβαίνουν το κατώφλι 95%, και ο έλεγχος απευθήνεται στη μεταβλητή d. Από τα παραπάνω συμπεραίνεται, όταν το αποτέλεσμα εμπίπτει στο (0,01, 0,99), τότε η δοκιμή τελειώνει με επιτυχία.

$$(P_{value}) = erfc(\frac{|d|}{\sqrt{2}}) \tag{9}$$

.2.8 Δοκιμή αντιστοίχισης μη επικαλυπτόμενων προτύπων

Η δοκιμή αυτή επικεντρώνεται κυρίως στην συχνότητα των προκαθορισμένων μη επικαλυπτόμενων μοτίβων παραγόμενες από μια γεννήτρια. Προκειμένου να πραγματοποίηθει ο παραπάνω ορισμός, η καθορισμένη αρχικοποίηση μη περιοδικής ροής μπιτ, χωρισμένη σε N μπλοκ μήκους M, εκτελείται σε ένα εικονικό παράθυρο ολίσθησης. Το παράθυρο αυτό, γεμίζει με τα αρχικά μπιτ δεδομένων, και σε περίπτωση που η σειτά στο παράθυρο δεν ταιριάζει με το πρότυπο, τότε ολισθαίνει κατά μία θέση m (μη

επικαλυπτόμενο) και συνεχίζεται η σύγκριση - δηλαδή, σε περίπτωση ταιριάσματος, ο μετρητής για αυτό το μπλοκ της επόμενης θέσης του, μαζί με το παράθυρο ολισθαίνει απευθείας στη θέση m, πράγμα που ισοδυναμεί με απόρριψη της τρέχουσας ροής και γέμισμα των επόμενων τιμών του εξεταζόμενου διανύσματος μέσα στο παράθυρο. Επιπροσθέτως, η τιμή P, συγκρίνεται με το επίπεδο σημαντικότητας, και η διαδικασία αυτή επαναλαμβάνεται για κάθε πρότυπο που δοκιμάζεται. Άρα, σε περίπτωση που η τιμή P είναι στο (0,01, 0,99), τότε το δείγμα περνάει την δοκιμή, διαφορετικά αποτυγχάνει.

$$(P_{value}) = igamc(\frac{N}{2}, \frac{x^2(obs)}{2}) \tag{10}$$

.2.9 Δοκιμή αντιστοίχισης επικαλυπτόμενων προτύπων

Παρόμοια με τη δοκιμή αντιστοίχισης μη επικαλυπτόμενων προτύπων, ερευνάται ο αριθμός των εμφανίσεων σε προκαθορισμένες συμβολοσειρές χρησιμοπόντας ένα παράθυρο m δυαδικών τιμών, για την αναζήτηση ενός συγκεκριμένουν προτύπου - με διαφορά ματαξύ της δοκιμής χωρίς επικάλυψη πως σε αυτή την δοκιμή, όταν βρεθεί το πρότυπο, το παράθυρο ολισθαίνει μόνο κατά μία θέση πριν συνεχίσει την αναζήτηση, ενώ ταυτόχρονα κατανέμετε ο χρόνος αντιστοίχισης κάθε μπλοκ. Ωστόσο, αυτός ο αριθμός δεν χρησιμοποιείται για τον άμεσο υπολογισμό της στατιστικής μέριμνας, αλλά εμπλέκεται σε διαφορετικές συχνότητες χρόνων. Κάθε μοτίβο, αντιστοιχεί σε μια τιμή P, και η ολίσθηση του παραθύρου βρήσκεται στον μετρητή N. Συνοψίζοντας, εάν η τιμή P εμπίπτει στο (0,01, 0,99), η δοκιμή είναι επιτυχής.

$$(P_{value}) = igamc(\frac{N}{2}, \frac{x^2(obs)}{2}) \tag{11}$$

.2.10 Το "καθολικό στατιστικό" τεστ του Maurer

Η δοκιμή του Ueli Maurer επικεντρώνεται απόσταση μεταξύ δύο ταιριαστών μοτίβων, και όταν οι αποστάσεις είναι μικρές, τότε υποθέτετε πως σημπίεση χωρίς απώλεια πληροφορίας είναι εφικτή, άρα να μην είναι τυχαία η εισερχόμενη ακολουθία ή οποία είναι χωρισμένη σε μπλοκ, και έτσι να αποτύχει το τεστ. Εκτός από αυτό, τα πρώτα μπλοκ χρησιμοποιούνται την αρχικοποίηση της ακολουθίας, και τα υπόλοιπα τμήματα χωρίζονται σε κάποιο επιτρεπτό όριο. Στη συνέχεια, δημιουργείται ένας

πίνακας για κάθε πιθανή τιμή, και για κάθε καταχώριση χρειάζεται να καταγραφεί μόνο ο αριθμός μπλοκ της τελευταίας εμφάνισης αυτής της καταχώρησης. Εάν μια εισαγωγή δεν έχει επαναλυφθεί ποτέ, ο αριθμός κάτω από αυτήν θα πρέπει να είναι μηδέν - παράλληλα για κάθε μπλοκ μετά την αρχικοποίηση, ελέγχεται ο αριθμός των μπλοκ από την τελευταία εμφάνιση του ίδιου μπλοκ, και αντικαθίσταται η τιμή του μετρητή στον πίνακα με τον αριθμό του τρέχοντος μπλοκ. Τον στατιστικό ελέγχο, αντιπρωσοπεύεται από την μεταβλητή s, και περιέχει το άθροισμα του αριθμού των ψηφίων στην απόσταση μεταξύ προτύπων με την κατανομή αναφοράς της μονόπλευρη παραλλαγής κανονικής κατανομής, όπως στην περίπτωση του τεστ συχνότητας /reffrequencytesttheory. Πρόσθετα, όπου $< L >$ είναι η αναμενόμενη τιμή που υπολογίζεται ο αριθμός διαίρεσης μπλοκ της τελευταίας εμφάνισης κάθε μπλοκ. Τελικά, για να μην περάσει το τεστ, το s πρέπει να διαφέρει σημαντικά από το $< L >$, δηλαδή να είναι η ακολουθία συμπιεσμένη.

$$(P_{value}) = igamc(|\ \frac{s- < L >}{\sqrt{2\sigma}}\ |) \tag{12}$$

.2.11 Δοκιμή γραμμικής πολυπλοκότητας

Σε αυτή την δοκιμή, προσδιορίζεται η πολυπλοκότητα ακολουθίας ώστε να θεωρηθεί τυχαία. Αυτό πραγματοποιείται κατά την έρευνα μήκους ενός καταχωρητή μετατόπισης γραμμικής ανάδρασης (Linear Feedback Shift Register ή LFSR), από τον οποίο καθορίζεται η πιθανή περίοδο της ροής, εξαρτώμενοι του σπόρου (seed). Αρχικά, το διάνυσμα διαμερίζεται σε μπλοκ, το καθένα με αντίστοιχο μήκος, και στη συνέχεια εφαρμόζεται ο αλγόριθμος Berlekamp-Massey σε κάθε μπλοκ. Συγκεκριμένα, με τον αλγόριθμο υπολογίζεται τον χαμηλότερο βαθμό του πολυωνύμου ανατροφοδότησης για μια συγκεκριμένη δυαδική ροή, βρίσκοντας την γραμμική πολυπλοκότητα του κάθε μπλοκ. Απότοκο όλων των παραπάνω, όταν η τιμή P συμπίπτει στο (0,01, 0,99), τότε η σειρά περνάει τη δοκιμή γιατί υποδεικνύεται πως οι μετρήσεις συχνότητας διαφέρουν από τις αναμενόμενες τιμές.

$$(P_{value}) = igamc(\frac{K}{2}, \frac{x^2(obs)}{2}) \tag{13}$$

.2.12 Σειριακή δοκιμή

Η δοκιμή αυτή αποσκοπεί στον προσδιορισμός συχνότητας αριθμού των εμφανίσεων των επικαλυπτόμενων μοτίβων είναι περίπου ο ίδιος με αυτόν που θα αναμενόταν για μια τυχαία ακολουθία. Επίκεντρο αυτής της δοκιμής είναι η εξέταση τιμών σε μια ουρά, ελέγχοντας την συχνότητα των ίδιων μοτίβων σε σχέση με τις αναμενόμενες συχνότητες ίδιου μήκους. Τα στατιστικά στοιχεία που καταγράφονται είναι ο αριθμός των ταυτοποιήσεων μέσω της εξεταζόμενης σειράς, η εμφάνιση κάθε προηγούμενου και αμέσως προηγούμενου μοτίβου. Τέλος, όταν οι τελεστές $\nabla\Psi_m^2$ και $\nabla^2\Psi_m^2$ είναι μεγάλα, τότε υπονοείται μη ομοιομορφία των μπλοκ, δηλαδή όταν η τιμή P ανήκει στην περιοχή (0.01, 0.99), η ροή περνάει τη δοκιμή – οπότε, όλα τα πιθανά μοτίβα έχουν περίπου ισοδύναμες εμφανίσεις.

$$(P_{value1}) = igamc(2^{m-2}, \nabla\Psi_m^2) \tag{14}$$

$$(P_{value2}) = igamc(2^{m-3}, \nabla^2\Psi_m^2) \tag{15}$$

.2.13 Προσεγγιστική δοκιμή εντροπίας

Σε αυτή την δοκιμή εξετάζεται η συχνότητα των επικαλυπτόμενων μπλοκ δύο διαδοχικών μηκών σε σύγκριση με το αναμενόμενο αποτέλεσμα για μια τυχαία ακολουθία. Αρχικά, γνωρίζοντας το μήκος της σειράς, εκτός από την καταμέτρηση όλων των μοτίβων, ερευνάται οι πιθανές ροές αντιμετάθεσης. Η διαφορά μεταξύ αυτών των δύο καταστάσεων συγκρίνεται με τη διαφορά στις πραγματικά τυχαίες ακολουθίες αριθμών, και εξετάζεται έαν η ακολουθία είναι τυχαία ή όχι. Τέλος, στο όριο (0,01, 0,99), η σειρά εισόδου περνάει τη δοκιμή.

$$(P_{value}) = igamc(2^{m-1}, \frac{x^2}{2}) \tag{16}$$

.2.14 Δοκιμή αθροιστικών αθροισμάτων

Σκοπός του ελέγχου αυτού, είναι να προσδιοριστεί η μέγιστη απόκλιση από το μηδέν αθροισμάτων μιας δεδομένης ακολουθίας σε σχέση με την αναμενόμενη συμπεριφορά αυτού του αθροίσματος για τυχαίες ακολουθίες. Στη μεθοδολογία αυτή εκτιμάται εάν ο τυχαίος περίπατος της δοθείσας σειράς εάν είναι πολύ μεγάλος ή πολύ μικρός σε σχέση με την αναμενόμενη συμπεριφορά του τυχαίου περιπάτου μιας πραγματικά τυχαίας ακολουθίας. Για μια πραγματικά τυχαία ακολουθία ο τυχαίος περίπατος θα πρέπει να είναι κοντά στο μηδέν.

$$(P_{value}) = 1 - [\sum_{k=\frac{(-\frac{n}{2}+1)}{4}}^{\frac{\frac{n}{2}}{4}}] \tag{17}$$

.2.15 Δοκιμή τυχαίων εκτροπών

Στόχος της δοκιμής αυτής είναι ο προσδιορισμός του αριθμού των κύκλων που έχουν ακριβώς πεπερασμένες επισκέψεις σε μια συγκεκριμένη κατάσταση εντός ενός κύκλου αποκλίνει από αυτό που θα αναμενόταν για μια τυχαία ακολουθία. Ένας τυχαίος περίπατος αποτελείται από μια ακολουθία βημάτων μοναδιαίου μήκους που λαμβάνονται τυχαία και ξεκινούν από την αφετηρία και επιστρέφουν στην αρχή και η δοκιμή εκτιμά αν ο αριθμός των επισκέψεων σε μια συγκεκριμένη κατάσταση μέσα σε έναν κύκλο αποκλίνει από ό,τι θα αναμενόταν για μια πραγματικά τυχαία ακολουθία. Η δοκιμή αυτή είναι μια σειρά από οκτώ διαχωρισμένες δοκιμές, και σε σχέση με το προηγούμενο είδος, αυτό το τεστ επικεντρώνεται περισσότερο στον αριθμό των κύκλων που έχουν ακακριβώς έναν συγκεκριμένο επισκέψεων. Τα αποτελέσματα είναι διφορούμενα σε περίπτωση που τουλάχιστον μια τιμή P από τις οκτώ είναι διαφορετική εντός του (0,01, 0,99).

$$(P_{value}) = igamc(\frac{5}{2}, \frac{x^2(obs)}{2}) \tag{18}$$

.2.16 Δοκιμή παραλλαγής τυχαίων εκτροπών

Απότερος σκοπός αυτής της δοκιμής είναι ο προσδιορισμός των κύκλων q που έχουν έναν συγκεκριμένο αριθμό επαναλήψεων σε έναν τυχαίο περίπατο, δηλαδή εκτιμάται εάν ο αριθμός των επισκέψεων σε μια συγκεκριμένη κατάσταση εντός ενός κύκλου αποκλίνει από αυτόν που θα αναμενόταν για μια πραγματικά τυχαία ακολουθία. Επίσης, εξάγονται δεκαοκτώ συμπεράσματα από τις σειρές δοκιμές για κάθε μια από τις καταστάσεις, δηλαδή υπολογίζεται ο συνολικός αριθμός των φορών που εμφανίστηκε υπό κάποια κατάσταση σε όλους τους q κύκλους. Για όλες τις παραπάνω διαδικασίες, όπου ξ είναι η αθροιστική συνάρτηση κατανομής μιας εκθετικής τυχαίας μεταβλητής με παράμετρο ρυθμού. Τέλος, όταν η τιμή P εμπίπτει στο (0,01, 0,99), η σειρά περνάει τη δοκιμή.

$$(P_{value}) = igamc(\frac{|\xi(x) - q|}{2q(4|x| - 2)}) \tag{19}$$

.2.17 Ερμηνεία των αποτελεσμάτων της δοκιμής

Αφού ολοκληρώσουν η επιθεώρηση ελέγχου, η ερμηνεία μιας αποτυχείας, δηλαδή η αντίστοιχη μηδενική υπόθεση πρέπει να απορριφθεί, τότε πρόσθετα αριθμητικά πειράματα σε διαφορετικά δείγματα της γεννήτριας διεξάγονται, προκειμένου να διαπιστωθεί αν το φαινόμενο ήταν μια στατιστική ανωμαλία ή μια σαφής ένδειξη μη τυχαιότητας. Γνωρίζοντας την μεθοδολογία υλοποίησης για ένα συγκεκριμένο τεστ, μπορεί να υπολογιστεί το ποσοστό των ακολουθιών που περνούν αφού μετρηθεί ο αριθμός των δυαδικών ακολουθιών με τιμή μεγαλήτερη του 0,01 και διαιρείται με τον συνολικό αριθμό των ακολουθιών για να προκύψει η αναλογία. Τελικά, προσδιορίζεται το έυρος αποδεκτών αναλογιών χρησιμοποιώντας το διάστημα εμπιστοσύνης (confidence interval ή CI). Όπως αναφερθήκαμε και παραπάνω, η τιμή P ορίζεται ως η πιθανότητα παραγωγής μιας τέλειας τυχαίας γεννήτριας σε σχέση με την ακολουθία που εξετάστηκε, δεδομένου του είδους της μη τυχαιότητας που αξιολογείται από τη δοκιμή - αυτό σημαίνει ότι όσο πλησιάζει στο ένα, η εξεταζόμενη ακολουθία είναι απολύτος τυχαία, και αντίστοιχα για μηδέν η ακολουθία ακτιμάται ότι ως μη τυχαία. Συγκεκριμένα, όπου p είναι η πιθανότητα εμφάνισης, n πλήθος των μπιτ, και για να επιτύχει το τεστ, η αναλογία πρέπει να βρίσκεται πάνω από το ελάχιστο όριο του CI.

$$CI = p \pm z\sqrt{\frac{1}{n}p(1-p)} \tag{20}$$

Η κατανομή των τιμών P εξετάζεται για να εξασφαλιστεί η ομοιομορφία, από το διάστημα μεταξύ 0 και 1, διαιρείται σε s υποδιαστήματα και καταμετρώνται οι τιμές P που βρίσκονται εντός κάθε υποδιαστήματος.Η ομοιομορφία προσδιορίζεται μέσω της εφαρμογής ενός ελέγχου x^2 και του τερματισμού μιας τιμής P που αντιστοιχεί στον έλεγχο κατανομής καλής προσαρμογής σε αυτές τις τιμές, και λαμβάνονται για έναν αυθαίρετο στατιστικό έλεγχο. Άρα, όταν η τιμή P είναι μεγαλήτερη ή ίση του 0,0001, τότε οι ακολουθίες μπορούν να θεωρηθούν ομοιόμορφα κατανεμημένες.

$$(P_{value}) = (\frac{s-1}{2}, \frac{x^2}{2}) \tag{21}$$

.3 Δοκιμές NIST SP 800-90B

Η δημοσίευση SP 800- 90B εκδώθηκε τον Ιανουάριο του 2018, και επικεντρόνεται στην ανάλυση πηγών εντροπίας, προκειμένου να μπορεί να χρησιμοποιηθεί για την παραγωγή τυχαίων μπιτ. Οι ιδιότητες που πρέπει να έχει μια πηγή εντροπίας για να είναι κατάλληλη για χρήση σε γεννήτριες πηγών τυχαίων αριθμών σε κρυπτογραφικές εφαρμογές, επικυρώνονται με τα αποτελέσματα των παρακάτω δοκιμών. Τα δυο κριτήριια που εξετάζονται σε κάθε περίτωση είναι, έαν τα μέλλοι της σειράς εισόδου είναι ξεχωριστά και δεν επιρεάζει το ένα με το άλλο(δεν αποτελούν ακολουθιακό μοτίβο), έπειτα εάν τα στοιχεία μιας ακολουθίας παράγονται με τον ίδιο τρόπο, η ακολουθία χαρακτηρίζεται ως αναγνωρίσιμη – όταν μια ακολουθία πληροί τις απαιτήσεις αυτές, τότε αυτή η κλάση ονομάζεται IID (Independent and Identically Distributed).

.3.1 Στατιστική δοκιμής διαδρομών

Στη στατιστική δοκιμή εκδρομής, υπολογίζεται τη μέση τιμή της ακολουθίας και στη συνέχεια εκτιμάται η απόκλιση της μέσης τιμής του συνόλου αριθμών σε στατιστική κατανομή.

.3.2 Δοκιμή αριθμού κατευθύνσεων

Η δοκιμή των κατευθύνσεων έχει σαν είσοδο μια νέα ακολουθία η οποία συγκρίμενεται με τα στοιχεία της ακολουθίας εισόδου, αφού πρώτα η σειρά διαιρεθεί σε μη επικαλυπτόμενα μπλοκ των οκτώ μπιτ, για την οποία τα μηδενικά προστίθενται στο τέλος όταν το τελευταίο μπλοκ έχει λιγότερα από οκτώ στοιχεία, και αντίστοιχα οι άσσοι μετριούνται σε κάθε μπλοκ.

.3.3 Δοκιμή διάρκειας κατευθύνσεων

Σε αυτό το τεστ, συγκρίνονται τα στοιχεία της ακολουθίας εισόδου με το μήκος της μεγαλύτερης διαδρομής, φτιάχνοντας έτσι μια νέα ακολουθία. Να σημειωθεί ότι η ακολουθία εισόδου πρέπει να επεξεργαστεί με τον ίδιο τρόπο οπώς την προηγούμενη δοκιμή.

.3.4 Δοκιμή αριθμού αυξήσεων και μειώσεων

Αρχικά η σειρά εισόδου μετράπεται όπως είδαμε και στις δυο παραπάνω δοκιμές, και μετά μαζεύονται οι αυξήσεις και μειώσεις μεταξύ των στοιχείων της ακολουθίας εισόδου.

.3.5 Δοκιμή αριθμού διαδρομών με βάση τη διάμεση τιμή

Αρχικά η ακολουθία εισόδου συγκρίνεται με τη διάμεσο, η οποία ταξινομεί τα στοιχεία της από το μικρό προς το μεγάλο, έχοντας σαν κεντροκό σημείο την διάμεσος της ακολουθίας εισόδου, χωρίς κάποια προεπεξεργασία στην σειρά εισόδου.

.3.6 Δοκιμή διάρκειας διαδρομών με βάση τη διάμεση τιμή

Η ζητούμενη ακολουθεία της δοκιμής προκείπτει συγκρίνοντας τα στοιχεία της δεδομένης ακολουθίας εισόδου με τη διάμεσο, η οποία βρίσκεται με την ταξινόμηση των στοιχείων της από το μικρό προς το μεγάλο, και δεν εφαρμόζεται κάποια μετατροπή στα δεδομένα εισόδου.

.3.7 Δοκιμή μέσης στατιστική σύγκρουσης

Η παρούσα δοκιμή συλλέγει τον αριθμό των συγκρούσεων των στοιχείων μιας ακολουθίας εισόδου, για την οποία αρχικά γίνεται μετατροπή. Ειδηκότερα, η ακολουθία διαιρείται σε μη επικαλυπτόμενα μπλοκ των οκτώ μπιτ και υπολογίζεται η ακέραια τιμή κάθε μπλοκ. Έπειτα, στο αποτελέσμα της μετατροπής, εκτελείτε σε βρόχο επανάληψης ελέγχεται εάν κάθε τιμή της σειράς είναι σταθερό μετά την μετατροπή, και έαν βρίσκεται τότε αποθηκεύεται σε ένα μετρητή.

.3.8 Δοκιμή μέγιστης στατιστικής σύγκρουσης

Και σε αυτή την δοκιμή η ακολουθία ενδέχεται να επεξεργαστεί, με τον ίδιο τρόπο παραπάνω, και μετά σε έναν βρόχο επανάληψης υπολογίζεται ο αριθμός των συγκρούσεων των στοιχείων σε σύγκριση με την ακολουθία εισόδου. Έαν το ελεγχόμενο στοιχείο είναι σταθερό, τότε αποθηκεύεται.

.3.9 Δοκιμή στατιστικής περιοδικότητας

Αρχικά η σειρά εισόδου διαιρείται σε σε μη επικαλυπτόμενα μπλοκ των μπιτ, όπου τα μηδενικά τοποθετούνται όταν το τελευταίο μπλοκ έχει λιγότερα από οκτώ στοιχεία, και μετά υπολογίζεται ο αριθμός των περιοδικών δομών στην ακολουθία εισόδου με διαφορετικούς συνδιασμούς παραμέτρων.

.3.10 Δοκιμή στατιστικής συνδιακύμανσης

Αφού γίνει η μετατροπή όπως στο προηγούμενο τεστ, υπολογίζεται η στατιστική ισχύς συσχέτισης.

.3.11 Δοκιμή στατιστικής συμπίεσης

Στην τελευταία δοκιμή υπολογίζεται το αποτέλεσμα των συμπιεσμένων δεδομένων, με τον αλγόριθμο συμπίεσης bzip2, ο οποίος είναι υπεύθηνος συμπιέζει τις μπιτοσειρές και μετατρέπονται σε ακολουθίες των ίδιων συμβολοσειρών χαρακτήρων, χωρίς καμία αρχική μετατροπή.

Test	Status
Excursion Test Statistic	PASS
Number of Directional Runs	PASS
Length of Directional Runs	PASS
Number of Increases and Decreases	PASS
Number of Runs Based on the Median	PASS
Length of Runs Based on Median	PASS
Average Collision Test Statistic	PASS
Maximum Collision Test Statistic	PASS
Periodicity Test Statistic	PASS
Covariance Test Statistic	PASS
Compression Test Statistic	PASS
Testing Independence for Non-Binary Data	PASS
Testing Goodness-of-fit for Non-Binary Data	PASS
Testing Independence for Binary Data	PASS
Testing Goodness-of-fit for Binary Data	PASS
Length of the Longest Repeated Substring Test	PASS

Fig. 1 Αναλυτικός πίνακας αποτελεσμάτων δοκιμών πλατφόμας NIST SP 800-90B [7], σε ένα εκκατομύριο δείγματα (1.4 εκκατομύρια) και ένα εκκατομύριο για καλύτερη ακρίβεια.

.3.12 Ενσωμάτωση του προτύπου στα πειράματα της έρευνας

Τα αποτελέσματα των παραπάνω δοκιμών στην αναλυσή μας ήταν θετικά. Έχοντας βάση τον πίνακα αποτελεσμάτων 1, συμπεράνετε πως τα εγγενεί χαρακτηριστικά μια μη αντιγράψημης πηγής τύπου SRAM, μπορούν να χρησιμοποιηθούν ως σημείο αναφοράς εντροπίας (σπόρος – seed) σε κρυπτογραφικά συστήματα.

.4 Σύνολο στατιστικών ελέγχνων Diehard

Σε αυτό το σημείο συγκεντρόνονται όλες οι δοκιμές της σουίτας Dieharder [151]. Αυτή η σουίτα στατιστικών δοκιμών θεωρείται ως μια απο τις πιο ισχυρές γενικές δοκιμές τυχαιότητας, και αποτελείται από 15 διαφορετικά ανεξάρτητα στατιστικά τεστ και απαιτεί τουλάχιστον 80 εκατομμύρια μπιτς σε δυαδική μορφή για όλες τις δοκιμές. Τέλος, μια τιμή P που κυμαίνεται μεταξύ 0,005 και 0,995 θεωρείται ότι έχει (περάσει) επιτυχία σε κάποιο τεστ, ενώ όταν είναι ακριβώς 0 ή 1 θεωρείται ότι έχει αποτύχει. Σε περίπτωση που είναι κάτω από 0,005 και πάνω από 0,995, τότε είναι

χαρακτηρίζεται το αποτέλεσμα ως αδύναμο, οπότε περαιτέρο αναλυση είναι απαραίτητα - μέσω περισσότερων δειγμάτων.

.4.1 Δοκιμή απόστασης γενεθλίων

Σε αυτή την δοκιμή επιλέγεται τυχαία διάφορα σημεία σε ένα μεγάλο διάστημα και απαριθμούνται οι αποστάσεις μεταξύ των σημείων. Ο αριθμός των τιμών που εμφανίζονται περισσότερες από μία φορές στη λίστα θα πρέπει να είναι ασυμπτωτικά κατανεμημένος κατά Poisson μέσης τιμής - μέσα από εννέα φορές χρησιμοποιώντας σύνολα διευθύνσεων για έναν τυχαίο ακέραιο αριθμό, δηλαδή επιστρέφονται εννέα τιμές P.

.4.2 Δοκιμή επικαλυπτόμενων μεταθέσεων

Αυτή η δοκιμή αναλύει αλληλουχίες ενός εκατομμυρίου τυχαίων ακέραιων αριθμών των 32 μπιτ, λαμβάνοντας πέντε διαδοχικούς ακέραιους αριθμούς και συγκρίνοντάς τους, αθροίζονται και κατανέμονται με σε σειρά. Ειδηκότερα, κάθε σύνολο ακεραίων αριθμών, μπορεί να βρίσκεται σε μία από τις καταστάσεις πιθανών διατάξεων των πέντε συστάδων, και γίνονται δύο επαναλήψεις για κάθε ακολουθία. Τελικά, επιστρέφονται δύο τιμές P.

.4.3 Δυαδική δοκιμή κατάταξης

Για αυτή την δοκιμή, οι έλεγχοι έχουν χωριστοί σε δύο επιμέρους δοκιμές δυαδικής κατάταξης, για πίνακες 31x31 και 32x32. Σε κάθε πίνακα, οι τιμές που είναι στα αριστερά, επιλέγονται από την ροή δεδομένων ια να σχηματίσουν ένα νέο πίνακα, για τον οποίο οι τάξεις προσδιορίζονται πάνω στο πεδίο [0,1], και τελικά επιστρέφεται μια τιμή P. Με την ίδια λογική, επιλέγονται έξι τυχαίοι ακέραιοι αριθμοί 32 μπιτ, για τον σχηματισμό πινάκων 6x8, και σε αυτή την περίπτωση η δοική επαναλαμβάνεται για 25 φορές για τις τιμές ακέραιων αριθμών της ακολουθείας - οπότε επιστρέφονται εικοσιπέντε τιμές P.

.4.4 Δοκιμή ροής δυαδικών δεδομένων

Σε αυτή την δοκιμή εξετάζεται σε 1 μπιτ, από τους ακέραιους εισόδου των 32 μπιτ, για εικοσιπέντε φορές, με την μέθοδο της επικάλυψης, όπου διαδοχικά από την αρχική (έως το 220), αυξάνοντας κατά ένα ελέγχονται είκοσι διευθύνσεις, και με αυτό τον τρόπο

ελέγχεται πόσες συστάδες δεν έχουν εμφανιστεί ποτέ. Σε αυτή την περίπτωση, ο αριθμός της συστάδας που λείπει, πρέπει να είναι κανονικά κατανεμημένος, δηλαδή μια τυπική κανονική μεταβλητή που οδηγεί σε μια ομοιόμορφη τιμή P. Στο τέλος της ανάλυσης, εικοσιπέντε P θα είναι διαθέσημα.

.4.5 Δοκιμή πιθήκου OPSO (Overlapping-Pairs-Sparse-Occupancy)

Στη δοκιμή OPSO ελέγχονται δυο συστάδες των είκοσι μιτ, μήκους 1024, και για η κάθε συστάδα καθορίζεται από ένα καθορισμένο αριθμό δέκα μπιτ αριθμού 32 μιτ της σειράς εισόδου. Παράλληλα, για 222 επικαλυπτόμενες τιμές, μετράται ο αριθμός των λέξεων που λείπουν, δηλαδή λέξεις 2 μπιτ που δεν εμφανίζονται σε ολόκληρη την ακολουθία.

.4.6 Δοκιμασία μαϊμού OQSO (Επικαλυπτόμενα τετράγωνα-διαχωρισμός πληρότητας)

Στο τεστ OQSO εξετάζονται τέσσερεις συστάδες των είκοσι μπιτ, και 32 σειρών, το οποίο καθορίζεται από μια καθορισμένη σειρά 5 διαδοχικών μπιτ από τις αρχικές ρυθμήσεις. Επομένος, παράγεται ο μέσος αριθμός των τιμών που λείπουν από τις 224 επικαλιπτόμενες τιμές.

.4.7 Δοκιμή μαϊμού DNA

Στη δοκιμή DNA για 4 συστάδες εξετάζεται σειρές με 10 τιμών, που καθορίζονται με δύο καθορισμένα μπιτς στην ακολουθία των τυχαίων ακέραιων αριθμών. Επιπροσθέτως, παράγονται 221 επικαλύψεις συστάδων, με 10 τιμές, από 230 μοτίβα και μετρά τον αριθμό των λέξεων των 10 τιμών που λείπουν.

.4.8 Μέτρηση των άσσους σε μια ροή bytes

Σε αυτή την δοκιμή, η ροή εισόδου δεδομένων (32 μπιτ) θεωρείται ως ροή bytes, ως εκ τούτου, κάθε byte μπορεί να περιέχει τιμές εύρους 0 έως 8 (διαφορετικές πιθανότητες) - και συνολικά χωρίζονται σε πέντε διαφορετικές τιμές, όπου οι μετρήσεις γίνονται με βάση τις συχνότητες των συστάδων σειράς 256.000 επικαλυπτόμενων λέξεων με 5 τιμές, όπου στο τέλος υπολογίζεται μια τιμή P.

.4.9 Μέτρηση των 1 σε συγκεκριμένα bytes

Σε αυτό τον έλεγχο όπως και στον προηγούμενο, εκτελείται για μια ροή από bytes, αλλά για συγκεκριμένο byte, που επιλέγεται πάντα το αριστερά για κάθε σειρά ακαιρέων. Ακόμη, αυτή η διαδικασία επαναλλαμβάενεται 25 φορές, από τους ακέραιους αριθμούς της ροής μπιτ, και επιστρέφει 25 τιμές P αντίστοιχα.

.4.10 Δοκιμή στάθμευσης

Αυτή η δοκιμή βασίζεται στο σκεπτικό πως υποθέτοντας ότι υπάρχει ένα τετράγωνο γκαράζ στάθμευσης με 100 διαθέσιμες θέσεις σε κάθε πλευρά, με άλλα λόγια είναι συνολικά διαθέσιμες 10.000 θέσεις στάθμευσης, και μετά από 12.000 προσπάθειες για 10 φορές, ο αριθμός των επιτυχώς παρκαρισμένων αυτοκινήτων θα πρέπει να ακολουθεί μια ορισμένη κανονική κατανομή. Ειδηκότερα, όταν ο χώρος είναι άδειος, τότε το παρκάρει εκεί και αυξάνει τη λίστα επιτυχημένης στάθμευσης, και όταν ο χώρος έχει καταληφθεί από άλλο αυτοκίνητο, η συντριβή αυξάνει μία και πρέπει να βρει άλλο χώρο στάθμευσης. Άρα, επιστρέφεται το P, που είναι ο αριθμός των επιτυχώς παρκαρισμένων αυτοκινήτων.

.4.11 Δοκιμή ελάχιστης απόστασης

Γι'αυτή τη δοκιμή, τοποθετούνται επιλεγμένα σημεία σε ένα τετράγωνο πλευράς πλήθους 10.000, και έπειτα τυχαιά επιλέγονται σημεία σε επανάλληψη 100 κύκλων, υπολογίζοντας ταυτόχρονα ην ελάχιστη απόσταση μεταξύ κάθε ζεύγους σημείων. Σε μια πραγματικά και ανεξάρτητα τυχαία περίπτωση, το τετράγωνο αυτής της απόστασης θα πρέπει να είναι εκθετικά κατανεμημένο.

.4.12 Δοκιμή τυχαίων διαστάσεων

Παρόμοια με την προηγούμενη δοκιμή, σε αυτή την δοκιμή επιλέγονται 4000 τυχαία σημεία 20 φορές, για έναν κύβο με κάθε ακμή πλήθους 1000, και σε κάθε σημείο, κεντράρεται μια σφαίρα η οποία είναι αρκετά μεγάλη ώστε να φτάσει στο πλησιέστερο σημείο. Έτσι, ο όγκος της μικρότερης σφαίρας πρέπει να είναι εκθετικά κατανεμημένος με μέση τιμή 40, και η ακτίνα των κύβων είναι εκθετική με μέση τιμή 30 η οποία προκύπτει από εκτεταμένη προσομοίωση.

.4.13 Δοκιμή συμπίεσης

Για είσοδο ενός μεγάλου ακέραιου αριθμού (τύπου float), πολλαπλασιάζεται με μια ακολουθία τυχαίων κινητών αριθμών μέχρι να φτάσετε στο ένα. Ειδηκότερα, οι τυχαίοι κινητοί αριθμοί κατασκευάζονται από αριθμητικές παραμέτρους(τύπου float), από μπιτ εισόδου, καθώς ο αριθμός επαναλήψεων που απαιτήται, πρέπει να ακολουθεία μια συγκεκριμένη κατανομή. Τέλος, η εκτέλεση της δοκιμής επαναλαμβάνεται 100.000 φορές, έπειτα υπολογίζεται ο ρυθμός εμάνισης των παραμέτρων (float) σε κάθε δοκιμή, και το σύνολο αυτό χρησιμοποιείται για την παραγωγή του αποτελέσματος.

.4.14 Δοκιμή επικαλυπτόμενων αθροισμάτων

Σε αυτή την δοκιμή τυχαίοι ακέραιοι αριθμοί, προστέτονται ακολουθίες 100 διαδοχικών κινητών αριθμών, 10 φορές, και το άθροισμα τους πρέπει να είναι κανονικά κατανεμημένο - το αποτελέσματα είναι μια μόνο τιμή P.

.4.15 Δοκιμή τρεξίματος

Σε αυτή την δοκιμή υπολογίζεται το σύνολο των διαδρομών προς τα πάνω και προς τα κάτω , 10 φορές, σε μια ακολουθία τυχαίων κυμαινόμενων αριθμών ομοιόμορφα στο [0,1] που λαμβάνονται από κυμαινόμενους ακέραιους αριθμούς των 32 μπιτ, καθώς τα ανοδικά και καθοδικά τρεξίματα καταμετρώνται για ακολουθίες μήκους 10.000.

.4.16 Δοκιμή των ζαριών

Αυτό το τεστ αφορά ένα δείγμα, για το οποίο κάθε τιμή (τύπου float) πολλαπλασιάζεται με το 6 και το ανακτόμενο μέρος αυξάνεται κάτα ένα - αυτή η διαδικασία εκετελείτε σε επανάληψη 200.000 φορές. Με την αναλογία των ευνοϊκών τιμών, καταγράφονται οι καλύτεροι συνδιασμοί, σε συνδιασμό με τον μετρητή συνολικής ρήψης, οπότυε αθροίζονται όλες οι ρίψεις για την αναγνώριση στατιστικών μοτίβων.

Άδεια