Σελίδα τίτλου

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΙΩΑΝΝΙΝΩΝ

ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΜΣ: ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΔΙΚΤΥΑ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

STUDY ON SIDE - CHANNEL ATTACKS – THE DIFERENTIAL POWER ANALYSIS (DPA) PARADIGM

Άρτεμις Δημοτάτση

Επιβλέπων: Φώτιος Βαρτζιώτης

ΔΕΠ Επίκουρος Καθηγητής

Άρτα, Απρίλιος, 2022

STUDY ON SIDE - CHANNEL ATTACKS – THE DIFERENTIAL POWER ANALYSIS (DPA) PARADIGM

Εγκρίθηκε από τριμελή εξεταστική επιτροπή

Τόπος, Ημερομηνία

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Επιβλέπων καθηγητής

   Όνομα Επίθετο,

   τίτλος, βαθμίδα

2. Μέλος επιτροπής

   Όνομα Επίθετο,

   τίτλος, βαθμίδα

3. Μέλος επιτροπής

   Όνομα Επίθετο,

   τίτλος, βαθμίδα

Δήλωση μη λογοκλοπής

Δηλώνω υπεύθυνα και γνωρίζοντας τις κυρώσεις του Ν. 2121/1993 περί Πνευματικής Ιδιοκτησίας, ότι η παρούσα μεταπτυχιακή εργασία είναι εκ ολοκλήρου αποτέλεσμα δικής μου ερευνητικής εργασίας, δεν αποτελεί προϊόν αντιγραφής ούτε προέρχεται από ανάθεση σε τρίτους. Όλες οι πηγές που χρησιμοποιήθηκαν (κάθε είδους, μορφής και προέλευσης) για τη συγγραφή της περιλαμβάνονται στη βιβλιογραφία.

Δημοτάτση, Άρτεμις

Υπογραφή

ΕΥΧΑΡΙΣΤΙΕΣ

Σε αυτό το σημείο θα ήθελα να απευθύνω τις ευχαριστίες μου σε ορισμένους ανθρώπους που με βοήθησαν να ολοκληρώσω αυτή τη διπλωματική εργασία. Αρχικά θα ήθελα να ευχαριστήσω τον επιβλέποντα κ. Βαρτζιώτη Φώτιο για την επιλογή του θέματος, την πρόσβαση σε βοηθητικό υλικό, τις συμβουλές και την άμεση βοήθεια που μου παρείχε σε κάθε σημείο ανάπτυξης της εργασίας. Θα ήθελα να ευχαριστήσω τους γονείς μου και το σύζυγο μου για την ηθική και έμπρακτη βοήθεια που μου παρείχαν, όχι μόνο όσον αφορά την ολοκλήρωση της εργασίας και των σπουδών μου, αλλά και σε κάθε σημαντικό σημείο στη ζωή μου.

ΠΕΡΙΛΗΨΗ

Ο σύγχρονος ψηφιακός κόσμος, ο οποίος είναι απόρροια από την αλληλεπίδραση της Τεχνολογίας και των Μαθηματικών, είχε ως αποτέλεσμα την εξέλιξη της Κρυπτογραφίας. Θα μπορούσε να χαρακτηριστεί και ως ένα είδους απαίτησης που αφορά την προστασία των ευαίσθητων δεδομένων που ανταλλάσσονται σχεδόν σε όλες τις εκφάνσεις της καθημερινής μας ζωής. Παράλληλα όμως εξελίχθηκαν και οι επιθέσεις ενάντια στα κρυπτογραφικά συστήματα. Άλλες επιθέσεις είναι πιο δυνατές και αποτελεσματικές με αποτέλεσμα να χρειάζονται πιο εξειδικευμένο εξοπλισμό και άλλες με λιγότερο εξοπλισμό, αλλά λόγω της φύσης τους επιφέρουν καίρια πλήγματα και φέρνουν αποτελέσματα.

Στο πλαίσιο της παρούσας εργασίας θα αναφερθούμε σε διάφορες κατηγορίες επιθέσεων καθώς και στον τρόπο λειτουργίας τους. Θα επικεντρωθούμε όμως στις Επιθέσεις Πλευρικών Καναλιών. Κάθε τύπος επίθεσης έχει κάποια αντίμετρα που μπορούν να εφαρμοστούν έτσι ώστε να παρέχουν στο σύστημα κάποια ασφάλεια. Έτσι και οι Επιθέσεις Πλευρικών Καναλιών έχουν τα δικά τους, τα οποία απορρέουν και από τα χαρακτηριστικά που εκμεταλλεύονται κατά την επίθεση.

Τέλος, θα αναφερθούμε σε μεθόδους αποκρυπτογράφησης και συγκεκριμένα στην ανάλυση ισχύος για εύρεση μυστικού κλειδιού. Η πιο ισχυρή μέθοδος μπορούμε να πούμε ότι είναι η Διαφορική Ανάλυση Ισχύος, την οποία και θα περιγράψουμε. Η παρούσα διπλωματική εργασία θα ολοκληρωθεί με την επίδειξη μιας επίθεσης σε συσκευή που υλοποιεί τον αλγόριθμο AES. Η επίθεση πραγματοποιείται με την μέθοδο της διαφορικής ανάλυσης ισχύος (DPA) και έχει ως στόχο την αναγνώριση του "κλειδιού" της συσκευής. Για τις ανάγκες της επίδειξης έχουν χρησιμοποιηθεί πειραματικά δεδομένα από τη βιβλιογραφία. Σημειώνεται ότι, η επίδειξη έχει υλοποιηθεί στο προγραμματιστικό περιβάλλον του εργαλείου Octave.

Λέξεις-κλειδιά: Επίθεση πλευρικών καναλιών, DPA, Αλγόριθμος AES, Αντίμετρα, Τεχνικές έγχυσης σφαλμάτων, Ανάλυση ισχύος

ABSTRACT

The modern digital world, which is the result of the interaction of Technology and Mathematics, has resulted in the evolution of Cryptography. It could also be described as a kind of requirement for the protection of sensitive data that is exchanged in almost all aspects of our daily lives. At the same time, however, attacks against cryptographic systems evolved. Other attacks are more powerful and effective, with the result that they require more specialized equipment and others with less equipment, but due to their nature they cause key blows and bring results.

In the context of this work, we will refer to different categories of attacks as well as how they work. But we will focus on Side Channel Attacks. Each type of attack has some countermeasures that can be applied to provide the system with some security. So, the Lateral Channel Attacks have their own, which derive from the characteristics they take advantage of during the attack.

Finally, we will refer to decryption methods and specifically to the power analysis to find a secret key. The most powerful method can be said to be the Differential Power Analysis, which we will describe. This dissertation will be completed by demonstrating an attack on a device that implements the AES algorithm. The attack is carried out by the method of differential power analysis (DPA) and aims to identify the "key" of the device. Experimental data from the literature have been used for the needs of the demonstration. Note that the demo has been implemented in the Octave tool development environment.

Keywords: Side channel attacks, DPA, AES algorithm, Ccountermeasures, Error injection techniques, Power Analysis

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΙΣΑΓΩΓΗ

Τα ενσωματωμένα συστήματα έκαναν την εμφάνισή τους στην ζωές μας πριν από λίγα χρόνια. Η ευρεία εφαρμογή τους όμως όπως στα μέσα μαζικής μεταφοράς κοκ έχουν δημιουργήσει θέματα όσον αφορά την προστασία και την ασφάλεια των δεδομένων. Προχωρώντας επίσης η τεχνολογία η χρήση τους γίνεται όλο και πιο ευρέως διαδεδομένη καθώς είναι αναπόσπαστο κομμάτι του Internet of Things (IoT). Αυτό βέβαια από ότι φαίνεται βοηθάει στο να κάνουμε τη ζωή μας πιο εύκολη σε πολλά πράγματα αλλά υπάρχει το θέμα πως όλες αυτές οι πληροφορίες που διακινούνται θα γίνεται με ασφάλεια.

Οι σχεδιαστές τέτοιων συστημάτων προέβλεψαν ότι μελλοντικά θα προκύψουν τέτοια προβλήματα με αποτέλεσμα να προμηθεύσουν τους ενσωματωμένους επεξεργαστές τους με εντολές γρήγορης κρυπτογράφησης και αποκρυπτογράφησης. Τα πρώτα πρωτόκολλα κρυπτογράφησης παρείχαν πολύ ισχυρή ασφάλεια έναντι μαθηματικών επιθέσεων. Τέτοιες επιθέσεις είναι οι επιθέσεις γραμμικής και διαφορικής κρυπτανάλυσης. Πλέον όμως με την εξέλιξη της τεχνολογίας έκαναν την εμφάνισή τους πιο σκληρού τύπου επιθέσεις οπότε τα υπολογιστικά συστήματα θα πρέπει να παρέχουν και πιο μακροχρόνια ασφάλεια.

Αυτού του είδους οι επιθέσεις λέγονται «σωματικές» καθώς έχουν σαν σκοπό, για μπορέσουν να εξάγουν τα δεδομένα και τις πληροφορίες που θέλουν, να προκαλέσουν σοβαρό πρόβλημα στο σώμα του υπολογιστικού συστήματος. Για να μπορέσει να γίνει με επιτυχία μια τέτοιου είδους επίθεση, ο αλγόριθμος προσπαθεί να εκμεταλλευτεί οποιοδήποτε τρωτό σημείο της συσκευής και να προκαλέσει ανωμαλία στη λειτουργία της.

Οι φυσικές επιθέσεις είναι αρκετά επικίνδυνες για τα ενσωματωμένα συστήματα καθώς όπως είναι φτιαγμένα μπορούν τα παραδώσουν τον πλήρη έλεγχο στον επιτιθέμενο αν επιτευχθεί η επίθεση. Οι επιθέσεις αυτού τύπου είναι δυο κατηγοριών: οι παθητικές και οι ενεργητικές.

Σχετικά με τις παθητικές επιθέσεις θα πρέπει να τονίσουμε την ανάλυση ισχύος κατά την οποία ο επιτιθέμενος αναλύει την κατανάλωση ισχύος σε συγκεκριμένες κρυπτογραφήσεις και με υποθέτοντας ένα μικρό κομμάτι του μυστικού κλειδιού ακολουθεί τα ίχνη ισχύος ώστε να κάνει επαλήθευση. Ωστόσο για το χρόνο που χρειάζεται για να ολοκληρωθεί μια κρυπτογράφηση, η ηλεκτρομαγνητική εκπομπή καθώς και η εκπομπή φωτονίων ενός τρανζίστορ έχουν χρησιμοποιηθεί επιτυχώς για κλοπή ευαίσθητων πληροφοριών.

Στις ενεργητικές επιθέσεις ο επιτιθέμενος εκτός από την παρατήρηση των πληροφοριών που διαρρέουν προσβάλει και την συσκευή σε πραγματικό χρόνο. Ο πιο κοινός τρόπος επίθεσης είναι η διοχέτευση σφαλμάτων. Σε αυτού του είδους τις επιθέσεις ο επιτιθέμενος επιβάλλει στη συσκευή να εκτελεί λανθασμένες πράξεις, μεταξύ των σωστών αποτελεσμάτων αλλά και των λανθασμένων προσπαθεί να προσδιορίσει το μυστικό κλειδί ή να περιορίσει το χώρο για την εύρεσή του. Η επίθεση με διοχέτευση σφάλματος αποτελείται από δυο τμήματα. Το πρώτο τμήμα είναι η ίδια η διοχέτευση του σφάλματος που προκαλεί προσωρινή ανωμαλία στη συσκευή και το δεύτερο τμήμα είναι η ίδια η επίθεση όπου το λάθος αποτέλεσμα είναι πηγή πληροφοριών. Αυτού του είδους οι επιθέσεις είναι αρκετά επικίνδυνες καθώς δεν απαιτούν πολύ χρόνο και επίσης μπορούν να επιτευχθούν με φθηνό εξοπλισμό.

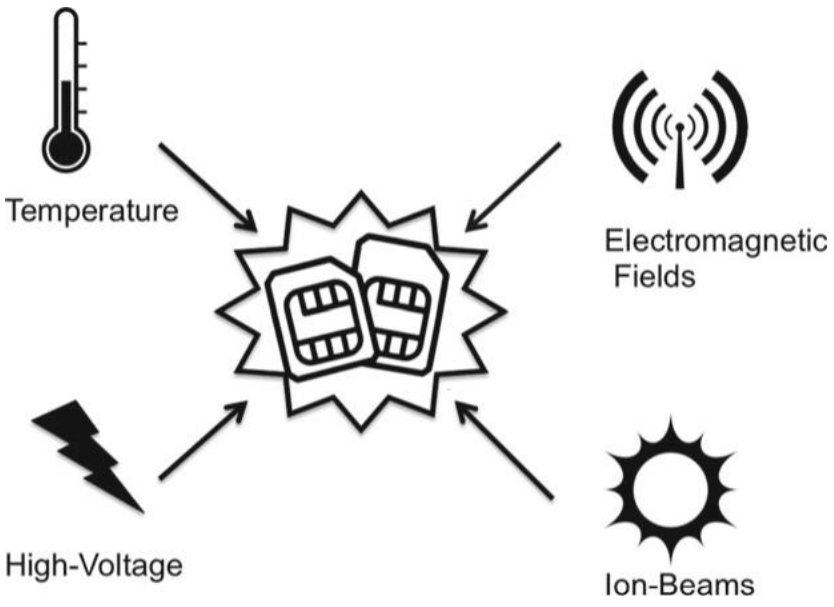
Η αντοχή έναντι τέτοιων επιθέσεων γίνεται σε εργαστήρια με χειροποίητες συσκευές στις οποίες είναι γνωστός ο αριθμός επιθέσεων. Δεν είναι αποτελεσματικό κάτι τέτοιο όμως για τους σχεδιαστές που θα πρέπει όσο γίνεται πιο έγκαιρα να βρουν το αντίμετρο. Αν και μπορεί τελικά να επιτευχθεί αντίσταση τη συσκευή, θα ήταν πιο αποτελεσματικό να δημιουργηθεί το αντίμετρο κατά το σχεδιασμό. Για να επιτευχθεί κάτι τέτοιο θα πρέπει να υπάρχουν τα κατάλληλα εργαλεία προσομοίωσης της συμπεριφοράς της συσκευής κατά την επίθεση έτσι ώστε να γίνεται σύγκριση των διάφορων αντιμέτρων.

1. Τεχνικές Έγχυσης Σφαλμάτων

Οι τεχνικές έγχυσης σφαλμάτων είναι ενεργητικές επιθέσεις που ο επιτιθέμενος χρησιμοποιεί εργαλεία παραποίησης για να μπορέσει να δημιουργήσει αυτά τα σφάλματα.

Οι τεχνικές διακρίνονται σε δυο ευρείς κατηγορίες, τις παγκόσμιες και τις τοπικές. Ως προς τις παγκόσμιες αυτό που έχουμε να παρατηρήσουμε είναι το χαμηλό κόστος εξοπλισμού και ότι τα σφάλματα είναι τυχαία. Αυτό έχει σαν αποτέλεσμα να χρειάζεται περισσότερος χρόνος για να βρεθούν τα σωστά σφάλματα. Σε τοπικό επίπεδο ανεβαίνει το κόστος ου εξοπλισμού αλλά οι επιθέσεις είναι πιο πετυχημένες.

Το σφάλμα που εγχέεται το ονομάζουμε μοντέλο σφάλματος, έχει δυο σημαντικές παραμέτρους την τοποθεσία και τον αντίκτυπο. Ως τοποθεσία ονομάζουμε τη χρονική στιγμή αλλά και τη θέση που γίνεται η έγχυση του σφάλματος στον αλγόριθμο στόχο. Επίσης εξαρτάται από την ακρίβεια της τεχνικής και μπορεί να είναι σε επίπεδο bit, μεταβλητών ή τυχαία. Όσον αφορά τον αντίκτυπο, είναι η επίπτωση που θα έχει το σφάλμα στα δεδομένα. Συνήθεις επιπτώσεις είναι, κόλλημα, αντιστροφή bit, τυχαίο byte, ή ανομοιόμορφη κατανομή τιμών.



Εικόνα 0.1.1 Σχηματική Απεικόνιση Τεχνικών Έγχυσης Σφαλμάτων

1.1 Κατηγορίες Σφαλμάτων

1.1.1 Έγχυση Σφάλματος μέσω Τροφοδοσίας

Το κάθε ενσωματωμένο σύστημα τροφοδοτείται είτε από μπαταρία είτε από εξωτερική τροφοδοσία. Σε αυτές λοιπόν τις περιπτώσεις είναι εύκολος και φυσικός ο τρόπος επίθεσης καθώς προκαλείται δυσλειτουργία απλά αλλάζοντας την τάση τροφοδοσίας. Οι τυπικές επιπτώσεις κατά την αλλαγή τροφοδοσίας είναι η αλλαγή στο χρόνο λειτουργίας των flip flop, τα οποία ενεργοποιούνται πριν φτάσει κάποιο σήμα ή κάποια τιμή. Τέτοιες τεχνικές μπορούν να χρησιμοποιηθούν για προσπεράσουν την εκτέλεση μια εντολής ενός μικροεπεξεργαστή. Η χρονική ακρίβεια της διοχέτευσης του σφάλματος εξαρτάται από την διάρκεια της πτώσης τάσης καθώς και το συγχρονισμό με τη συσκευή στόχο. Με την υποτροφοδότηση για μεγάλο χρονικό διάστημα μπορούν να διοχετευτούν σφάλματα του ενός bit και όσο συνεχίζει η τάση να βρίσκεται χαμηλά να αυξάνεται η πολυπλοκότητα. Αυτό μπορεί να επιτευχθεί εύκολα με βασικές γνώσεις και χωρίς να αφήσει ίχνη παραβίασης στη συσκευή. Το μειονέκτημα σε αυτή τη τεχνική είναι η χρονική ακρίβεια καθώς δεν μπορεί να προσδιοριστεί ο χρόνος που θα συμβεί το σφάλμα. Με αποτέλεσμα να πρέπει ο επιτιθέμενος να είναι σε εγρήγορση έτσι ώστε να μπορεί σε πραγματικό χρόνο να επιλέξει το σωστό σφάλμα και να απορρίψει τα λάθος.

1.1.2 Έγχυση Σφαλμάτων μέσω Ρολογιού

Τα σφάλματα που χρησιμοποιούνται κατά τη χρήση αυτής της τεχνικής είναι παρόμοια με αυτά στην περίπτωση τροφοδοσίας. Ο στόχος αυτών των επιθέσεων είναι συσκευές που χρησιμοποιούν εξωτερικό ρολόι που σηματοδοτεί όπως για παράδειγμα οι έξυπνες κάρτες. Ο επιτιθέμενος μπορεί να τροφοδοτήσει τις συσκευές με αλλαγμένο σήμα ρολογιού το οποίο μπορεί να είναι ένας παλμός μικρότερος από αυτόν που περιμένει το ρολόι της συσκευής. Οι παλμοί που παράγονται με αυτόν τον τρόπο είναι δυσλειτουργίες ρολογιού και πολλές φορές είναι μικρότεροι από τις αποκλίσεις που μπορούν να δεχτούν οι συσκευές με αποτέλεσμα να προκαλέσουν παραβίαση του χρόνου εγκατάστασης ή παράλειψη κάποιων εντολών κατά την εκτέλεση ενός προγράμματος. Τα σφάλματα είναι παροδικά και δεν

προκαλούν ζημιά στη συσκευή. Αυτός ο τύπος διοχέτευσης σφαλμάτων έχει τα ίδια αποτελέσματα με την υποτροφοδοσία και μπορεί ν επιτευχθεί με εξοπλισμό χαμηλού κόστους.

1.1.3 Έγχυση Σφαλμάτων μέσω Θερμοκρασίας

Όλα τα ηλεκτρονικά κυκλώματα είναι κατασκευασμένα με τέτοιο τρόπο που έχουν ένα ανώτερο και ένα κατώτερο όριο θερμοκρασίας. Εκτός αυτού του εύρους θερμοκρασιών δεν μπορεί να εγγυηθεί κανείς ότι το κύκλωμα μπορεί να λειτουργήσει κανονικά. Πιθανές επιπτώσεις είναι τροποποίηση στο περιεχόμενο μνήμης της συσκευής αλλά και περιορισμένη λειτουργικότητα. Ο επιτιθέμενος μπορεί να προκαλέσει σφάλματα στη συσκευή είτε με το να την εκθέσει σε υψηλή θερμοκρασία είτε με το να πιέσει τη συσκευή να αυξήσει τη θερμοκρασία της. Ένα παράδειγμα είναι η πρόκληση μεγάλου αριθμού εντολών φόρτωσης και αποθήκευσης κάτι το οποίο μπορεί να αυξήσει τη θερμοκρασία της μνήμης. Η υπερβολή έκθεση σε θερμοκρασία υψηλή μπορεί να προκαλέσει μόνιμη βλάβη στο στόχο.

1.1.4 Έγχυση Σφάλματος μέσω Φωτός

Οι οπτικές επιθέσεις είναι ημι-επεμβατικές επειδή απαιτείται αφαίρεση τμήματος της συσκευής το οποίο θα χτυπηθεί με ελαφρύ παλμό φωτός ή με δέσμη λέιζερ. Ο παλμός φωτός ή η δέσμη λέιζερ μπορούν να κατευθυνθούν είναι στο μπροστά μέρος είτε στο πίσω ανάλογα με το είδος της επίθεσης. Στην πραγματικότητα όμως με την εξέλιξη της τεχνολογίας η από μπροστά επίθεση είναι σχετικά δύσκολη λόγω των πολλών μεταλλικών στρωμάτων τα οποία καλύπτουν πλέον το τσιπ. Οι παλμοί φωτός πρέπει να εστιαστούν σωστά με τη βοήθεια οπτικού μικροσκοπίου και φακού ώστε να εφαρμοστούν ακριβώς στο σωστό σημείο της επιφάνειας της συσκευής. Προκειμένου να αποφευχθεί η μόνιμη βλάβη στη συσκευή θα πρέπει να δοθεί μεγάλη προσοχή στην εστίαση των παλμών. Η ακρίβεια του παλμού φωτός είναι περιορισμένη όσο ο παλμός σκορπίζεται. Μεγαλύτερη ακρίβεια μας δίνει η δέσμη λέιζερ. Μπορεί επίσης να χρησιμοποιηθεί στο πίσω μέρος του τσιπ μήκος κύματος

υπέρυθρων. Η συγκεκριμένη τεχνική απαιτεί ακριβό εξοπλισμό και μπορεί να δημιουργήσει μόνιμη βλάβη. Παρόλα αυτά παρέχει μεγάλη ακρίβεια όσον φορά το αποτέλεσμα.

1.1.5 Έγχυση Σφάλματος μέσω Ηλεκτρομαγνητικού Πεδίου

Οι ηλεκτρομαγνητικοί παλμοί μπορούν να προκαλέσουν βλάβη στη μνήμη της συσκευής αλλά επίσης και στην ενεργοποίησή της. Αυτό οφείλεται στα λεγόμενα δινορεύματα τα οποία δημιουργούνται με τη χρήση ενός ενεργού πηνίου. Οι ηλεκτρομαγνητικοί παλμοί μπορούν να προκαλέσουν ένα σφάλμα πολύ ακριβές και εντοπισμένο σωστά ενώ ο εξοπλισμός που θα χρειαστεί είναι σχετικά φθηνός. Η επίθεση μπορεί να πραγματοποιηθεί εξωτερικά της συσκευής όμως θα πρέπει να γνωρίζουμε λεπτομέρειες σχετικά με τη διάταξη του τσιπ ώστε να είμαστε ακριβείς στο σημείο επίθεσης. Ένας παλμός μπορεί να διοχετευθεί από την ισχύς της συσκευής με αποτέλεσμα να επηρεάσει ομοιόμορφα όλη τη συσκευή ή μπορούμε με ένα μικρότερο πηνίο να κάνουμε επαγωγή ενός πρόσθετου ρεύματος σε ένα συγκεκριμένο μέρος του τσιπ. Η τεχνική αυτή δεν είναι πολύ αποτελεσματική σε συσκευές που χρησιμοποιούν γείωση ή μεταλλικές συσκευασίες.

1.1.6 Έγχυση Σφάλματος μέσω Εστιασμένης Δέσμης Ιόντων

Οι εστιασμένες δέσμες ιόντων είναι ένας ακριβός τρόπος διοχέτευσης σφαλμάτων σε μια συσκευή, ωστόσο δίνουν το δικαίωμα στον επιτιθέμενο να τροποποιήσει αυθαίρετα συγκεκριμένο κομμάτι του κυκλώματος. Ο επιτιθέμενος μπορεί να κόψει καλώδια, να προσθέσει συνδέσεις και να λειτουργήσει από διαφορετικά επίπεδα. Ο εξοπλισμός είναι πολύ ακριβός και χρειάζεται μεγάλη τεχνογνωσία αλλά η ακρίβειά του είναι πολύ υψηλή.

1.2 Επιθέσεις Σφαλμάτων

Οι επιθέσεις σφαλμάτων έχουν διαδοθεί σαν σοβαρή απειλή για τα ενσωματωμένα συστήματα όλο και περισσότερο τα τελευταία χρόνια. Οι επιθέσεις μπορούν να τροποποιήσουν έναν αλγόριθμο ή να τροποποιήσουν τη ροή του προγράμματος προς όφελος του εισβολέα.

1.2.1 Επιθέσεις Ειδικών Αλγορίθμων

Οι επιθέσεις σφαλμάτων σχεδιάζονται για να εκμεταλλευτούν συγκεκριμένα τρωτά σημεία του αλγορίθμου στόχου. Ωστόσο αυτή η επίθεση μπορεί να έχει αποτέλεσμα μόνο όταν ο εισβολέας έχει τη δυνατότητα να εισάγει το σφάλμα σε πολύ ακριβή χρονισμό και σε πολύ συγκεκριμένη θέση. Η ασφάλεια των ασύμμετρων κρυπτοσυστημάτων βασίζεται σε προβλήματα που είναι μαθηματικά δύσκολο να λυθούν. Οι επιθέσεις αυτές μπορούν να σχεδιαστούν να αποδυναμώσουν το πρόβλημα και να αποδυναμωθεί και η ασφάλεια του αλγόριθμου που βασίζεται σε αυτό. Κοινός στόχος για αυτού του είδους τις επιθέσεις είναι αλγόριθμοι κρυπτογράφησης δημόσιου κλειδιού.

1.2.2 Παραβίαση της Ροής Προγράμματος

Υπάρχει επίσης η τεχνική κατά την οποία διοχετεύονται σφάλματα με σκοπό την αλλαγή στη ροή ενός εκτελούμενο κώδικα λογισμικού. Ένα σφάλμα τέτοιου τύπου είναι η αλλαγή στο μετρητή ενός προγράμματος. Η εφαρμογή κρυπτογραφικών αλγορίθμων για να αλλάξει η ροή ενός προγράμματος μπορεί να είναι ένας ασφαλής τρόπος απειλής. Η παράλειψη εντολών στη ροή ενός προγράμματος αλλοιώνει το αποτέλεσμα σε κρίσιμο κομμάτι του αλγορίθμου με αποτέλεσμα να τον αποδυναμώνει. Έτσι συχνά το αντίμετρο είναι απλά πλεονασμός στους ελέγχους λογικής.

1.2.3 Ανάλυση διαφορικών σφαλμάτων

Οι ανάλυση διαφορικών σφαλμάτων είναι μια από τις πιο κοινές επιθέσεις για κρυπτογραφικούς αλγορίθμους. Η κύρια ιδέα είναι να διοχετευθούν σφάλματα έτσι ώστε να αλλάξουν τους υπολογισμούς του αλγορίθμου στόχου. Όταν μια διοχέτευση σφάλματος είναι επιτυχής αυτό φαίνεται στο κρυπτογραφημένο κείμενο εξόδου. Ο εισβολέας επίσης υπολογίζει το σωστό κρυπτογραφημένο κείμενο με τις ίδιες εισόδους. Με το μαζευτούν αρκετά ζεύγη σωστών – ελλαττωματικών κρυπτογραφημένων κειμένων μπορούν μετά να εφαρμοστούν τεχνικές διαφορικής ανάλυσης και να γίνει απόρριψη την υποψήφιων κλειδιών. Με την ακριβή διοχέτευση σφαλμάτων μπορεί ο εισβολέας να μειώσει τα βασικά υποψήφια κλειδιά σε μοναδικά.

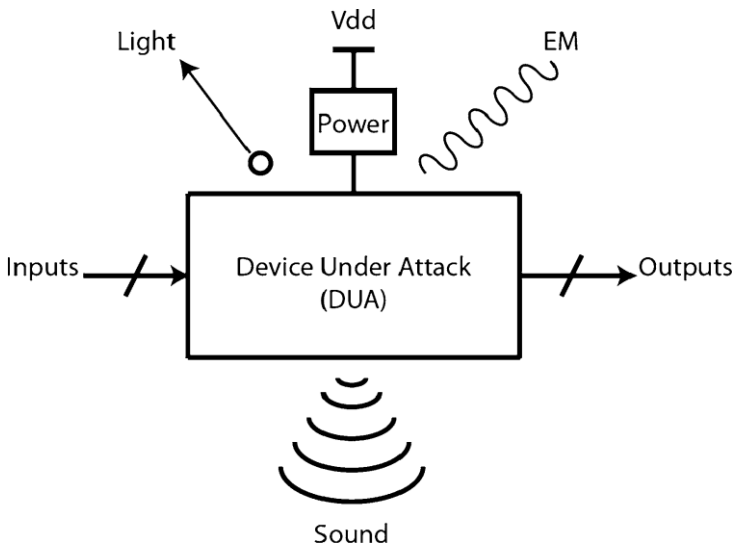
2. Επιθέσεις Πλευρικών Καναλιών

Η αδυναμία στην εφαρμογή κρυπτογραφικού συστήματος στο υλικό όσον αφορά τις εισόδους και τις εξόδους είναι αυτή που εκμεταλλεύονται πολλές φορές οι επιθέσεις πλευρικού καναλιού και παρακάμπτουν τη δύναμη του κρυπτογραφικού αλγόριθμου. Οι συνήθεις έξοδοι ενός πλευρικού καναλιού είναι η κατανάλωση ισχύος, οι ηλεκτρομαγνητικές εκροές, το φως και ο χρονισμός. Επίσης η τάση τροφοδοσίας είναι μια είσοδος ενός πλευρικού καναλιού. Άλλες βασικές πηγές πληροφοριών που ασχολείται η κρυπτογραφία είναι η θερμοκρασία, το φως και άλλες βασικές πηγές σημάτων πληροφορίας. Οι επιθέσεις συνδυάζουν τις περισσότερες φορές παρατήρηση της εξόδου του πλευρικού καναλιού, χειρισμό της εισόδου του πλευρικού καναλιού και παρατήρηση της αρχικής εξόδου για να χειριστούν τις μυστικές πληροφορίες. Οι επιθέσεις που έχουν σαν στόχο τις εξόδους είναι οι λεγόμενες παθητικές επιθέσεις πλευρικών καναλιών ενώ αυτές που στοχεύουν στις εισόδους είναι οι λεγόμενες ενεργητικές επιθέσεις πλευρικών καναλιών ή αλλιώς επιθέσεις διοχέτευσης σφάλματος.

Εδώ θα ασχοληθούμε κυρίως με τις παθητικές επιθέσεις πλευρικού καναλιού και για μέτρα σε ολοκληρωμένα κυκλώματα και ως προς το υλικό. Οι παθητικές επιθέσεις πλευρικού καναλιού επιτυγχάνουν επί το πλείστο καθώς στοχεύουν σε κρυπτογραφικά συστήματα μη

επεμβατικής φύσης, στα οποία απαιτείται μέτριος εξοπλισμός και υπολογιστές υψηλής απόδοσης για ανάλυση των δεδομένων. Οι εκπομπές πλευρικών καναλιών μπορεί να είναι υψηλές εκτός κι αν το σύστημα κρυπτογράφησης είναι σχεδιασμένο για χαμηλές εκπομπές.

Θα κάνουμε λοιπόν μια ανασκόπηση στις παθητικές επιθέσεις πλευρικού καναλιού και της προστασίας του υλικού, επειδή όμως δεν θα μας έφτανε ολόκληρη η εργασία για να το αναλύσουμε εκτενώς, θα επικεντρωθούμε στις πιο συχνά χρησιμοποιούμενες επιθέσεις πλευρικού καναλιού για να γίνουμε η αφετηρία για περισσότερη έρευνα και κατανόηση. Ξεκινώντας θα ασχοληθούμε με την βασική προέλευση μερικών εκπομπών πλευρικών καναλιών αλλά και των τεχνικών μέτρησης. Μετά θα ασχοληθούμε με το πώς μπορούμε να εκμεταλλευτούμε τις πληροφορίες των πλευρικών καναλιών για να επιτεθούμε σε κρυπτογραφικά μπλοκ. Τέλος θα εξετάσουμε τα αντιμέτρα υλικού για να αποφύγουμε τέτοιες επιθέσεις.

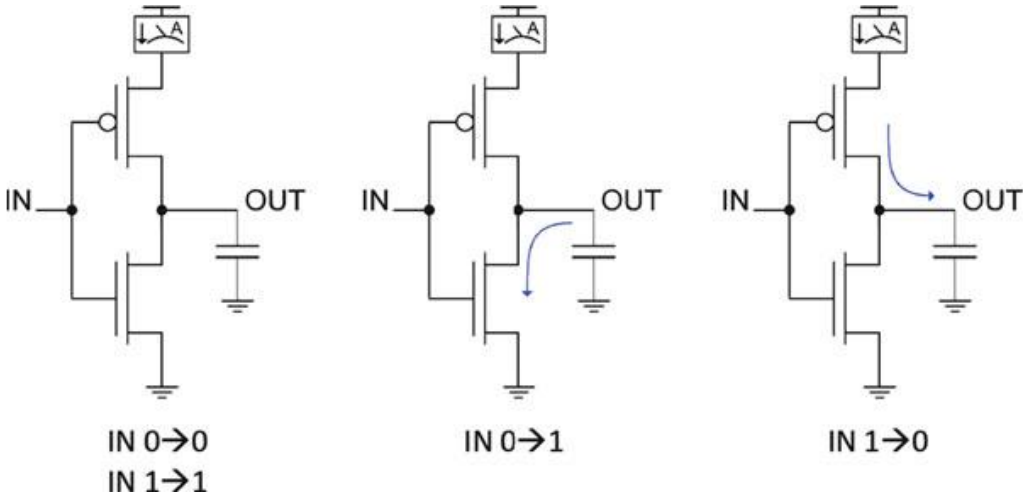


Εικόνα 0.1 Σχηματική Απεικόνιση Επιθέσεων Πλευρικών Καναλιών

2.1 Πλευρικά Κανάλια

Οι πρώτες μελέτες για περιπτώσεις επιθέσεων σε πλευρικά κανάλια κυρίως σχετικά με την κρυπτογραφία έγιναν κατά τη διάρκεια του 2^{ου} Παγκοσμίου Πολέμου. Οι υπάλληλοι της εταιρείας Bell Labs κατά τη διάρκεια πειραμάτων πάνω σε συστήματα κρυπτογραφίας

παρατήρησαν κάποιες επιδράσεις σε παλμογράφο σε άλλο δωμάτιο του εργαστηρίου κάθε φορά που ενεργοποιούνταν το σύστημα. Το πρόγραμμα TEMPEST της NSA ήταν μια μακρά έρευνα που χρηματοδοτήθηκε από την κυβέρνηση και είχε να κάνει με τις επιθέσεις σε πλευρικά κανάλια. Ένα μεγάλο μέρος από αυτή την πρώιμη εργασία έδειξε επιθέσεις και τα αποτελέσματά τους τα οποία χρησιμοποιούνται μέχρι και σήμερα. Όταν άρχισαν να δημοσιεύονται επιτυχημένες μελέτες και επιδείξεις επιθέσεων πλευρικών καναλιών ξεκίνησε να υπάρχει ενδιαφέρον από ακαδημαϊκούς και βιομηχανικούς κύκλους. Θα ασχοληθούμε με μερικές από τις πιο συνηθισμένες εκπομπές πλευρικών καναλιών.



Εικόνα 2.1 Στατικός μετατροπέας CMOS

Δεν μεταφέρεται δυναμική ισχύς εάν η είσοδος δεν αλλάξει. Για μετάβαση 0-σε-1 στην είσοδο, η φόρτιση απορρίπτεται στη γείωση. Για μετάβαση 1 σε 0 στην είσοδο, η φόρτιση τραβάει από Vdd

2.1.1 Κατανάλωση Ενέργειας

Η κατανάλωση ενέργειας ενός κρυπτογραφικού συστήματος είναι από τα πιο επιτυχημένα πλευρικά κανάλια στη σύγχρονη εποχή. Η κατανάλωση ενέργειας ενώ IC μπορεί να είναι είτε δυναμική είτε στατική. Η κατανάλωση ενέργειας λόγω φόρτισης ή λόγω εκτόνωσης των

χωρητικοτήτων των πυκνωτών αναφέρεται σαν δυναμική ισχύς. Λόγω των ακροδεκτών ενός τρανζίστορ αλλά και των καλωδίων που συνδέονται σε αυτό οποιοδήποτε κύκλωμα σε ένα σύστημα έχει χωρητικότητα. Το φορτίο είτε έλκεται στο Vdd του κυκλώματος είτε απορρίπτεται στο Gnd καθώς το κύκλωμα αλλάζει τάση σε ένα ψηφιακό σύστημα για δηλώσει μια κατάσταση 1 ή 0.

Η δυναμική ισχύς ενός κυκλώματος υπολογίζεται από τον τύπο: P(dynmic)= ½*C*Vdd*ΔV*f, όπου C είναι η χωρητικότητα του κυκλώματος, Vdd είναι η τάση τροφοδοσίας, ΔV είναι η διαφορά τάσης του κυκλώματος και f είναι η συχνότητα εναλλαγής. Επειδή μας ενδιαφέρουν οι μισές μεταβάσεις (0! 1 ή 1!0 ανάλογα με το αν μετράμε τη φόρτιση από το Vdd ή την εκφόρτιση από το Gnd) περιλαμβάνεται ο παράγοντας 1/2. Αυτό συχνά για ένα πλήρες σύστημα δηλώνεται ως εξής: Ptot(dynamic)= Σ(½*C*Vdd*ΔV*f). Αυτό πολλές φορές διατυπώνεται και ως f από τη συχνότητα του ρολογιού του συστήματος και το συντελεστή δραστηριότητας που ενσωματώνεται στο C (και αλλάζει σε Ceff).

Η στατική ισχύς παράγεται από κυκλώματα που αντλούν σκόπιμα στατική ισχύ ή από διαρροές ρεύματος σε τρανζίστορ. Παραδείγματα κυκλωμάτων που αντλούν στατικής ισχύς είναι τα αναλογικά κυκλώματα με πηγή ρεύματος και μερικές από τις ψηφιακές λογικές πύλες. Η διαρροή στο κανάλι υποκατωφλίου της συσκευής, η διαρροή αντίστροφης πόλωσης σύνδεσης PN και η διαρροή πύλης στα τρανζίστορ μπορούν να δημιουργήσουν ρεύμα διαρροής. Οι διηλεκτρικές μιας υψηλής Κ πύλης (και ως εκ τούτου μια μεταλλική πύλη) έχουν χρησιμοποιηθεί για να ενισχύσουν το πάχος της πύλης τρανζίστορ στα 45nm και για τεχνολογίες χαμηλής διεργασίας για τη σημαντική μείωση διαρροής μια πύλης. Η διαρροή ισχύος έχει εξελιχθεί σε μείζον ζήτημα και αποτελεί μέγιστο εμπόδιο στη βέλτιστη κλιμάκωση της τάσης τροφοδοσίας. Αποτέλεσμα αυτού η κλιμάκωση της τάσης τροφοδοσίας να είναι περιορισμένη και κατ' επέκταση και η εξοικονόμηση ενέργειας το ίδιο. Τα κυκλώματα που καταναλώνουν στατική ισχύς είναι χρονισμένα σε ορισμένα σχέδια ώστε να διασφαλίζεται ότι ενεργοποιούνται όταν απαιτείται.

Μια ή περισσότερες μεταλλικές συνδέσεις σε διαφορετικά επίπεδα συνθέτουν το δίκτυο τροφοδοσίας σε ένα τσιπ. Επειδή υπάρχουν ενώσεις με μεγαλύτερη αλλά και με μικρότερη αντίσταση, όταν πρόκειται για παγκόσμιας εμβέλειας δίκτυα επιλέγονται μέταλλα ανώτερης ποιότητας. Για τη σύνδεση των τρανζίστορ επιλέγεται χαμηλότερης ποιότητας μέταλλο για τη δημιουργία του πλέγματος. Οι μεγάλοι πυκνωτές τοποθετούνται μεταξύ Vdd και Gnd,

εκτός από το δίκτυο και χρησιμεύουν στο να σταθεροποιούν την τάση έναντι του θορύβου αλλά επίσης λειτουργούν και σαν πηγές φόρτισης λόγω των επαγωγών στο δίκτυο ηλεκτρικής ενέργειας. Αρκετά μπλοκ του τσιπ τροφοδοτούνται στο εσωτερικό του τσιπ με τις κολλήσεις αλλά και με άλλες συνδέσεις. Το μπλοκ τροφοδοσίας καταλαμβάνει συνήθως το μισό χώρο του τσιπ. Οι ρυθμιστές τάσης στην πλακέτα έχουν σαν σκοπό να μειώνουν τις υψηλές εξωτερικές τάσεις σε χαμηλότερες ανάλογα με τις απαιτήσεις του τσιπ. Αρκετά συστήματα επίσης χρησιμοποιούν δυναμική κλιμάκωση τάσης και συχνότητας για να μπορούν να τροποποιούν την ενέργεια ανάλογα με το φόρτο εργασίας.

Μια επίθεση ως προς την κατανάλωση ενέργειας ενός πλευρικού καναλιού βασίζεται στο γεγονός ότι ένα κύκλωμα διαχειρίζεται διαφορετικές ποσότητες ενέργειας ανάλογα με τα δεδομένα εισόδου. Κατά τη διάρκεια μιας κρυπτογραφικής λειτουργίας μια επίθεση μπορεί να προσδιορίσει πια μπλοκ του τσιπ είναι ενεργά εκείνη τη στιγμή και μια συγκεκριμένη ποσότητα δεδομένων που διαχειρίζονται. Η πιο χρησιμοποιούμενη οικογένεια λογικών πυλών είναι οι στατικές CMOS αλλά δεν διαχέει καμία δυναμικοί ισχύς αν οι είσοδοι είναι σταθερές, αλλά διαχέει μεγάλη δυναμική ισχύς αν η είσοδος αλλάξει συνδυαστικά με την έξοδο.

Επειδή η εξωτερική πηγή ρεύματος συνδέεται μόνο σε ένα σημείο και η ρυθμιζόμενη τάση φεύγει και από ένα σημείο, το πιο συχνό σημείο μέτρησης για ίχνη ισχύος είναι είτε πριν την πλακέτα είτε μετά. Η ισχύς προέρχεται συχνά από το επίπεδο PCB και στη συνέχεια με πολλές ακίδες δρομολογείτε στο IC με αποτέλεσμα να είναι δύσκολη η απομόνωση πέρα απ’ το ενσωματωμένο VRM. Η κυριότερη μέθοδος μέτρησης είναι η τοποθέτηση αντίστασης στον τροφοδοτικό και η μέτρηση της τάσης σε αυτό. Έτσι μπορούμε να προσδιορίσουμε το ρεύμα και την τάση σε αυτό. Μειώνουμε την πτώση τάσης στην αντίσταση χρησιμοποιώντας μια χαμηλής τιμής αντίσταση κάτι που επηρεάζει την παρατηρούμενη τάση. Ένας ανιχνευτής ρεύματος ο οποίος πολλές φορές ονομάζεται και σφιγκτήρας ισχύος μπορεί να χρησιμοποιηθεί για τη μέτρηση ρεύματος από ένα καλώδιο της πηγής ισχύος στην πλακέτα με μη επεμβατικό τρόπο. Οι ανιχνευτές ρεύματος βασίζονται στο φαινόμενο Hall και μπορούν να χρησιμοποιηθούν για τη μέτρηση εναλλασσόμενου και συνεχούς ρεύματος αν και η εφαρμογή τους θεωρείται σαν μέτρηση HM πλευρικού καναλιού παρά την κατανάλωση ενέργειας.

Λόγω της πολυπλοκότητας των σύγχρονων πολυπύρηνων επεξεργαστών και των SoC, πολλές επιθέσεις προσπαθούν να εντοπίσουν καλύτερα τη μέτρηση ισχύος ενός

κρυπτογραφικού μπλοκ. Οι συνδέσεις Vdd και Gnd είναι κοινές ακόμη και σε μεγάλα IC. Οι επιθέσεις πιθανότατα θα μπορούσαν να επιτύχουν μεγαλύτερο ίχνος ισχύος SNR εάν αυτό διαχωριζόταν από αυτό που βρίσκεται πιο κοντά στο κρυπτογραφικό μπλοκ. Μεμονωμένες συνδέσεις τροφοδοσίας μπορούν να απομονωθούν χρησιμοποιώντας διάφορους τρόπους ακόμη και με χρήση μικρών επαγωγικών βρόγχων. Το φιλτράρισμα υψηλής συχνότητας τροφοδοσίας συνήθως παρακάμπτεται.

2.1.2 Ηλεκτρομαγνητισμός

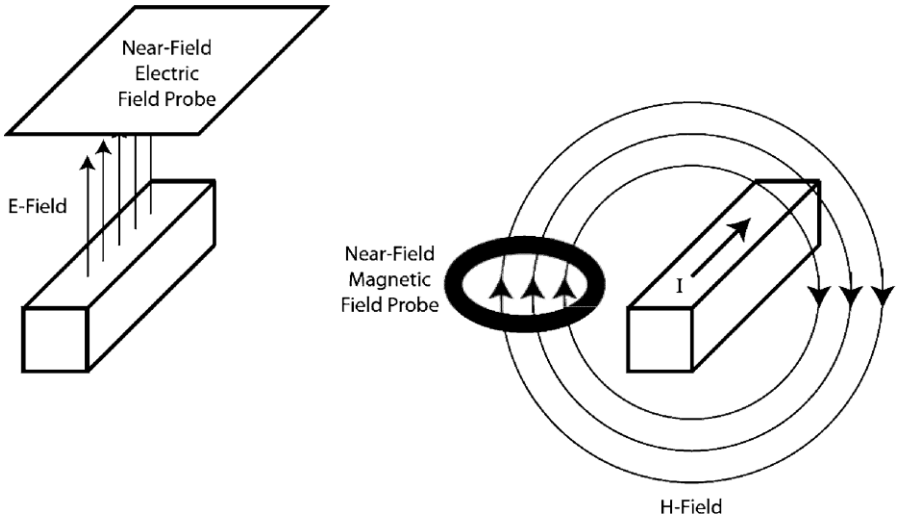
Η επιτάχυνση των φορτίων σε έναν αγωγό, που αναφέρεται ως κεραία, προκαλεί ηλεκτρομαγνητικές εκπομπές. Τα φαινόμενα ηλεκτρικού και μαγνητικού πεδίου πρωταγωνιστούν στο εκπεμπόμενο κύμα, το οποίο ορίζεται ως χώρος ανάμεσα σε δυο μήκη κύματος μιας κεραίας. Η δύναμη ωστόσο μειώνεται όσο απομακρυνόμαστε από την κεραία με τέτοιο ρυθμό όσο το τετράγωνο της απόστασης. Η περιοχή κοντινού πεδίου μπορεί να είναι αρκετά μεγάλη για τις συχνότητες ενδιαφέροντος. Ένα σήμα 1 MHz για παράδειγμα έχει μήκος κύματος 300μ. Οι εκπομπές υψηλής συχνότητας από την άλλη έχουν μικρότερο εύρος πεδίου, για παράδειγμα ένα σήμα 10 GHz έχει μήκος κύματος 3 εκατοστά. Το μακρινό εύρος είναι η περιοχή μεταξύ δυο μηκών κύματος και του άπειρου όπου η ακτινοβολούμενη ισχύς κύματος κυριαρχεί. Η ισχύς του ακτινοβολούμενου κύματος μειώνεται τόσο όσο το τετράγωνο της απόστασης. Επειδή λοιπόν η ισχύς στο μακρινό πεδίο είναι μικρότερη από το κοντινό, για ανίχνευση χρησιμοποιείται πάντα το κοντινότερο πεδίο.

Οι ηλεκτρομαγνητικές εκπομπές επηρεάζουν εύκολα άλλα σήματα στη συσκευή ιδιαίτερα μέσω επαγωγικής ή χωρητικής σύζευξης κοντινού εύρους. Με τη χρήση άλλων σημάτων σαν φορείς μπορούμε να παρατηρήσουμε προσεγγιστικά σήματα ενδιαφέροντος. Λόγω ηλεκτρομαγνητικών ζεύξεων, οι ερευνητές έχουν ανιχνεύσει τη διαμόρφωση πλάτους αλλά και τη διαμόρφωση συχνότητας των σημάτων φορέων. Λόγω των μεγάλων ηλεκτρομαγνητικών εκπομπών, το σήμα ρολογιού αλλά και η παροχή τροφοδοσίας είναι καλοί φορείς. Οι ηλεκτρομαγνητικές εκπομπές χωρίζονται σε δυο κατηγορίες: τις σκόπιμες, άμεσες εκπομπές από το σήμα ενδιαφέροντος και τις ακούσιες εκπομπές που προκαλούνται από το συνδυασμό του σήματος ενδιαφέροντος και των σημάτων φορέων.

Ο εντοπισμός της πηγής σήματος μπορεί να είναι δύσκολος στις σύγχρονες γεωμετρίες παραγωγής IC λόγω της μεγάλης πυκνότητας των κεραιών εκπομπής. Η τοποθέτηση και ο προσανατολισμός του αισθητήρα καθώς και η χρήση πολλών αισθητήρων μπορούν να βοηθήσουν στο να εντοπιστεί μια πηγή και ν βελτιωθεί η ισχύς του σήματος καθώς και το SNR. Η τοποθέτηση και ο προσανατολισμός των αισθητήρων κοντινού εύρους ζώνης πιθανόν να έχει σημαντικό αντίκτυπο στο SNR που λαμβάνεται. Οι κεραίες σε ολοκληρωμένα κυκλώματα κατά κύριο λόγο είναι μεταλλικές κατασκευές οι οποίες είναι παράλληλες με το επίπεδο του πυριτίου. Αυτές είναι διασυνδέσεις μπορεί να είναι τόσο μικρές όσο ένα micron ή αρκετά χιλιοστά.

Τα πεδία που εκπέμπονται κοντά στο τσιπ είναι παράλληλα με την επιφάνεια του πυριτίου. Οι αισθητήρες ηλεκτρικού και μαγνητικού κοντινού πεδίου προσανατολίζονται καλύτερα σε επίπεδο παράλληλο με το επίπεδο του πυριτίου όταν τοποθετούνται κοντά στο τσιπ. Απαιτείται μεγαλύτερη αναλογία σήματος προς θόρυβο για να πλησιάσουμε φυσικά το τσιπ και να μπορέσουμε να αφαιρέσουμε οτιδήποτε από τη συσκευασία του εξασθενεί το σήμα ενδιαφέροντος. Λόγω του μειωμένου θορύβου στις υψηλές συχνότητες, οι υψηλές συχνότητες συνήθως προτιμώνται από τις εκπομπές σημάτων χαμηλής συχνότητας.

Οι απλές HM επιθέσεις και οι διαφορικές HM επιθέσεις είναι δυο τύποι επιθέσεων που εκμεταλλεύονται τα HM πλευρικά κανάλια. Οι απλές επιθέσεις καθορίζουν την εσωτερική λειτουργία χρησιμοποιώντας μόνο HM ίχνος, ενώ οι διαφορικές επιθέσεις είναι ανώτερης τάξης καθώς συλλέγουν πολλά ίχνη ώστε να αυξήσουν την πιστότητα του συλλεγόμενου σήματος. Έχει παρατηρηθεί ότι τα HM πλευρικά κανάλια συνδέονται με τα πλευρικά κανάλια ισχύος, υποδεικνύοντας πολλές φορές πως η διαρροή από HM πλευρικό κανάλι σχετίζονταν σε κάθε περίπτωση με μια συσκευή υπό επίθεση που είχε διαρροή σε πλευρικό κανάλι ισχύος. Απ’ την άλλη πλευρά τα ηλεκτρικά αντίμετρα πλευρικού καναλιού μπορεί να μην ελαχιστοποιήσουν τις εκπομπές του HM πλευρικού καναλιού και σε κάποιες περιπτώσεις τις αυξάνουν σημαντικά.



Εικόνα 2.1.2 Ο βέλτιστος προσανατολισμός του αισθητήρα ηλεκτρικού και μαγνητικού πεδίου είναι σε παράλληλο επίπεδο με το ολοκληρωμένο κύκλωμα.

2.1.3 Οπτικά

Για αρκετά χρόνια, είναι γνωστό ότι οι κινητοί φορείς, συμπεριλαμβανομένων των ηλεκτρονίων, σε ένα κανάλι FET μπορούν να δημιουργήσουν εκπομπές ορατού ή υπέρυθρου φωτός. Έργα της IBM και προσπάθειες της Intel έχουν εκμεταλλευτεί πρόσφατα αυτά τα φαινόμενα για να βοηθήσουν στη δοκιμή IC και τον εντοπισμό σφαλμάτων συλλέγοντας εκπομπές φωτονίων στην επιφάνεια του τσιπ. Επειδή οι εκπομπές είναι ασυνήθιστες, το IC ανακυκλώνει πολλές φορές τις ίδιες εισόδους, με αποτέλεσμα έναν χάρτη εκπομπών.

Για να δημιουργηθεί ένας δισδιάστατος χάρτης εκπομπών φωτονίων, απαιτείται η τεχνική με μια σειρά από φωτοπολλαπλασιαστές που απλώνονται σε όλο τον ημιαγωγό. Μπορεί επίσης να χρησιμοποιηθεί μια κάμερα CCD ευαίσθητη στην περιοχή υπέρυθρων. Οι μεμονωμένες ενεργοποιήσεις πύλης ή συσκευής μπορούν να αναγνωριστούν χρησιμοποιώντας τέτοιες τεχνικές, αλλά απαιτούν μεγάλο αριθμό επαναλαμβανόμενων εισόδων και κατά συνέπεια εκτεταμένες περιόδους απόκτησης των δεδομένων. Ο μικρός αριθμός φωτονίων που εκπέμπονται από συσκευές MOSFET, καθώς και ο τεράστιος αριθμός πυκνά τοποθετημένων συσκευών σε ένα μεγάλο καλούπι που κατασκευάζεται με τη σύγχρονη διαδικασία, καθιστούν τη μέτρηση των εκπομπών φωτονίων από την εναλλαγή συσκευών MOSFET μια σοβαρή πρόκληση.

Μεταβάλλοντας την τάση ή το ρεύμα στο πυρίτιο, τα οπτικά χαρακτηριστικά του πυριτίου μπορούν να αλλάξουν. Σε συσκευές ανίχνευσης τάσης λέιζερ (LVP), οι αλλαγές ανακλαστικότητας των διασταυρώσεων p-n έχουν ανιχνευθεί από την πίσω πλευρά του τσιπ χρησιμοποιώντας σύντομους παλμούς φωτός από λέιζερ κλειδωμένου τρόπου λειτουργίας για την ανίχνευση αλλαγών τάσης κόμβου. Αυτές οι μέθοδοι περιορίζονται σε μικρό αριθμό μετρήσεων και λαμβάνονται ταυτόχρονα. Η άμεση ανάγνωση των τιμών των εσωτερικών κόμβων αποθήκευσης ενός IC καθώς και η παρατήρηση των ενδιάμεσων τιμών κόμβου υπολογισμού κατά τη λειτουργία γίνονται με τις προσεγγίσεις LVP.

Οι προσεγγίσεις οπτικής παρατήρησης βασίζονται στο IC που λειτουργεί σε επαναλαμβανόμενο σύγχρονο βρόχο λόγω της χαμηλής πιθανότητας σύλληψης εκπεμπόμενων φωτονίων (ορισμένοι ερευνητές βάζουν την πιθανότητα σύλληψης σε λιγότερο από 0,1 τοις εκατό). Οι προσεγγίσεις σχεδίασης που προκαλούν τυχαίες καθυστερήσεις στη λογική μπορεί να κάνουν την οπτική παρατήρηση πιο δύσκολη και ανακριβή, απαιτώντας μεγαλύτερες διαδρομές παρατήρησης για να επιτευχθούν εύλογα ακριβή αποτελέσματα.

2.1.4 Χρονισμός και Καθυστέρηση

Οι επιθέσεις χρονισμού σε κρυπτογραφικούς αλγόριθμους εκμεταλλεύονται τις αλλαγές στον χρόνο υπολογισμού που απαιτείται από τα δεδομένα. Η πρώτη εργασία για επιθέσεις και αντίμετρα πλευρικού καναλιού δημοσιεύτηκε το 1996 η οποία πυροδότησε μια σημαντική ερευνητική προσπάθεια στη βιομηχανία και τον ακαδημαϊκό κόσμο σχετικά με τις επιθέσεις και τις άμυνες πλευρικών καναλιών. Οι επιθέσεις χρονισμού εκμεταλλεύονται τον χρόνο που χρειάζεται για να ολοκληρωθεί ένας υπολογισμός. Εάν κατά τη λειτουργία γίνει μια επιλογή ροής ελέγχου που εξαρτάται από δεδομένα και οι διαφορετικοί κλάδοι έχουν τυχαίες καθυστερήσεις, οι πληροφορίες μπορούν να χρησιμοποιηθούν για τον προσδιορισμό της κατάστασης της μεταβλητής ελέγχου. Αυτές οι επιθέσεις έχουν χρησιμοποιηθεί κυρίως σε συστήματα που βασίζονται σε CPU, όπου η καθυστέρηση επεξεργασίας υπολογίζεται σε κύκλους ρολογιού της CPU.

Η καθυστέρηση ενός συγκεκριμένου λογικού μπλοκ μπορεί, να μετρηθεί και να χρησιμοποιηθεί στο πλαίσιο αποκλειστικού υλικού. Οι μεμονωμένες καθυστερήσεις μπλοκ

δεν είναι εξωτερικά παρατηρήσιμες στις κύριες εξόδους σε σύγχρονα συστήματα, καθώς τα λειτουργικά μπλοκ συχνά οριοθετούνται από χρονομετρημένες μονάδες αποθήκευσης (π.χ. flip-flop). Όμως, με την εξέταση ενός άλλου πλευρικού καναλιού, μπορεί να υπολογιστεί η καθυστέρηση του μπλοκ (π.χ. οπτικές εκπομπές). Επειδή η καθυστέρηση ενός λειτουργικού μπλοκ ή ολόκληρη η λειτουργία μπορεί να είναι ορατή στην κύρια έξοδο σε ασύγχρονα συστήματα, πρέπει να μεριμνήσουμε στο σχεδιασμό του συστήματος για να αποφευχθεί η διαρροή πληροφοριών χρονισμού.

Ο χειρισμός του ρολογιού είναι μια εναλλακτική μέθοδος για τον προσδιορισμό της καθυστέρησης ενός λειτουργικού μπλοκ σε ένα σύγχρονο σύστημα. Μια επίθεση θα μπορούσε να μειώσει ή να παρατείνει έναν συγκεκριμένο κύκλο ρολογιού ενός υπολογισμού εάν είχε πρόσβαση στα εργαλεία συντονισμού ενός σύγχρονου δέντρου διανομής ρολογιού. Η καθυστέρηση της λειτουργίας θα αντικατοπτρίζεται στην ελάχιστη περίοδο λειτουργίας του ρολογιού.

2.1.5 Ηχητικά

Για αρκετά χρόνια, οι εισβολείς έχουν χρησιμοποιήσει ακουστικές επιθέσεις πλευρικού καναλιού σε συστήματα μακρο-κλίμακας. Οι πράκτορες των βρετανικών μυστικών υπηρεσιών βρήκαν τις αρχικές θέσεις των αιγυπτιακών μηχανών κρυπτογράφησης ακούγοντας την επαναφορά των τροχών κλειδιών στη δεκαετία του 1950, επιτρέποντάς τους να παραβιάσουν την κρυπτογράφηση. Οι ερευνητές έχουν χρησιμοποιήσει πρόσφατα εκπομπές ακουστικών πλευρικών καναλιών για να διακρίνουν το κείμενο που παράγεται από εκτυπωτές κουκκίδων και το πλήκτρο που χτυπιέται σε ένα πληκτρολόγιο. Παρόλα αυτά, μόνο ένας μικρός όγκος έρευνας έχει γίνει σχετικά με τη χρήση εκπομπών ακουστικών πλευρικών καναλιών σε μικροηλεκτρονικές συσκευές, κυρίως από τους Shamir και Tromer.

Έλεγξαν αν μπορούσαν να καταλάβουν πότε χρησιμοποιήθηκε η κρυπτογράφηση RSA τοποθετώντας μικρόφωνα κοντά σε έναν συμβατικό οικιακό υπολογιστή. Κατάφεραν έτσι να κάνουν διάκριση όχι μόνο μεταξύ άλλων δραστηριοτήτων και της κρυπτογράφησης RSA, αλλά και μεταξύ διαφόρων εκτελέσεων RSA με διαφορετικά κλειδιά. Θεωρούσαν ότι οι ακουστικές εκπομπές προκλήθηκαν από τις πιεζοηλεκτρικές δυνατότητες των κεραμικών πυκνωτών που χρησιμοποιούνται για το φιλτράρισμα τροφοδοσίας και τη μετατροπή AC σε

DC στη μητρική πλακέτα. Οι ακουστικές εκπομπές μπορεί να είναι ένα υποπροϊόν της ζήτησης ρεύματος τροφοδοσίας και επομένως να αναλυθούν με τον ίδιο τρόπο όπως η ανάλυση τροφοδοσίας, αλλά σε μια φιλτραρισμένη μορφή χαμηλής διέλευσης. Με αποτέλεσμα, τα αντίμετρα που στοχεύουν στην ανάλυση ισχύος μπορεί επίσης να είναι αποτελεσματικά έναντι της ανάλυσης του ακουστικού πλευρικού καναλιού.

Ένας άγνωστος τομέας έρευνας είναι εάν τα ακουστικά κύματα θα μπορούσαν να χρησιμοποιηθούν ως είσοδος πλευρικού καναλιού ενός συστήματος. Θεωρητικά, ένας μηχανικός κραδασμός μπορεί να χρησιμοποιηθεί για την παραγωγή θορύβου στο τροφοδοτικό μέσω του ίδιου καναλιού με το πιεζοηλεκτρικό φαινόμενο. Επίσης, οποιοδήποτε μέρος του συστήματος βασίζεται σε μηχανικά εξαρτήματα (όπως η μονάδα σκληρού δίσκου) μπορεί να υποστεί ακουστικούς/μηχανικούς κραδασμούς, οι οποίοι ενδέχεται να προκαλέσουν προβλήματα ή να αλλάξουν τη συμπεριφορά του.

2.2 Αντίμετρα

Οι ερευνητές ερευνούν λύσεις για την αποτροπή επιθέσεων πλευρικού καναλιού από την ανακάλυψη διαρροής ΗΜ πλευρικού καναλιού από μηχανή κρυπτογράφησης των ΗΠΑ κατά τη διάρκεια του Β 'Παγκοσμίου Πολέμου. Αυτά τα αντίμετρα χωρίζονται σε διάφορες κατηγορίες: Φυσική Ασφάλεια, Απόκρυψη, Κάλυψη / Τύφλωση και Διαμέριση Σχεδιασμού.

2.2.1 Φυσική Ασφάλεια

Για τη μέγιστη ανίχνευση πλευρικού καναλιού SNR, ο εισβολέας χρειάζεται συχνά φυσική πρόσβαση στο DUA για εκτεταμένη χρονική περίοδο και μπορεί να χρειαστεί να χρησιμοποιήσει επεμβατικές προσεγγίσεις (π.χ. αποκάψωση, αλλαγή πλακέτας ή τσιπ). Με αποτέλεσμα, η άρνηση της εγγύτητας, της πρόσβασης και της κατοχής του εισβολέα είναι κρίσιμη για τον περιορισμό της ικανότητας του αντιπάλου να εξαπολύει επιθέσεις πλευρικού καναλιού.

Η φυσική ασφάλεια της ζώνης γύρω από το τσιπ, για παράδειγμα, μπορεί να εμποδίσει την ανίχνευση του ΗΜ πλευρικού καναλιού επειδή οι εκπομπές ΕΜ υψηλότερης ισχύος πρέπει να ανιχνεύονται κοντά στο τσιπ. Σύμφωνα με τα έγγραφα TEMPEST που αποκαλύφθηκαν

πρόσφατα, η κυβέρνηση των ΗΠΑ απαιτεί μια ζώνη προστασίας 200 ποδιών γύρω από τα κέντρα κρυπτογράφησης. Η έκταση της απαιτούμενης ασφαλούς ζώνης καθορίστηκε περισσότερο από την εκτίμηση της NSA για το τι θα μπορούσε πρακτικά να διασφαλιστεί παρά από την τεχνική βιωσιμότητα της ανίχνευσης ΗΜ εκπομπών. Τα σήματα σε χαμηλές συχνότητες (π.χ. 1 MHz) έχουν μήκη κύματος που εκτείνονται πέρα από 200 πόδια, με αποτέλεσμα ζώνες κοντινού εύρους να εκτείνονται πέρα από 200 πόδια.
Οι ερευνητές αναγνώρισαν την ανάγκη να τοποθετηθεί το μικρόφωνο κοντά στο DUA σε προηγούμενη εργασία σε ακουστικά πλευρικά κανάλια. Αυτή η απαίτηση θα μπορούσε να θεωρηθεί ως περιορισμός αυτού του τύπου επίθεσης, αλλά υπάρχει μια σειρά από τεχνολογίες μικροφώνου μεγάλης εμβέλειας που χρησιμοποιούν ανακλώμενο φως (π.χ. υπέρυθρη δέσμη ή λέιζερ) για την ανίχνευση ηχητικών δονήσεων και συνεπώς την εξάλειψη της ανάγκης για φυσική εγγύτητα ή ακόμα και άμεσης φυσικής πρόσβασης στο DUA. Έτσι, θα απαιτείται ακουστική θωράκιση του περιβάλλοντος χώρου που περιβάλλει το DUA.

2.2.2 Απόκρυψη

Ένας εισβολέας που εκμεταλλεύεται μια έξοδο πλευρικού καναλιού ελπίζει να λάβει αρκετές πληροφορίες από το πλευρικό κανάλι για να συλλέξει ορισμένες μυστικές πληροφορίες σχετικά με τη λειτουργία του τσιπ. Αυτό έχει σαν σκοπό, αναζητούν έναν τρόπο να ανακτήσουν ένα σήμα από το πλευρικό κανάλι, το οποίο είναι συχνά θορυβώδες. Αυτή η διαδικασία μπορεί να θεωρηθεί ως μια προσπάθεια αύξησης του λόγου σήματος προς θόρυβο (SNR) των πληροφοριών του πλευρικού καναλιού όσο είναι εφικτό. Με αποτέλεσμα, πολλά αντίμετρα να στοχεύουν στη μείωση του SNR είτε ενισχύοντας το θόρυβο είτε μειώνοντας το σήμα.

2.2.2.1 Γεννήτριες θορύβου

Η αύξηση του θορύβου είναι μια τεχνική για τη μείωση του SNR. Για την αντιμετώπιση επιθέσεων πλευρικού καναλιού, αρκετοί ακαδημαϊκοί έχουν υποστηρίξει την προσθήκη γεννητριών θορύβου σε ασφαλή IC. Οι σχεδιαστές έχουν προτείνει την προσθήκη κυκλωμάτων που απορροφούν τυχαίες ποσότητες ισχύος κατά τη λειτουργία του τσιπ ή που

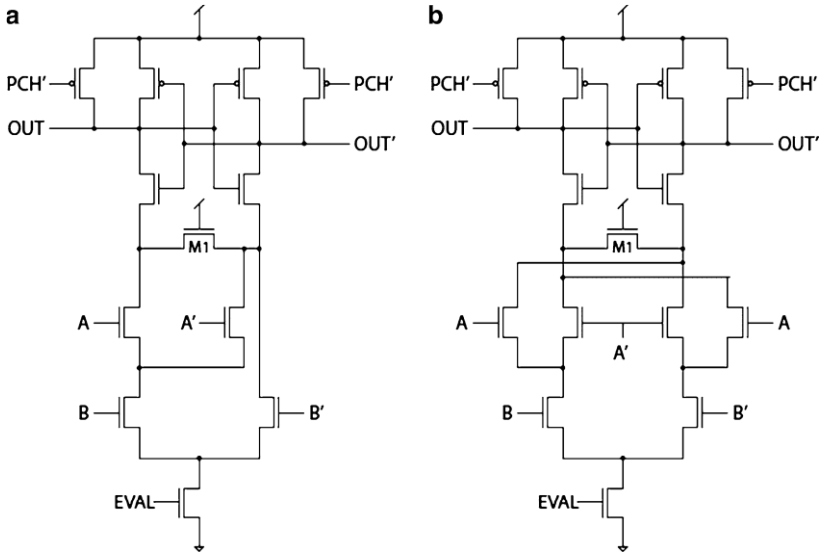
διατηρούν σταθερή τη συνολική απαγωγή ισχύος συμπληρώνοντας τη διαρροή ισχύος εάν είναι μικρότερο από ένα προκαθορισμένο επίπεδο. Οι ερευνητές έχουν προτείνει την ενσωμάτωση κυκλωμάτων με τυχαία καθυστέρηση στη λογική διαδρομή για την πρόληψη επιθέσεων χρονισμού. Ωστόσο, η προσθήκη αυτού του τύπου κυκλώματος σε σύγχρονα συστήματα που πρέπει να περάσουν από όλες τις λογικές διαδρομές μέχρι το τέλος της περιόδου ρολογιού μπορεί να δημιουργήσει ένα δίλημμα. Οποιαδήποτε παρατήρηση πλευρικού καναλιού που βασίζεται σε δειγματοληψία (π.χ. οπτική εκπομπή) ή ευθυγράμμιση ίχνους θα είναι πιο δύσκολη με τυχαιοποιημένες καθυστερήσεις. Για τη μείωση του SNR κατά τη διάρκεια HM επιθέσεων, μπορεί να εφαρμοστεί EM θόρυβος. Το πρόβλημα είναι ότι το φάσμα εκπομπών είναι μάλλον ευρύ, καθιστώντας αναγκαία μια σημαντική ποσότητα πρόσθετου θορύβου σε ένα ευρύ φάσμα συχνοτήτων. Οι ενοποιητές συστημάτων των οποίων τα σχέδια πρέπει να περάσουν από κυβερνητικές δοκιμές για ηλεκτρονικές παρεμβολές αντιμετωπίζουν ένα δίλημμα με ένα τέτοιο HM δυνατό τσιπ. Επιπλέον, οι παραγωγοί θορύβου θα απαιτούσαν μεγάλη ποσότητα ηλεκτρικής ενέργειας, αν όχι νεκρή περιοχή. Τέλος, λόγω της σύζευξης σήματος, οι γεννήτριες θορύβου ενδέχεται να μην μπορούν να συνεισφέρουν θόρυβο σε όλες τις ακούσιες εκπομπές HM εκτός εάν βρίσκονται σε στρατηγική τοποθεσία. Η προσθήκη θορύβου στο πλευρικό κανάλι μπορεί να είναι αρκετή για να καταστήσει αδύνατες τις απλές επιθέσεις στο πλευρικό κανάλι, οι διαφορικές επιθέσεις θα απαιτήσουν περισσότερα ίχνη ή πιο περίπλοκη επεξεργασία σήματος.

2.2.2.2 Ισορροπημένη λογική

Μια άλλη τεχνική για τη μείωση του SNR είναι οι εκπομπές του πλευρικού καναλιού των λογικών πυλών να γίνουν ανεξάρτητες από τα δεδομένα που υποβάλλονται σε επεξεργασία. Η διαφορά των δεδομένων στις εκπομπές του πλευρικού καναλιού είναι η βάση πολλών επιθέσεων στα πλευρικά κανάλια (π.χ. ισχύς, EM, χρονισμός). Το πλευρικό κανάλι δεν θα μπορούσε πλέον να αξιοποιηθεί εάν οι λογικές εκπομπές ήταν ανεξάρτητες από τα επεξεργασμένα δεδομένα. Έχει αναπτυχθεί ένα σημαντικός αριθμός λογικών οικογενειών που παρουσιάζουν χαμηλή διαρροή πλευρικού καναλιού σε ένα δεδομένο πλευρικό κανάλι, όπως η ηλεκτρική ενέργεια. Όμως, όταν σχεδιάζετε πιο σκληρά λογικά στυλ, πρέπει να

δίνεται προσοχή γιατί η μείωση των εκπομπών σε ένα πλευρικό κανάλι μπορεί να οδηγήσει σε αυξημένες εκπομπές σε άλλο.

Αρκετοί τύποι συνεκτικής λογικής χρησιμοποιούν λογική προφόρτισης διπλής ράγας (DRP), στην οποία η πύλη έχει δύο εξόδους (έξοδος και έξοδος b) και λειτουργεί σε δύο φάσεις (επαναφορά και αξιολόγηση). Οι κόμβοι αρχικά επαναφέρονται σε γνωστές τιμές και, στη συνέχεια, οι μεταβάσεις είτε προς την έξοδο είτε έξοδο β αξιολογούνται στη φάση αξιολόγησης, αλλά όχι και οι δύο. Οι συνεκτικές πύλες είναι σχεδιασμένες έτσι ώστε οι εκπομπές του πλευρικού καναλιού από την έξοδο ή την έξοδο β να είναι κατά προτίμηση οι ίδιες. Οι κόμβοι εξόδου και εξόδου β μιας πύλης που έχουν γίνει πιο ανθεκτικοί έναντι της ανάλυσης ισχύος, για παράδειγμα, θα έχουν την ίδια χωρητικότητα και επομένως θα διαχέουν την ίδια ποσότητα δυναμικής ισχύος σε ένα συμβάν μεταγωγής. Η αντιστοίχιση της εξόδου και της εξόδου β, ειδικά σε ένα κανονικό σημείο κυψέλης και ροή σύνθεσης διαδρομής, είναι δύσκολη και απαιτεί εξειδικευμένα εργαλεία CAD. Οι εκπομπές πλευρικού καναλιού μπορούν επίσης να προκληθούν από αναντιστοιχίες στην εκφόρτιση των χωρητικοτήτων της εσωτερικής πύλης. Τα WDDL, SABL και η λογική διπλού διαστήματος είναι παραδείγματα αυτού του τύπου λογικής οικογένειας.



Εικόνα 2.2.2.2.1 Παράδειγμα λογικών πυλών προφόρτισης διπλής όδευσης: Λογική βασισμένη στον ενισχυτή αίσθησης (SABL)

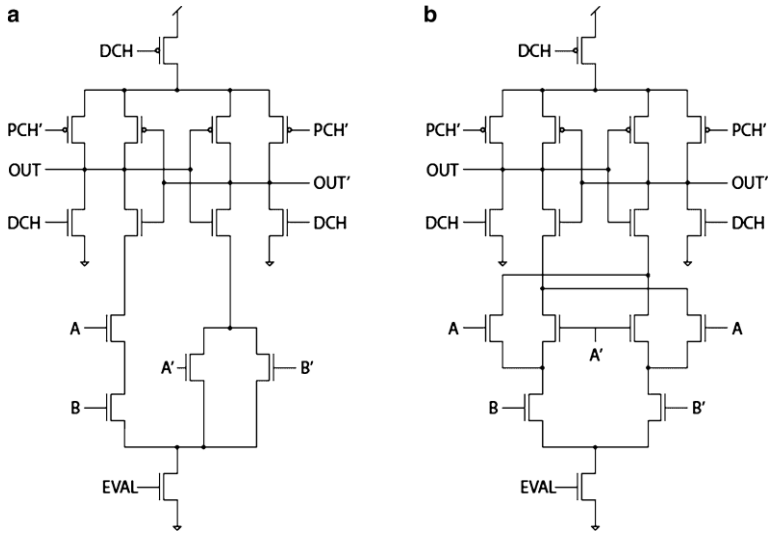
Οι ερευνητές ανέπτυξαν τρεις λογικές οικογένειες φάσεων, όπως το TDPL και το TSPL, για να εξαλείψουν την ανάγκη εξισορρόπησης των εξόδων. Έχουν τρεις φάσεις (προφόρτιση, αξιολόγηση και εκφόρτιση) και δεν απαιτούν εξισορρόπηση φορτίου εξόδου. Τα δύο πρώτα στάδια είναι πανομοιότυπα με το DRP, αλλά η τρίτη φάση εκφορτώνει όλους τους κόμβους εξόδου στη γείωση. Αυτό διασφαλίζει ότι σε κάθε κύκλο, ανεξάρτητα από τα δεδομένα εισόδου, όλες οι έξοδοι βλέπουν ένα συμβάν φόρτισης και εκφόρτισης, με αποτέλεσμα την ίδια απαγωγή ισχύος. Οι τρεις φάσεις λειτουργίας έχει επίσης επεκταθεί ώστε να λειτουργεί σε επίπεδο μπλοκ, επιτρέποντας στους σχεδιαστές να χρησιμοποιούν κοινά λογικά στυλ στο λειτουργικό μπλοκ πυρήνα, αλλά το λειτουργικό μπλοκ πυρήνα παραμένει ευαίσθητο στην HM επίθεση.

Αυτές οι λογικές οικογένειες απαιτούν επίσης τριφασικά μη επικαλυπτόμενα ρολόγια, δεν είναι όμως συνηθισμένος τύπος χρονισμού, αν και υπάρχουν τρόποι για να τα φτιάξετε. Απ' την άλλη πλευρά τα στυλ λογικής τριών φάσεων, βασίζονται στην αδυναμία του εισβολέα να διακρίνει μεταξύ των φάσεων της λειτουργίας. Η διάκριση μεταξύ των φάσεων σε συστήματα που λειτουργούν σε υψηλές συχνότητες (δηλαδή στην περιοχή GHz) και περιέχουν συσκευές σταθεροποίησης τροφοδοσίας (π.χ. χωρητικότητα αποσύνδεσης, ρυθμιστές τάσης) μπορεί να είναι δύσκολη. Ωστόσο, αυτό σημαίνει ότι τα σχέδια που χρησιμοποιούν αυτές τις λογικές οικογένειες πρέπει να διαθέτουν δικλείδες ασφαλείας ώστε να αποτρέπεται η παρέμβαση στο χρονομετρητή του συστήματος από έναν εισβολέα.

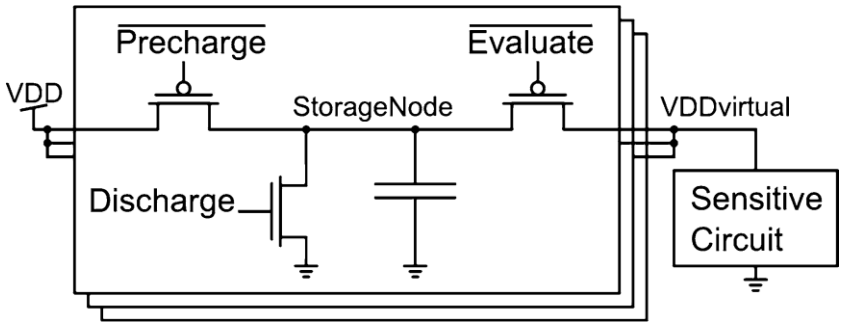
Το φαινόμενο πρόωρης διάδοσης (EPE), το οποίο οδηγεί σε διαρροή πληροφοριών μέσω του χρονισμού μεταγωγής εξόδου, είναι ένα άλλο πρόβλημα με τις λογικές οικογένειες. Μια λογική πύλη μπορεί να αλλάξει την έξοδο της στην τελική της τιμή πριν φτάσουν όλες οι είσοδοι, ανάλογα με τη λογική συνάρτηση και τις τιμές εισόδου. Ως αποτέλεσμα, ο χρόνος μεταγωγής της πύλης θα εξαρτάται από δεδομένα, τα οποία μπορούν να φανούν μέσω οποιουδήποτε αριθμού πλευρικών καναλιών (π.χ. ισχύς, HM, οπτικά) και να αξιοποιηθούν σε μια επίθεση χρονισμού. Έχει προταθεί μια λύση για αυτό το πρόβλημα, η οποία περιλαμβάνει τη χρήση «διαιτητών» για την αποτροπή πυροδότησης της πύλης μέχρι να φτάσουν όλες οι είσοδοι. Εναλλακτικά, όλες οι πύλες μπορούν να ενεργοποιηθούν με ένα καθορισμένο βήμα καθυστέρησης που είναι εγγυημένο ότι είναι μεγαλύτερο από τη μεγαλύτερη καθυστέρηση της πύλης στο προηγούμενο στάδιο.

Τέλος, οι ασφαλείς λογικές οικογένειες έχουν σημαντικές εξόδους VLSI όσον αφορά την περιοχή, την ισχύ και την καθυστέρηση σε σύγκριση με τους συνηθισμένους τύπους

λογικής, συχνά 3 φορές ή περισσότερο. Επιπλέον, σε αντίθεση με την κανονική λογική, οι οικογένειες συνεκτικής λογικής συχνά απαιτούν πρόσθετα σήματα ελέγχου και έχουν πρόσθετες χρονικές απαιτήσεις. Ως αποτέλεσμα, αυτές οι λογικές οικογένειες είναι απίθανο να χρησιμοποιηθούν σε κάθε τμήμα ενός σημαντικού σχεδιασμού SoC ή CPU, αλλά μάλλον σε μέρη του σχεδιασμού που απαιτούν ασφαλή λειτουργία.



Εικόνα 2.2.2.2.2 Παράδειγμα οικογένειας τριφασικής λογικής: Τριφασική Διπλή Όδευση Λογικής Προφόρτισης (TDPL)



Εικόνα 2.2.2.2.3 Σχέδιο φίλτρου τριφασικής τροφοδοσίας με χρήση πυκνωτών μεταγωγής.

2.2.2.3 Ασύγχρονη λογική

Λόγω της αντίστασης στην ανάλυση ισχύος (οι περισσότερες ασύγχρονες οικογένειες λογικής χρησιμοποιούν κωδικοποίηση σήματος διπλής ράγας ή 1-εως-n), ΗΜ χαμηλότερες εκπομπές λόγω έλλειψης συγχρονισμού ρολογιού, αντίστασης στην διαρροή σφάλματος και ικανότητας κωδικοποίησης κατάστασης συναγερμού στα δεδομένα, Οι ασύγχρονες πύλες έχουν επίσης προταθεί για χρήση σε ασφαλή συστήματα. Ένα κοινό πλεονέκτημα της ασύγχρονης λογικής είναι ότι ολοκληρώνει τους υπολογισμούς όσο πιο γρήγορα γίνεται με βάση τα παρεχόμενα δεδομένα. Αυτό είναι ένα μειονέκτημα όσον αφορά την ανάλυση πλευρικού καναλιού, καθώς παρέχει πληροφορίες σχετικά με τα δεδομένα εισόδου με βάση τον χρόνο υπολογισμού. Η καθυστέρηση του κυκλώματος για μεταβλητά δεδομένα εισόδου μπορεί να εξισωθεί με προσεκτικό σχεδιασμό μικροαρχιτεκτονικής, εισαγωγή «διαιτητών» (π.χ. στοιχεία C Muller) ή εισαγωγή τυχαίων καθυστερήσεων.

2.2.2.4 Χαμηλής ισχύος σχεδιασμός

Ένας τρόπος για να περιοριστούν οι εκπομπές στα πλευρικά κανάλια είναι να μετριαστούν οι συνολικές εκπομπές του τσιπ, καθιστώντας πιο δύσκολο τον εντοπισμό τους. Μια απλή προσέγγιση για να επιτευχθεί αυτό είναι να μειωθεί η συνολική απαγωγή ισχύος του τσιπ, μειώνοντας έτσι την ισχύ που παρέχεται στα πλευρικά κανάλια. Δυστυχώς, οι τυπικές προσεγγίσεις ανίχνευσης χαμηλής ισχύος μπορούν ακόμα να ανακτήσουν τις εκπομπές πλευρικών καναλιών από ημιαγωγούς. Οι ακραίες προσεγγίσεις χαμηλής κατανάλωσης, όπως η λειτουργία κατωφλίου ή ο αδιαβατικός υπολογισμός, μπορούν να μειώσουν τη διασπορά ισχύος του τσιπ κατά τάξεις μεγέθους, αλλά με κόστος τη ριζικά μειωμένη απόδοση, η οποία θα μπορούσε να είναι κάτω από το ανεκτό όριο για τις περισσότερες εφαρμογές. Επιπλέον, εντείνοντας την αναντιστοιχία τρανζίστορ λόγω της μεταβλητότητας της διαδικασίας, η λειτουργία κατωφλίου μπορεί να επιδεινώσει τη διαρροή του πλευρικού καναλιού.

2.2.2.5 Προστασία

Η φυσική θωράκιση ή το φιλτράρισμα της διαρροής στο πλευρικό κανάλι είναι ένα άλλο μέσο μείωσης των συνολικών εκπομπών ενός τσιπ. Για ενεργό φιλτράρισμα, αυτό θα μπορούσε να σημαίνει την προσθήκη περισσότερων πυκνωτών αποσύνδεσης στην τροφοδοσία ρεύματος ή στους ρυθμιστές τάσης στο καλούπι. Επί του παρόντος, χρησιμοποιούνται για τη μετατροπή υψηλών εξωτερικών τάσεων (π.χ. 1,8 V) στις χαμηλότερες τάσεις πυρήνα που απαιτούνται για 45 nm και μικρότερες γεωμετρίες διεργασίας (π.χ. 1,0 V).

Η χρήση των υφιστάμενων μεταλλικών στρωμάτων ανώτερου επιπέδου ως ασπίδα έχει προταθεί ως μία τεχνική μείωσης των εκπομπών ηλεκτρομαγνητικής ακτινοβολίας μέσω θωράκισης. Δυστυχώς, τα μεγάλα SOC και οι CPU χρησιμοποιούν συχνά τα ανώτερα μεταλλικά στρώματα για τη διανομή ρολογιού και τροφοδοσίας, τα οποία είναι τα ίδια σήματα που εκμεταλλεύονται συχνά τα έμμεσα HM πλευρικά κανάλια. Παρά το γεγονός ότι οι σύγχρονες διαδικασίες κατασκευής ημιαγωγών έχουν πάνω από δέκα μεταλλικά στρώματα, η αφιέρωση ενός ή περισσότερων από αυτά τα στρώματα για HM θωράκιση είναι αρκετά δαπανηρή. Επιπλέον, η πλευρά του υποστρώματος της συσκευής δεν είναι θωρακισμένη. Οποιοδήποτε μεταλλικό στρώμα που χρησιμοποιείται ως θωράκιση θα πρέπει να είναι αρκετά πορώδες ώστε να παρέχει πρόσβαση στα σήματα I/O και τροφοδοσίας στην πλειονότητα των επιφανειών δεσμών. Για κατανομή τροφοδοσίας χαμηλότερης αντίστασης, κάποιες CPU περιλαμβάνουν δύο μεταλλικά στρώματα αφιερωμένα σε επίπεδα Vdd και Gnd. Αν και αυτή η δομή δεν σχεδιάστηκε για χρήση ως ασπίδα ηλεκτρομαγνητικής ακτινοβολίας, έχει χρησιμοποιηθεί στο παρελθόν. Ένας εξωτερικός κλωβός Faraday μπορεί να χρησιμοποιηθεί για τη μόνωση του τσιπ, αν και θα πρέπει να είναι σχετικά πορώδες για συνδέσεις I/O και τροφοδοσίας. Επίσης, διάφορα στοιχεία φυσικής μορφής θα καθιστούσαν αδύνατη την επίτευξη αυτού του τύπου θωράκισης (π.χ. έξυπνες κάρτες).

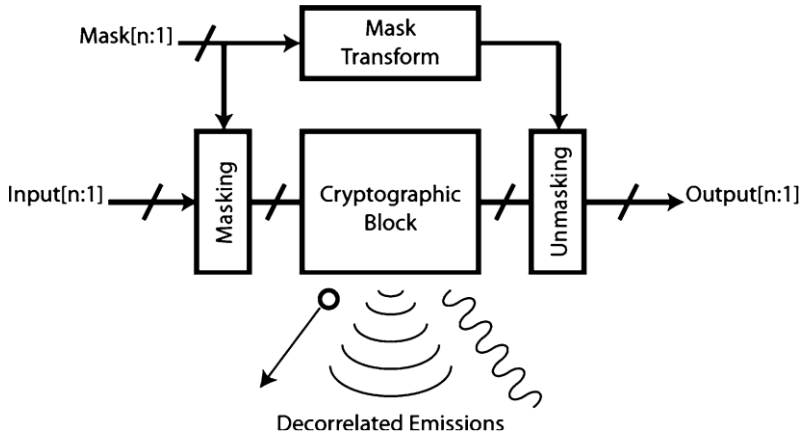
Η απόσβεση του ήχου στη θήκη του συστήματος θα μπορούσε να χρησιμοποιηθεί για την παροχή ακουστικής προστασίας. Τα συνηθισμένα μεταλλικά στρώματα τσιπ καλύπτουν την επάνω πλευρά του τσιπ από οπτική ανίχνευση για οπτικά πλευρικά κανάλια, αλλά η πίσω πλευρά μπορεί να είναι εκτεθειμένη. Ενώ μπορεί να είναι εφικτές διάφορες επιλογές συσκευασίας για την αποφυγή της οπτικής ανίχνευσης στο πίσω μέρος, τα αποτελέσματα αυτών των αντίμετρων στην απαγωγή θερμότητας κατά τη λειτουργία (καθώς η πίσω

πλευρά είναι η πλευρά του τσιπ όπου είναι προσαρτημένες οι ψήκτρες) και τη δυνατότητα δοκιμής (καθώς η οπτική ανίχνευση στο πίσω μέρος χρησιμοποιείται σε πολλές τεχνολογίες οπτικών δοκιμών) είναι άγνωστες. Για μεγαλύτερο SNR, η διερεύνηση στο πίσω μέρος θα απαιτούσε την αραίωση της πλακέτας, η οποία μπορεί να επιτευχθεί χρησιμοποιώντας μια ποικιλία υπαρχουσών προσεγγίσεων.

2.2.3 Κάλυψη/ Τύφλωση

Η κάλυψη, επίσης αναφέρεται και ως τύφλωση, είναι ένα αντίμετρο που στοχεύει στην εξάλειψη της συσχέτισης μεταξύ των δεδομένων εισόδου και των εκπομπών του πλευρικού καναλιού από ενδιάμεσους κόμβους στο λειτουργικό μπλοκ. Αυτό μπορεί να γίνει πύλη προς πύλη ή μπλοκ προς μπλοκ. Οι τεχνικές ανά πύλη χρησιμοποιούν εξειδικευμένες λογικές οικογένειες κάλυψης (π.χ. RSL ή MDPL) που αναστρέφουν υπό όρους τις εξόδους της πύλης χρησιμοποιώντας ένα τυχαίο bit κάλυψης παγκοσμίως κατανεμημένο (δηλαδή, καλύπτουν την έξοδο XOR με το bit μάσκας).

Πριν εισάγετε το κρυπτογραφικό μπλοκ, οι τεχνικές ανά λέξη χρησιμοποιούν ένα τυχαίο διάνυσμα bit για να τυχαιοποιήσουν τα δεδομένα εισόδου. Ακόμη και αν απελευθερωθούν πληροφορίες πλευρικού καναλιού, δεν συσχετίζονται με τα αρχικά δεδομένα εισόδου, επειδή το κρυπτογραφικό μπλοκ δρα με τυχαία δεδομένα. Μετά την αναχώρηση από το κρυπτογραφικό μπλοκ, τα δεδομένα μετασχηματίζονται προς την άλλη κατεύθυνση για να ανακτηθούν τα δεδομένα εξόδου. Ένας εισβολέας μπορεί να είναι σε θέση να συλλέγει τις ενδιάμεσες τιμές που χρησιμοποιούνται στο κρυπτογραφικό μπλοκ, αλλά δεν μπορούν να ληφθούν πληροφορίες σχετικά με τα αρχικά δεδομένα, εφόσον η μάσκα παραμένει κρυφή. Αυτές οι λειτουργίες είναι πολύ απλές για γραμμικές συναρτήσεις, και μη γραμμικές συναρτήσεις όπως το AES S-Box εξακολουθούν να είναι εφικτές, αν και πιο δύσκολες.



Εικόνα 2.2.3 Σύστημα κάλυψης ανά λέξη που διασυσχετίζει τις ενδιάμεσες τιμές στο κρυπτογραφικό αποκλεισμός από τα δεδομένα εισόδου.

2.2.4 Διαμέριση σχεδιασμού

Λόγω της σύζευξης μυστικών σημάτων σε άλλους κόμβους, ορισμένα πλευρικά κανάλια (π.χ. ακούσιες εκπομπές EM) διαρρέουν πληροφορίες. Οι σχεδιαστές μπορούν να χωρίσουν περιοχές του τσιπ που λειτουργούν με απλό κείμενο από τμήματα που λειτουργούν με κρυπτογραφημένο κείμενο για να μειώσουν τις εκπομπές. Είναι ο τυπικός διαχωρισμός RED (απλό κείμενο) από το BLACK στο NSA TEMPEST (κρυπτογραφημένο κείμενο). Ο διαχωρισμός αυτός θα μπορούσε να περιλαμβάνει όχι μόνο τον φυσικό διαχωρισμό των στοιχείων του τσιπ, αλλά και τον διαχωρισμό οποιασδήποτε κοινόχρηστης υποδομής. Αυτό θα περιλαμβάνει την υποδομή τροφοδοσίας (δίκτυα διανομής, ρυθμιστές, ακίδες), χωριστή υποδομή χρονισμού (βρόχους κλειδώματος φάσης, δίκτυο διανομής, ακίδες, κρύσταλλοι πλακέτας) και ξεχωριστή υποδομή δοκιμών (βρόχοι κλειδώματος φάσης, δίκτυο διανομής, ακίδες, κρύσταλλοι πλακέτας) και ξεχωριστή υποδομή δοκιμών (αλυσίδα σάρωσης flip-flop, ενσωματωμένος αυτοέλεγχος). Ορισμένα κυκλώματα μικτού σήματος (αναλογικά και ψηφιακά) με ιδιαίτερα ευαίσθητα αναλογικά κυκλώματα δεν θέλουν θόρυβο από το ψηφιακό τμήμα του τσιπ στην τροφοδοσία ή τα σήματα χρονισμού, επομένως αυτή η μορφή διαχωρισμού είναι κοινή. Στη συχνότητα ρολογιού και τις αρμονικές της, αυτός ο θόρυβος έχει διάφορες φασματικές συνιστώσες.

Η στοίχιση 3D καλουπιών επιτρέπει τον πιο δραστικό διαχωρισμό των ζωνών RED και BLACK. Οι δύο ζώνες μπορούν να κατασκευαστούν σε ξεχωριστά τσιπ και στη συνέχεια να ενωθούν μεταξύ τους για να δημιουργήσουν μια στοίβα καλουπιών. Για τη στοίχιση τσιπ

3D, υπάρχει μια ποικιλία εμπορικά προσβάσιμων τεχνολογιών και προσεγγίσεων. Μέσω πυριτίου (TSV), οι οποίες παρέχουν συνδεσιμότητα υψηλής πυκνότητας και χαμηλής καθυστέρησης, μπορούν να χρησιμοποιηθούν για τη σύνδεση των διαφορετικών καλουπιών. Η κατασκευή ενός στοιχείου του σχεδίου σε ένα αναξιόπιστο χυτήριο και ενός τμήματος σε ένα αξιόπιστο χυτήριο, στη συνέχεια η ένωση των δύο καλουπιών μέσω τρισδιάστατης στοίχισης, έχει επίσης προσφερθεί ως στρατηγική για να ξεπεραστούν τα τρωτά σημεία της διασφάλισης παραγωγής και της εφοδιαστικής αλυσίδας.

3. Ανάλυση Ισχύος (Power Analysis)

Από όταν ξεκίνησε η ανταλλαγή προσωπικών δεδομένων να γίνεται μέσω της ηλεκτρονικής διαδικασίας, η ανάγκη για την προστασία των δεδομένων γίνεται όλο και μεγαλύτερη. Οι ασφαλείς επικοινωνίες στα ενσωματωμένα συστήματα απειλείται συνεχώς από επιθέσεις εξελιγμένης ανάλυσης πλευρικών καναλιών (Side Channel Attacks - SCA). Οι επιθέσεις αυτές εκμεταλλεύονται εμπιστευτικές (διάφορα είδη διαρροών μυστικών) πληροφορίες που διαρρέουν από κρυπτογραφικές συσκευές. Οι φυσικές διαρροές προέρχονται από την κατανάλωση ρεύματος, την ηλεκτρομαγνητική ακτινοβολία, καθώς και από τη συμπεριφορά της συσκευής σχετικά με το χρόνο. Εμείς θα ασχοληθούμε με τις επιθέσεις που εκμεταλλεύονται την κατανάλωση ρεύματος για τις διαρροές, οι οποίες ονομάζονται επιθέσεις ανάλυσης ισχύος. Αυτές οι επιθέσεις στηρίζονται στο γεγονός πως κατά τη μετάδοση ενός σήματος εντός της συσκευής γίνεται ρευματοδότηση ενός σημείου της συσκευής ή γείωση του κυκλώματος. Όταν η είσοδος από λογικό 1 γίνεται λογικό 0 και το αντίθετο, η έξοδος κάνει ακριβώς το αντίθετο με αποτέλεσμα την φόρτιση ή την εκ φόρτιση ενός πυκνωτή. Όταν η είσοδος παραμένει σταθερή δεν υπάρχει ρεύμα άρα δεν υπάρχει και κατανάλωση ισχύος. Αυτή τη φυσική συμπεριφορά εκμεταλλεύονται οι επιθέσεις ισχύος και εξάγουν δεδομένα που επεξεργάζονται στο εσωτερικό της συσκευής.

Στο κομμάτι της ανάλυσης ισχύος των κρυπτογραφικών υλοποιήσεων υπάρχουν διάφορες μέθοδοι όπως η Απλή Ανάλυση Ισχύος (SPA), η Διαφορική Ανάλυση Ισχύος (DPA) και η Ανάλυση Σύγκρουσης (CA). Η Απλή Ανάλυση χρησιμοποιεί μονό ίχνος ή πολλά ίχνη, όπως θα ήταν η στιγμιαία κατανάλωση ισχύος κατά την εκτέλεση ενός αλγορίθμου για μια

συγκεκριμένη χρονική στιγμή. Αντιθέτως η Διαφορική Ανάλυση χρησιμοποιεί στατιστικές μεθόδους εξαγωγής των δεδομένων από πολλαπλά ίχνη. Η Σύγκρουση εκμεταλλεύεται τη διαρροή από δυο τμήματα των ιχνών όταν χρησιμοποιούν την ίδια τιμή.

Οι απλές υλοποιήσεις κρυπτοσυστημάτων δημόσιου κλειδιού είναι επιρρεπείς σε επιθέσεις SPA λόγω της διακλαδώσεων υπό όρους. Στην RSA κρυπτογραφία αυτές οι διακλαδώσεις βρίσκονται στο δομημένο αλγόριθμο και όταν εκτελούνται χρησιμοποιούν μια επανάληψη δομημένων τετραγωνισμών και δομημένων πολλαπλασιασμών. Στις απλές υλοποιήσεις χρησιμοποιείται η μέθοδος double-and-add (διπλά και πρόσθεση) που διαθέτει διαδοχικούς διπλασιασμούς σημείων και προσθήκες σημείων, όπου μια προσθήκη σημείου εκτελείται μόνο όταν το bit του κλειδιού είναι 1. Με αυτό τον τρόπο ένα μονό ίχνος ισχύος εμφανίζει λογικό 1 στο κλειδί όταν παρουσιάζεται προσθήκη σημείου. Κάποια αντίμετρα εξισορροπούν τους υπολογισμούς έτσι ώστε τα ίχνη ισχύος να φαίνονται τα ίδια ή παρόμοια ανεξάρτητα από τα επεξεργασμένα bit. Κάποια άλλα αντίμετρα τυχαιοποιούν τους υπολογισμούς έτσι ώστε ο εισβολέας να μην μπορεί να τα συσχετίσει ίχνη ισχύος με τα επεξεργασμένα δεδομένα.

Οι επιθέσεις που έχουν σαν στόχο πολλά μέρη ενός συστήματος ασφαλείας είναι δύσκολο να προβλεφθούν και να μοντελοποιηθούν. Θα πρέπει οι σχεδιαστές κρυπτογράφησης, προγραμματιστές λογισμικού και οι μηχανικοί υλικού να μπορούν να κατανοήσουν ο ένας τη δουλειά του άλλου έτσι ώστε η ασφάλεια σε κάθε επίπεδο σχεδιασμού ενός συστήματος να μην είναι ελλιπής και να είναι ρεαλιστική. Αποτέλεσμα αυτού τα σφάλματα που προκύπτουν να περιλαμβάνουν απρόβλεπτες αλληλεπιδράσεις μεταξύ διαφόρων στοιχείων λόγω του ότι έχουν σχεδιαστεί από διαφορετικούς ανθρώπους.

3.1 Απλή Ανάλυση Ισχύος (SPA)

Τα τελευταία χρόνια οι κρυπτογραφικές συσκευές υλοποιούνται με τη βοήθεια λογικών πυλών ημιαγωγών που είναι κατασκευασμένες από τρανζίστορ. Τα ηλεκτρόνια διασχίζουν το στρώμα πυριτίου όταν εφαρμόζεται ρεύμα στην πύλη του τρανζίστορ με αποτέλεσμα να καταναλώνεται ισχύς και να παράγεται ηλεκτρομαγνητική ενέργεια.

Για να μπορέσουμε να μετρήσουμε την κατανάλωση ισχύος τοποθετούμε σε σειρά με την είσοδο ή με τη γείωση μια μικρή αντίσταση. Η διαφορά τάσης στην αντίσταση διαιρούμενη με την αντίσταση μας δίνει σαν αποτέλεσμα το ρεύμα. Εργαστήρια ηλεκτρονικών που είναι πολύ καλά εξοπλισμένα διαθέτουν εξοπλισμό ο οποίος μπορεί να εκτελέσει αυτές τις δοκιμές ψηφιακά και σε μεγάλες συχνότητες και με μεγάλη ακρίβεια.

Η Απλή Ανάλυση Ισχύος (SPA) είναι μια τεχνική που ερμηνεύει τις μετρήσεις κατανάλωσης ενέργειας που συλλέγονται κατά την εκτέλεση κρυπτογραφημένων λειτουργιών. Η SPA μπορεί να δώσει πληροφορίες για τη λειτουργία μιας συσκευής καθώς και για το βασικό υλικό της. Επειδή η SPA μπορεί να αποκαλύψει την ακολουθία των εντολών που εκτελούνται, μπορεί να χρησιμοποιηθεί για κρυπτογραφήσεις που η εκτέλεσής τους εξαρτάται από τα δεδομένα που επεξεργάζονται.

3.2 Πρόληψη SPA

Το να αποτρέψουμε την απλή ανάλυση ισχύος είναι αρκετά απλό να επιτευχθεί. Οι διαδικασίες αποφυγής που χρησιμοποιούν μυστικά ενδιάμεσα κλειδιά και λειτουργίες διακλάδωσης υπό όρους θα καλύψει αρκετά χαρακτηριστικά SPA. Στις περιπτώσεις που ο αλγόριθμος χρειάζεται διακλάδωση θα χρειαστεί μια πιο δημιουργική κωδικοποίηση η οποία θα προκαλέσει σοβαρό πρόβλημα όσον αφορά την απόδοση.

Ακόμα ο κώδικας σε μερικούς μικροεπεξεργαστές μπορεί να προκαλέσει προβλήματα στην κατανάλωση ενέργειας ανάλογα με τον τελεστή. Για αυτά τα συστήματα ακόμα και η διαδρομή εκτέλεσης μπορεί να έχει πολλά σοβαρά τρωτά σημεία ως προς την SPA. Οι περισσότερες υλοποιήσεις υλικού των συμμετρικών κρυπτογραφικών αλγορίθμων έχουν αρκετά μικρές διακυμάνσεις στην κατανάλωση ενέργειας στις οποίες η SPA δεν παράγει ουσιαστικό αποτέλεσμα.

3.3 Διαφορική Ανάλυση Ισχύος (DPA)

Αντιθέτως η μεγάλης κλίμακας διακυμάνσεις κατανάλωσης ισχύος λόγω της ακολουθίας των εντολών σχετίζεται και με τα στοιχεία από τις τιμές των δεδομένων που χειρίζονται. Οι παραλλαγές αυτές συχνά είναι μικρότερες και μερικές φορές καλύπτονται από σφάλματα μετρήσεων και από άλλους θορύβους. Σε αυτές τις περιπτώσεις είναι δυνατό να σπάσει το σύστημα αν χρησιμοποιήσουμε στατιστικές συναρτήσεις προσαρμοσμένες στον αλγόριθμο στόχο.

Για να επιτευχθεί μια επίθεση DPA θα πρέπει ο εισβολέας να παρακολουθεί τις λειτουργίες κρυπτογράφησης και να καταγράφει τα ίχνη ισχύος.

Η DPA χρησιμοποιεί τις μετρήσεις κατανάλωσης για να προσδιορίσει αν τα δεδομένα είναι σωστά. Ο εισβολέας υπολογίζει ένα διαφορικό δείγμα ίχνους, βρίσκοντας το μέσο όρο των ιχνών που είναι 1 και το μέσο όρο που είναι μηδέν.

Πολλές πηγές εισάγουν θορύβους στην ανάλυση DPA όπως είναι η ηλεκτρομαγνητική ακτινοβολία αλλά και ο θερμικός θόρυβος. Σφάλματα κβαντισμού μπορούν να προκαλέσουν πρόσθετα προβλήματα λόγω αναντιστοιχίας ρολογιών συσκευής και ρολογιών δειγμάτων. Έλος λανθασμένη χρονική ευθυγράμμιση ιχνών μπορεί να προκαλέσει μείωση του θορύβου.

Μπορούν να εφαρμοστούν πολλές βελτιώσεις στις διαδικασίες συλλογής δεδομένων και στην ανάλυση DPA για να μειωθεί ο αριθμός ων δειγμάτων για την παράκαμψη των αντί-μέτρων. Επίσης μπορούν να χρησιμοποιηθούν εξελιγμένες λειτουργίες επιλογής. Ιδιαίτερη σημασία έχουν οι λειτουργίες DPA που συνδυάζουν πολλά δείγματα μέσα από ένα ίχνος.

Οι λειτουργίες επιλογής μπορούν να αντιστοιχίσουν διαφορετικά βάρη σε ίχνη και να τα χωρίσουν σε περισσότερες από δυο κατηγορίες. Τέτοιες συναρτήσεις επιλογής μπορούν να πετύχουν πολλά αντίμετρα ή να επιτεθούν σε συστήματα με μερικές ή καθόλου πληροφορίες σχετικά με απλά ή και κρυπτογραφημένα κείμενα. Η ανάλυση δεδομένων χρησιμοποιεί συναρτήσεις διαφορετικές από το μέσο όρο και είναι χρήσιμη σε σύνολα δεδομένων που έχουν ασυνήθιστες κατανομές.

3.4 Πρόληψη DPA

Οι τεχνικές αποτροπής επιθέσεων DPA και σχετικών επιθέσεων είναι τριών κατηγοριών.

Η πρώτη προσέγγιση είναι η μείωση των μεγεθών των σημάτων, η χρήση κώδικα σταθερής εκτέλεσης ή η εκτέλεση λειτουργιών που διαρρέουν λιγότερες πληροφορίες, η εξισορρόπηση βαρών Hamming, η μεταβάσεις καταστάσεων και η φυσική θωράκιση της συσκευής.

Μια μείωση του σήματος δεν μπορεί να κάνει μείωση μέχρι το μηδέν, καθώς ένας εισβολέας θα μπορεί να εκτελεί άπειρο αριθμό δειγμάτων και θα μπορεί να εκτελέσει DPA στο σήμα. Στην πράξη οι επιθετική θωράκιση μπορεί να κάνει τις επιθέσεις ανέφικτες αλλά θα πρέπει να αυξηθεί το μέγεθος και το κόστος της συσκευής.

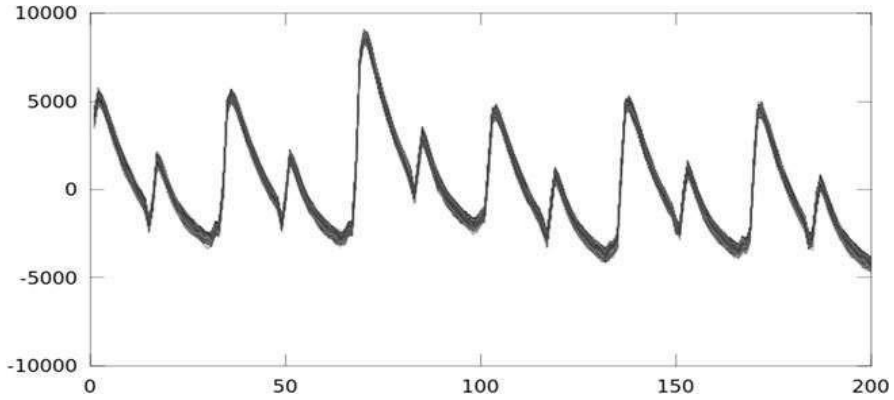
Η δεύτερη προσέγγιση περιλαμβάνει εισαγωγή θορύβου στις μετρήσεις κατανάλωσης ισχύος. Όπως και η μειώσεις μεγέθους σημάτων έτσι και η εισαγωγή θορύβου αυξάνει των αριθμό των δειγμάτων που χρειάζονται για μια επίθεση. Επίσης ο χρόνος εκτέλεσης και η σειρά μπορούν να τυχαιοποιηθούν. Η προσέγγιση των σχεδιαστών και των αναθεωρητών θα πρέπει να γίνεται με μεγάλη προσοχή καθώς πολλές τεχνικές μπορούν να χρησιμοποιηθούν για να παρακάμψουν και να αντισταθμίσουν αυτά τα αποτελέσματα. Πολλά ευάλωτα προϊόντα έχουν περάσει αξιολογήσεις που χρησιμοποίησαν μεθόδους επεξεργασίας δεδομένων.

Μια εθνική προσέγγιση περιλαμβάνει το σχεδιασμό κρυπτοσυστημάτων με ρεαλιστικές υποθέσεις σχετικά με το υποκείμενο υλικό. Μπορούν να χρησιμοποιηθούν μη γραμμικές διαδικασίες ενημέρωσης κλειδιού για να διασφαλιστεί ότι τα ίχνη ισχύος δεν μπορούν να συσχετιστούν μεταξύ των συναλλαγών. Ως απλό παράδειγμα, ο κατακερματισμός ενός κλειδιού 160-bit με το SHA θα πρέπει να καταστρέψει ουσιαστικά μερικές πληροφορίες που μπορεί να είχε συγκεντρώσει ένας εισβολέας σχετικά με το κλειδί. Ομοίως, η επιθετική χρήση των διαδικασιών αλλαγής εκθέτη και συντελεστή σε σχήματα δημόσιου κλειδιού μπορεί να χρησιμοποιηθεί για να αποτρέψει τους εισβολείς από τη συσσώρευση δεδομένων σε μεγάλο αριθμό λειτουργιών. Οι μετρητές βασικής χρήσης μπορούν να αποτρέψουν τους εισβολείς από τη συλλογή μεγάλου αριθμού δειγμάτων.

Χρησιμοποιώντας μια μεθοδολογία σχεδιασμού με ανεκτική διαρροή, ένας σχεδιαστής κρυπτοσυστήματος πρέπει να καθορίσει τους ρυθμούς διαρροής και τις λειτουργίες που μπορεί να επιβιώσει η κρυπτογραφία. Οι συναρτήσεις διαρροής μπορούν να αναλυθούν ως χρησμοί που παρέχουν πληροφορίες σχετικά με υπολογιστικές διαδικασίες και δεδομένα, όπου ο ρυθμός διαρροής είναι το ανώτερο όριο του όγκου των πληροφοριών που παρέχονται από τη συνάρτηση διαρροής. Οι υπεύθυνοι υλοποίησης μπορούν στη συνέχεια να χρησιμοποιήσουν τεχνικές μείωσης διαρροών και κάλυψης διαρροών, όπως απαιτείται για να ανταποκριθούν στις παραμέτρους του είδους. Τέλος, οι αναθεωρητές πρέπει να επαληθεύσουν ότι οι υποθέσεις σχεδιασμού είναι κατάλληλες και αντιστοιχούν στα φυσικά χαρακτηριστικά της ολοκληρωμένης συσκευής.

4. Πρακτικό Μέρος

Στο κεφάλαιο αυτό θα περιγράψουμε και θα αναλύσουμε το πρακτικό κομμάτι της εργασίας με το οποίο ασχοληθήκαμε. Πιο συγκεκριμένα ασχοληθήκαμε με την Διαφορική Ανάλυση Ισχύος (Differential Power Analysis -DPA) και με τον τρόπο λεοτουργίας της. Δηλαδή, πως (αυτή) δρα σε ένα κρυπτογραφημένο σύστημα και πως μας βοηθάει να βρούμε το μυστικό κλειδί για αποκρυπτογράφηση και ανάκτηση ευαίσθητων δεδομένων. Η DPA είναι από τις πιο ισχυρές μεθόδους κρυπτογράφησης. Η DPA χρησιμοποιεί την πληροφορία που διαρρέει από μια συσκευή κρυπτογράφησης, και πρόκειται για την κατανάλωση ισχύος. Δηλαδή, ως βασικός της στόχος είναι η μέτρηση της κατανάλωσης ισχύος με ακρίβεια. Εν συνεχεία, απαιτείται η γνώση του αλγόριθμου που εκτελείται και τέλος το σύνολο των κρυπτογραφημάτων ή των αυθεντικών μηνυμάτων. ο τρόπος επίθεσης είναι όχι κατευθείαν στην κρυπτογράφηση αλλά στην φυσική εφαρμογή του κρυπτογραφικού συστήματος. Η DPA βασίζεται στο γεγονός ότι κάθε ηλεκτρονικό σύστημα καταναλώνει ενέργεια – ισχύς. Αν μετρήσουμε την κατανάλωση ενέργειας ενός συστήματος το πιθανότερο είναι να δούμε ένα ίχνος ισχύος σαν αυτό που φαίνεται στην εικόνα πιο κάτω. Οι κορυφές δείχνουν τις ανερχόμενες και τις πτωτικές άκρες του ρολογιού.



Εικόνα 4.1 Το σχήμα δείχνει 500 ίχνη ισχύος στο ίδιο χρονικό διάστημα 200 δειγμάτων.

Κάθε ίχνος ισχύος εκτελείται για μοναδικά δεδομένα εισόδου, τα ίχνη ισχύος επικαλύπτονται. Οι διακυμάνσεις στα ίχνη ισχύος προκαλούνται από διακυμάνσεις στα επεξεργασμένα δεδομένα.

Ακόμα αυτό που μπορούμε να δούμε στην εικόνα πιο πάνω είναι ότι αν ένα σύστημα εκελεί μια κρυπτογράφηση και εμείς του δίνουμε διαφορετικά δεδομένα εισόδου, παρατηρούνται μικρές διακυμάνσεις στα ίχνη ισχύος. Υπάρχουν πολλοί παράγοντες που προκαλούν αυτές τις διακυμάνσεις όπως είναι για παράδειγμα η μεταβαλόμενη θερμοκρασία. Άλλος ένα παράγοντας είναι τα εσωτερικά δεδομένα που επεξεργάζονται. Η DPA εκμεταλλεύεται αυτή την εξάρτηση της κατανάλωσης ενέργειας από αυτά τα δεδομένα και έτσι σπάει την κρυπτογράφηση.

4.1 Στάδια υλοποίησης DPA επίθεσης

Σε αυτό το κεφάλαιο παρέχουμε μία ολοκληρωμένη διαδικασία επίθεσης DPA για αποκρυπτογράφηση κλειδιού ενός κρυπτογραφημένου κειμένου με την βοήθεια του αλγορίθμου AES. Η Κρυπτογράφηση AES ή αλλιώς το προηγμένο πρότυπο κρυπτογράφησης είναι ένα συμμετρικό μπλοκ κρυπτογράφησης που χρησιμοποιεί ένα κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων. Ο AES είναι ένας επαναληπτικός κρυπταλγόριθμος τμήματος. Το απλό κείμενο χωρίζεται σε τμήματα(blocks) 128 bits (16 bytes), ενώ το κλειδί μπορεί να έχει μήκος 128,192 ή 256 bits (16,24 ή 32 bytes), ανάλογα με το επιθυμητό επίπεδο ασφαλείας. Αναπτύχθηκε από δύο

κρυπτογράφους, τον Joan Daemen και τον Vincent Rijmen και είναι το πρότυπο κρυπτογράφησης δεδομένων του σήμερα.

Η διαδικασία μιας επίθεσης dpa αποτελείται από κάποια στάδια. Στο πρώτο στάδιο επιλέγουμε ένα ενδιάμεσο αποτέλεσμα του κρυπτογραφικού αλγορίθμου που εκτελείται από την συσκευή που δέχεται επίθεση. Αυτό το ενδιάμεσο αποτελέσματα πρέπει να είναι μια συνάρτηση f(d,k) όπου d είναι είτε το αρχικό κείμενο, είτε το κρυπτογραφημένο.

Στο δεύτερο στάδιο παίρνουμε την μέτρηση της κατανάλωσης ισχύος της κρυπτογραφημένης συσκευής ενώ κρυπτογραφεί ή αποκρυπτογραφεί διαφορετικά D μπλοκ δεδομένων. Για κάθε μία από αυτές τις ενέργειες , ο εισβολέας χρειάζεται να γνωρίζει την αντίστοιχη τιμή δεδομένων d, η οποία εμπλέκεται στον υπολογισμό των ενδιάμεσων αποτελεσμάτων που αναφέραμε στο πρώτο στάδιο. Οι τιμές δεδομένων ορίζονται ως διάνυσμα $d = (d_1, ..., d_D)$, όπου d_i υποδηλώνει την τιμή των δεδομένων για την i κρυπτογράφηση ή αποκρυπτογράφηση. Ακόμη, κατά τη διάρκεια αυτών των εκτελέσεων , ο εισβολέας καταγράφει το ίχνος ισχύος, όπου αντιστοιχεί στο μπλοκ δεδομένων d_i ως $t_i = (t_i, 1, …., t_i, T)$, όπου T υποδηλώνει το μήκος του ίχνους. Ο εισβολέας μετρά το ίχνος για καθένα από τα μπλοκ δεδομένων D και ως εκ τούτου, τα ίχνη μπορούν να γραφτούν στον πίνακα T μεγέθους D*T.

Στο τρίτο στάδιο γίνεται ο υπολογισμός μιας υποθετικής ενδιάμεσης τιμής για κάθε πιθανή επιλογή του k, που ορίζεται ως διάνυσμα $k = (k_1, ……, k_K)$, όπου K υποδηλώνει τον συνολικό αριθμό των πιθανών επιλογών για το k. Στο πλαίσιο των επιθέσεων DPA, συνήθως αναφέρουμε τα στοιχεία του διανύσματος k, ως υποθετικά κλειδιά. Δεδομένου του διανύσματος δεδομένων d και των υποθετικών κλειδιών k, ο εισβολέας μπορεί εύκολα να υπολογίσει υποθετικές ενδιάμεσες τιμές f(d,k) για τις εκτελέσεις κρυπτογράφησης D, καθώς και για όλα τα υποθετικά κλειδιά K. Ο υπολογισμός αυτός οδηγεί στη δημιουργία ενός πίνακα V μεγέθους D*K και απεικονίζεται ως $V_{ij} = f (d_i,k_j)$, όπου i = 1, …., D και j = 1, …., K

Η στήλη j του V περιέχει τα ενδιάμεσα αποτελέσματα που έχουν υπολογιστεί με βάση το υποθετικό κλειδί k_j και η στήλη i του V περιέχει τις ενδιάμεσες τιμές που έχουν υπολογιστεί κατά την διάρκεια των εκτελέσεων κρυπτογράφησης και αποκρυπτογράφησης di. Θυμόμαστε ότι το k περιέχει όλες τις υποθετικές επιλογές για το διάνυσμα k. Ως εκ τούτου, η τιμή που χρησιμοποιείται στην συσκευή είναι ένα στοιχείο του διανύσματος k.

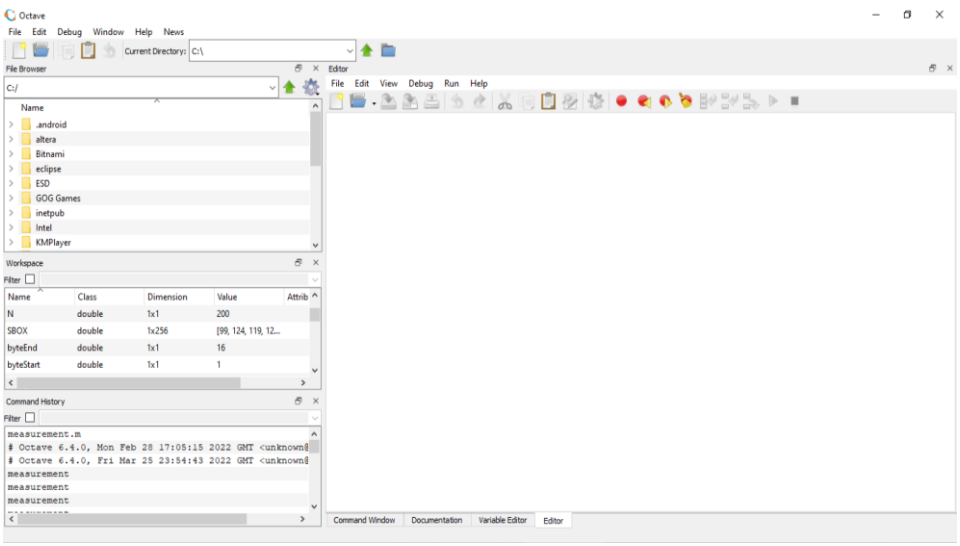
Αναφερόμαστε δηλαδή στο περιεχόμενο αυτού του στοιχείου ως ck, όπου k_{ck} είναι το κλειδί της συσκευής. Ωστόσο αν μάθουμε ποια στήλη του V έχει υποστεί επεξεργασία στη συσκευή που επιτέθηκε, αυτομάτως γνωρίζουμε και το $k_{ck.}$

Στο τέταρτο στάδιο πραγματοποιείται η αντιστοίχιση των ενδιάμεσων τιμών του πίνακα V , σε ένα πίνακα H των υποθετικών τιμών της κατανάλωσης ισχύος. Για το σκοπό αυτό ο εισβολέας χρησιμοποιεί κάποια από τις τεχνικές προσομοίωσης για τη κάθε υποθετική ενδιάμεση τιμή $V_{i,j}$, ώστε να ληφθεί μία υποθετική τιμή κατανάλωση ισχύος $h_{i,j}$. Τα πιο συχνά χρησιμοποιούμενα μοντέλα ισχύος για την επίτευξη της αντιστοίχισης του V στον H είναι το Hamming-distance και το Hamming-weight.

Στο πέμπτο και τελευταίο στάδιο της DPA επίθεσης, γίνεται η σύγκριση των υποθετικών τιμών κατανάλωσης ισχύος με τα ίχνη ισχύος. Πιο συγκεκριμένα, κάθε στήλη h_i του πίνακα H συγκρίνεται με τη κάθε στήλη t_j του πίνακα T. Αυτό σημαίνει ότι ο εισβολέας συγκρίνει τις υποθετικές τιμές κατανάλωσης ισχύος κάθε υποθετικού κλειδιού με τα καταγεγραμμένα ίχνη σε κάθε θέση. Τα αποτελέσματα αυτής της σύγκρισης αποθηκεύονται σε ένα πίνακα R μεγέθους K*T, όπου κάθε στοιχείο $r_{i,j}$ περιέχει το αποτέλεσμα της σύγκρισης μεταξύ των στηλών h_i και t_j. Η σύγκριση αυτή γίνεται με διάφορους αλγορίθμους, και στην συγκεκριμένη περίπτωση με τον αλγόριθμο AES. Το κλειδί της συσκευής που επιτέθηκε μπορεί να αποκαλυφθεί, αν τα ίχνη ισχύος αντιστοιχούν στην κατανάλωση ισχύος της συσκευής ενώ εκτελεί έναν κρυπταλγόριθμο, χρησιμοποιώντας διαφορετικές εισόδους δεδομένων. Έτσι, η συσκευή πρέπει να υπολογίσει τις ενδιάμεσες τιμές V_{ck} κατά τις διαφορετικές εκτελέσεις του αλγορίθμου. Συνεπώς και τα κρυπτογραφημένα ίχνη εξαρτώνται από αυτές τις ενδιάμεσες τιμές σε κάποια θέση ιχνών ισχύος, η οποία δηλώνεται ως ct. Δηλαδή η στήλη t_{ct} περιέχει τις τιμές κατανάλωσης ισχύος που εξαρτώνται από τις ενδιάμεσες τιμές V_{ck}. Επίσης, οι υποθετικές τιμές κατανάλωσης ισχύος h_{ck} έχουν προσημειωθεί από τον εισβολέα με βάση τις τιμές $V_{ck.}$ Επομένως, οι στήλες h_{ck} και t_{ct} σχετίζονται αρκετά. Στην πραγματικότητα, αυτές οι δύο στήλες οδηγούν στην «υψηλότερη» τιμή του R, η οποία είναι η $r_{ck,ct.}$ Όλες οι υπόλοιπες τιμές του R είναι «χαμηλότερες» επειδή οι άλλες στήλες των H και T δεν σχετίζονται αρκετά. Έτσι λέμε, πως ο εισβολέας μπορεί να αποκαλύψει το περιεχόμενο για το σωστό κλειδί ck και τη χρονική στιγμή ct, αναζητώντας απλώς την «υψηλότερη» τιμή του R. Οι δείκτες αυτής της τιμής ορίζει το αποτέλεσμα της επίθεσης DPA.

4.2 Κώδικας

Αφού έχουμε κάνει τις παραπάνω ενέργειες θα δούμε το πρόγραμμα που θα χρησιμοποιήσουμε για να εφαρμόσουμε την DPA. Θα χρησιμοποιήσουμε το πρόγραμμα Octave για να δούμε τον αλγόριθμο καθώς και για να πάρουμε τα αποτελέσματα.



Εικόνα 4.2 Περιβάλλον Octave

Στην εικόνα 4.2 βλέπουμε το περιβάλλον που θα εργαστούμε. Στα αριστερά μπορούμε να βρούμε τους φακέλους του project που θα δημιουργήσουμε. Στο κυρίως παράθυρο είναι ο editor που ανοίγει ο κώδικας που μπορούμε να τον επεξεργαστούμε να διορθώσουμε πιθανά λάθη κλπ. Στα αριστερά μας επίσης κάτω από τους φακέλους βλέπουμε και τις μεταβλητές που δημιουργούνται καθώς τρέχει ο κώδικας. Ακόμα μαζί με τον editor είναι και το command window στο οποίο όταν γίνεται compile ο κώδικας βλέπουμε τα λάθη σε ποια σημεία του κώδικα βρίσκονται για να τα διορθώσουμε εναλλακτικά βλέπουμε τα αποτελέσματα μας.

Έτσι λοιπόν φορτώνουμε το κυρίως κομμάτι του κώδικά μας που έχει ονομασία measurement.m και φαίνεται πιο κάτω η διάρθρωσή του.

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Matlab key recovery exercise template %
% Υλοποίηση προγράμματος ανάκτησης κλειδιού μέσω Matlab %
%                                %
% 2014, Filip Stepanek and Jiri Bucek   %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%This is it
% declaration of the SBOX (might be useful to calculate the power hypothesis)
% Αρχικοποίηση του SBOX (ίσως φανεί χρήσιμο για τον υπολογισμό της ισχύος)

SBOX=[099 124 119 123 242 107 111 197 048 001 103 043 254 215 171 118 ...
    202 130 201 125 250 089 071 240 173 212 162 175 156 164 114 192 ...
    183 253 147 038 054 063 247 204 052 165 229 241 113 216 049 021 ...
    004 199 035 195 024 150 005 154 007 018 128 226 235 039 178 117 ...
    009 131 044 026 027 110 090 160 082 059 214 179 041 227 047 132 ...
    083 209 000 237 032 252 177 091 106 203 190 057 074 076 088 207 ...
    208 239 170 251 067 077 051 133 069 249 002 127 080 060 159 168 ...
    081 163 064 143 146 157 056 245 188 182 218 033 016 255 243 210 ...
    205 012 019 236 095 151 068 023 196 167 126 061 100 093 025 115 ...
    096 129 079 220 034 042 144 136 070 238 184 020 222 094 011 219 ...
    224 050 058 010 073 006 036 092 194 211 172 098 145 149 228 121 ...
    231 200 055 109 141 213 078 169 108 086 244 234 101 122 174 008 ...
    186 120 037 046 028 166 180 198 232 221 116 031 075 189 139 138 ...
    112 062 181 102 072 003 246 014 097 053 087 185 134 193 029 158 ...
    225 248 152 017 105 217 142 148 155 030 135 233 206 085 040 223 ...
    140 161 137 013 191 230 066 104 065 153 045 015 176 084 187 022];
```

Ξεκινώντας ο κώδικας μας αρχικοποιούμε το S-Box. Το οποίο αν τρέξουμε τον κώδικα θα δούμε ότι είναι ένας δυσδιάστατος πίνακας [1,256]. Όμως εδώ θα πρέπει να αναφέρουμε και τι είναι το S-Box και σε τι θα μας βοηθήσει. Το S-Box στην κρυπτογραφία ή αλλιώς Substitution Box όπως ονομάζεται κανονικά είναι ένα βασικό συστατικό στοιχείο στους αλγορίθμους συμμετρικών κλειδιών. Σκοπός του S-Box είναι η αντικατάσταση και όταν λέμε αντικατάσταση εννοούμε την κάλυψη της σχέσης μεταξύ κλειδιού και

κρυπτογραφημένου κειμένου. Μαθηματικά μπορούμε να πούμε ότι είναι μια συνάρτηση Boolean. Ως προς τις διαστάσεις του, αυτές ερμηνεύονται ως εξής αριθμός bit εισόδου στην περίπτωσή μας 1 και αριθμός bit εξόδου σε εμάς 256.

```
%%%%%%%%%%%%%%%%%%
% LOADING the DATA %
% Φόρτωση δεδομένων%
%%%%%%%%%%%%%%%%%%
tab=load("tab.mat");
% modify following variables so they correspond
% your measurement setup
% Τροποποίηση των ακόλουθων μεταβλητών ώστε να αντιστοιχούν στις ρυθμίσεις της %μέτρησης

numberOfTraces = 200;
traceSize = 370000;
```

Ορίζουμε τον αριθμό των ιχνών ισχύος που έχουμε κάνει καθώς και το μήκος τους.

```
% modify the following variables to speed-up the measurement
% Τροποποιούμαι τις ακόλουθες μεταβλητές για να επιταχυνθεί η μέτρηση
% (this can be done later after analysing the power trace)
% (Αυτό μπορεί να γίνει αργότερα, δηλαδή μετά την ανάλυση ισχύος)

%offset = 0;
%segmentLength = 370000; % for the beginning the segmentLength = traceSize
offset = 50000;
segmentLength = 10000; % for the beginning the segmentLength = traceSize
% columns and rows variables are used as inputs
% to the function loading the plaintext/ciphertext
% Οι μεταβλητές στηλών και γραμμών χρησιμοποιούνται σαν είσοδοι στη συνάρτηση που φορτώνει είτε το αρχικό κείμενο, είτε το κρυπτοκείμενο
```

```
columns = 16;
rows = numberOfTraces;

%%%%%%%%%%%%%%%%%%%%%%%%
% Calling the functions %
%%%%%%%%%%%%%%%%%%%%%%%%
% Κλήση συναρτήσεων %

% function myload processes the binary file containing the measured traces and
% stores the data in the output matrix so the traces (or their reduced parts)
% can be used for the key recovery process.
% Η συνάρτηση myload επεξεργάζεται το δυαδικό αρχείο που περιέχει τα ίχνη και
%αποθηκεύει τα δεδομένα στον πίνακα εξόδου, ώστε τα ίχνη ( ή κάποια μεμονωμένα
%κομμάτια τους) να μπορούν να χρησιμοποιηθούν για τη διαδικασία ανάκτησης κλειδιού

% Inputs:
% Είσοδοι

%   'file' - name of the file containing the measured traces
%  'αρχείο' – όνομα αρχείου που περιέχει τα μετρημένα ίχνη
%   traceSize - number of samples in each trace
%  traceSize – ο αριθμός των δειγμάτων για κάθε ίχνος
%   offset - used to define different beginning of the power trace
%  offset – χρησιμοποιείται για να ορίσει το διαφορετικό ξεκίνημα του ίχνους ισχύος
%   segmentLength - used to define different/reduced length of the power trace
%  segmentLength – χρησιμοποιείται για τον καθορισμό διαφορετικού/μειωμένου μήκους
%για τα ίχνη ισχύος
%   numberOfTraces - number of traces to be loaded
%  numberOfTraces – αριθμός ιχνών που φορτώνονται
%
% To reduce the size of the trace (e.g., to speed-up the computation process)
% modify the offset and segmentLength inputs so the loaded parts of the
% traces correspond to the trace segment you are using for the recovery.
```

% Για μείωση του μεγέθους του ίχνους (π.χ. επιτάχυνση της διαδικασίας υπολογισμού) %τροποποιούμαι τις εισόδους offset και segmentLength, ώστε να φορτώνονται μέρη των %ιχνών που αντιστοιχούν στο τμήμα ίχνους και χρησιμοποιείται για την ανάκτηση κλειδιού

traces = myload('traces-00112233445566778899aabbccddeeff.bin', traceSize, offset, segmentLength, numberOfTraces);

Από τη διαδικασία των μετρήσεων έχουμε εξάγει τα ίχνη ισχύος σε ένα αρχείο τύπου bin το οποίο και χρησιμοποιούμε. Για να το εκμεταλλευτούμε όμως έχουμε δημιουργήσει μια συνάρτηση με το όνομα myload.m και της οποίας τον κώδικα θα δούμε πιο κάτω. Εν συντομία η συγκεκριμένη συνάρτηση θα χρησιμοποιήσει αυτό το αρχείο και σύμφωνα με τα στοιχεία που τις έχουμε ορίσει θα φορτώσει το αρχείο για να μπορέσουμε να το χρησιμοποιήσουμε.

% function myin is used to load the plaintext and ciphertext
% to the corresponding matrices.
% Η συνάρτηση myin χρησιμοποιείται για τη φόρτωση του αρχικού κειμένου και του %κρυπτοκειμένου στους αντίστοιχους πίνακες

% Inputs:
% 'file' - name of the file containing the plaintext or ciphertext
% file – όνομα αρχείου που περιέχει το απλό κείμενο ή το κρυπτογραφημένο κείμενο
% columns - number of columns (e.g., size of the AES data block)
% columns – ο αριθμός των στηλών (π.χ. μέγεθος του AES μπλοκ δεδομένων)
% rows - number of rows (e.g., number of measurements)
% rows – ο αριθμός των γραμμών (π.χ. ο αριθμός των μετρήσεων)

plaintext = myin('plaintext-00112233445566778899aabbccddeeff.txt', columns, rows);
ciphertext = myin('ciphertext-00112233445566778899aabbccddeeff.txt', columns, rows);

Στη συνέχεια με μια άλλη συνάρτηση την myin.m που θα την δούμε και αυτή πιο κάτω φορτώνουμε δυο αρχεία txt τα οποία είναι το plaintext και το ciphertext που τα έχουμε αναφέρει και πιο πάνω. Το plaintext είναι ένα αρχείο με τα δεδομένα που επεξεργάζεται η smartcard μας και είναι ζεύγος με το ciphertext όπως είπαμε. Επίσης όπως αναφέραμε αυτά

είναι ένα ζευγάρι για κάθε ίχνος ισχύος. Έτσι στην περίπτωσή μας που έχουμε μετρήσει 200 ίχνη αν ανοίξουμε τα αρχεία θα δούμε ότι είναι δυσδιάστατοι πίνακες με 200 γραμμές και επειδή η κρυπτογράφησή μας είναι 16byte έχουν 16 στήλες.

%%
%%%
% EXERCISE 1 -- Plotting the power trace(s): %
% Σχεδίαση του ίχνος ισχύος %
%%
%%%
% Plot one trace (or plot the mean value of traces) and check that it is complete
% and then select the appropriate part of the traces (e.g., containing the first round).
% Σχεδιάζουμε ένα ίχνους (ή σχεδιάζουμε μια ενδιάμεση τιμή των ιχνών) και ελέγχουμε %κατά πόσο είναι πλήρες και στη συνέχεια επιλέγουμε το κατάλληλο μέρος των ιχνών

% --> create the plots here <--
%plot(traces(1,1:350000))

Στη συνέχει ακολουθεί ο κώδικας για την εύρεση του κλειδιού. Δημιουργούμε ένα υποθετικό πίνακα για κατανάλωση ενέργειας. Καλώντας τη συνάρτηση mycorr κάνουμε συσχέτιση του αρχικού πίνακα με τις μετρήσεις με το πίνακα που φτιάξαμε με την υποθετική κατανάλωση και αυτό μας βοηθάει να βρούμε το κλειδί.
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% EXERCISE 2 -- Key recovery: %
% Ανάκτηση κλειδιού%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Create the power hypothesis for each byte of the key and then correlate
% the hypothesis with the power traces to extract the key.
% Δημιουργούμε υποθετική τιμή ισχύος για κάθε byte του κλειδιού και στη συνέχεια γίνεται η αντιστοίχιση με τα υποθετικά ίχνη ισχύος για την δημιουργία του κλειδιού

% Task consists of the following parts:
% Η διαδικασία αποτελείται από τα ακόλουθα στάδια
%   - create the power hypothesis

```
%  - δημιουργία υποθετικών τιμών ισχύος
%   - extract the key using the results of the mycorr function
%  - εξαγωγή κλειδιού χρησιμοποιώντας τα αποτελέσματα από τη συνάρτηση mycorr

% variables declaration
% δήλωση μεταβλητών
byteStart = 1;
byteEnd = 16;
keyCandidateStart = 0;
keyCandidateStop = 255;
key = zeros(byteStart, byteEnd);
%step1 =  bitxor(plaintext(N,1), keyCandidateStart)
%powerHypothesis(N, K + 1) =
tab.byte_Hamming_weight((tab.SubBytes(bitxor(plaintext(N,BYTE), keyCandidateStart)
+ 1)) + 1);
% for every byte in the key do:
for BYTE=byteStart:byteEnd

 % Create the power hypothesis matrix (dimensions:
 % Δημιουργούμαι έναν πίνακα για τις υποθετικές μετρήσεις
 % rows = numberOfTraces, columns = 256).
% Οι γραμμές αποτελούνται από την τιμή του numberOfTaces που στην περίπτωση μας
%είναι η τιμή 200 και οι στήλες έχουν την τιμή 256
% The number 256 represents all possible bytes (e.g., 0x00..0xFF).

powerHypothesis = zeros(numberOfTraces,256);
for K = keyCandidateStart:keyCandidateStop
    for N = 1:numberOfTraces
    % --> create the power hypothesis here <--
     powerHypothesis(N, K + 1) =
tab.byte_Hamming_weight((tab.SubBytes(bitxor(plaintext(N,BYTE), K) + 1)) + 1);
    end;
end;
```

```
% function mycorr returns the correlation coeficients matrix calculated
% from the power consumption hypothesis matrix powerHypothesis and the
% measured power traces. The resulting correlation coeficients stored in
% the matrix CC are later used to extract the correct key.
% Η συνάρτηση mycorr επιστρέφει τον πίνακα των συντελεστών αντιστοίχισης
%υπολογίζοντας από τον πίνακα των υποθετικών μετρήσεων κατανάλωσης ισχύος και των
% ιχνών ισχύος που μετρήθηκαν

CC = mycorr(powerHypothesis, traces);

% --> do some operations here to find the correct byte of the key <--
% → κάνουμε κάποιους υπολογισμούς για την εύρεση του σωστού byte του κλειδιού ←

[maxval, row] = max(max(CC,[],2))
[maxval, col] = max(max(CC,[],1))
key(BYTE) = row - 1;
plot(CC(row, 1:10000));
hold on;
end;
for i =1:16
  fprintf ('Byte %d of the key is 0x%2.2X \n', i , key ( i ) ) ;
end ;
```

Κώδικας myin.m

Ο κώδικας αυτός έχει να κάνει με τη συνάρτηση που προαναφέραμε η οποία με χρησιμεύει στο φορτώσουμε τα αρχεία txt που είναι το αρχείο των αρχικών δεδομένων και το αρχείο των κρυπτογραφημένων. Σαν όρισμα η συνάρτηση παίρνει το όνομα του αρχείου το μήκος των δεδομένων και το πλήθος τους. Στην περίπτωσή μας επειδή έχουμε να κάνουμε με πίνακες σαν μήκος εννοούμε τις στήλες και σαν πλήθος τις γραμμές.

```
function [inputs]=myin(fname,ilen,n)
myfile=fopen(fname,'r');
inputs=zeros(n,ilen);
```

```
for i=1:n
        s = fgets(myfile, 1024);
        [ii, l]=sscanf(s, '%02x ', ilen);
        inputs(i,:)=ii;
end
fclose(myfile);
```

Κώδικας myload.m

Ο κώδικας αυτός έχει να κάνει με τη συνάρτηση που προαναφέραμε η οποία με χρησιμεύει στο φορτώσουμε το αρχείο bin που έχει καταχωρημένα τα ίχνη ισχύος από τις μετρήσεις που κάναμε. Σαν όρισμα παίρνει το όνομα του αρχείου πρέπει να ψάξει στο φάκελο του project, το μήκος των δεδομένων του αρχείου, το πρώτο στοιχείο που πρέπει να ξεκινήσει καθώς και το πλήθος των δεδομένων.

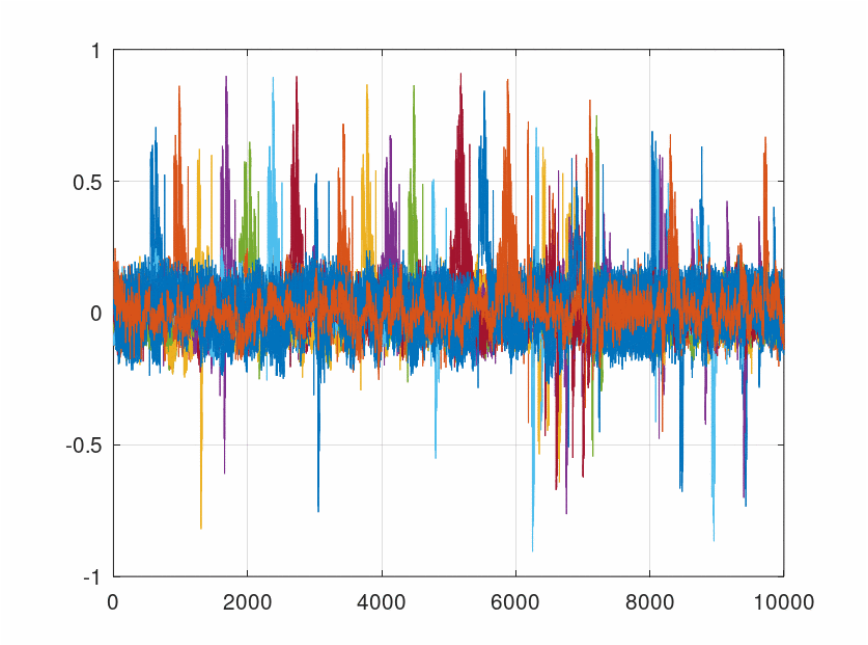
```
function [traces] = myload(fname,trlen,start,len,n)
myfile=fopen(fname,'r');
traces=zeros(n,len);
for i=1:n
        fseek(myfile, start, 'cof');
   if (len+start > trlen)
      t=fread(myfile, len-start, 'uint8');
   else
      t=fread(myfile, len, 'uint8');
   end;
        fseek(myfile, (trlen-len-start), 'cof');
        traces(i,:)=t;
end
fclose(myfile);
```

Κώδικας mycorr.m

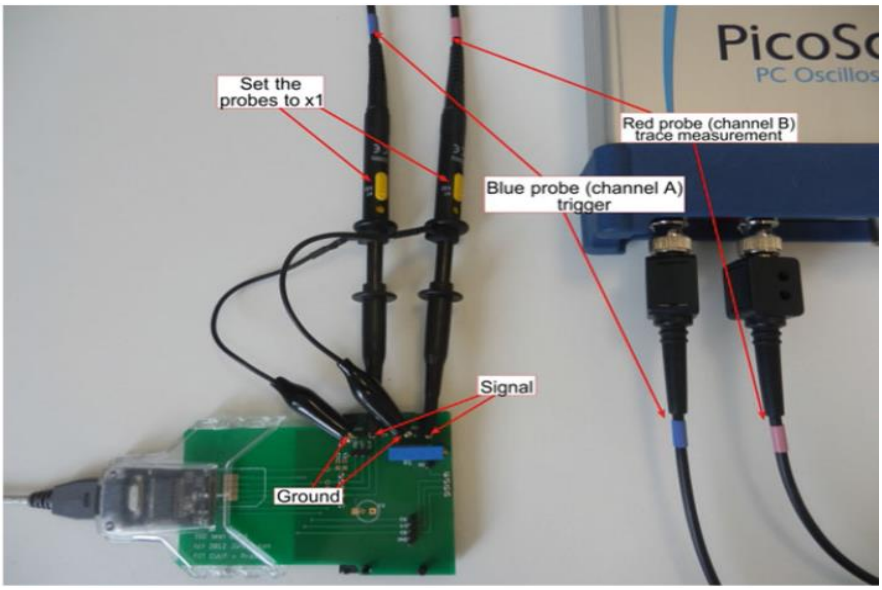
Ο κώδικας της συνάρτησης αυτής μας βοηθάει στο να βρούμε το μυστικό κλειδί.Κάνει συσχέτιση δυο πινάκων. Του πίνακα με τις αρχικές μετρήσεις και του πίνακα υποθετικής κατανάλωσης.

```
function C = mycorr(x,y)
%faster corrcoef for two matrices (octave style)
% γρήγορος συσχετισμός δύο πινάκων
%only real numbers(?)
% μόνο πραγματικοί αριθμοί
%rows ... observations
% γραμμές … παρατηρήσεις
%columns ... variables
% στήλες …. μεταβλητές
  [xr,xc] = size(x);
  [yr,yc] = size(y);
  assert((xr==yr), 'Matrix row count mismatch');
  x = x - repmat(mean(x,1),xr,1); % remove means
  y = y - repmat(mean(y,1),yr,1);
  C = x'*y; % (n-1)cov(x,y)
  C = C ./ repmat((sqrt(sum(x.^2,1)))',1,yc); % divide by sqrt((n-1)var(x))
  C = C ./ repmat(sqrt(sum(y.^2,1)),xc,1); % divide by sqrt((n-1)var(y))
  % resulting C ... correlation coefficient
  %  C = C ./ (repmat((sqrt(sum(x.^2,1)))',1,yc) .* repmat(sqrt(sum(y.^2,1)),xc,1));
end;
```

4.3 Γράφημα



Στο γράφημα βλέπουμε την απεικόνιση κατά την εκτέλεση της Διαφορικής Ανάλυσης. Όπως είχαμε αναφέρει και πιο πάνω όταν επαναλαμβάνουμε την ίδια διαδικασία αλλά δίνουμε διαφορετικά δεδομένα εισόδου έχουμε μικρές διακυμάνσεις οι οποίες φαίνονται με διαφορετικό χρώμα. Οι κορυφές που δημιουργεί το γράφημα είναι τα σημεία που κατά συσχέτιση πιθανό σωστό στοιχείο του κλειδιού.



Εικόνα 4.3: Σύνδεση του προσαργέα ή της πλακέτας στο picosope *για να πάρουμε μετρήσεις [1]*

4.4 Command Window

Εδώ θα δούμε τα αποτελέσματα από το command window που καθώς γίνεται η συσχέτιση για την εύρεση του κλειδιού καταλήγει με το αποτέλεσμα του κλειδιού ανά byte.

maxval = 0.7057

row = 1

maxval = 0.7057

col = 632

maxval = 0.8622

row = 18

maxval = 0.8622

col = 982

maxval = 0.6222

row = 35

maxval = 0.6222

col = 1282

maxval = 0.8999

row = 52

maxval = 0.8999

col = 1682

maxval = 0.6495

row = 69

maxval = 0.6495

col = 2032

maxval = 0.8954

row = 86

maxval = 0.8954

col = 2382

maxval = 0.8986

row = 103

maxval = 0.8986

col = 2732

maxval = 0.6898

row = 120

maxval = 0.6898

col = 8038

maxval = 0.7180

row = 137

maxval = 0.7180

col = 3426

maxval = 0.8673

row = 154

maxval = 0.8673

col = 3782

maxval = 0.6736

row = 171

maxval = 0.6736

col = 4127

maxval = 0.8639

row = 188

maxval = 0.8639

col = 4482

maxval = 0.5073

row = 205

maxval = 0.5073

col = 4776

maxval = 0.9100

row = 222

maxval = 0.9100

col = 5182

maxval = 0.8437

row = 239

maxval = 0.8437

col = 5532

maxval = 0.8878

row = 256

maxval = 0.8878

col = 5882

Byte 1 of the key is 0x00

Byte 2 of the key is 0x11

Byte 3 of the key is 0x22

Byte 4 of the key is 0x33

Byte 5 of the key is 0x44

Byte 6 of the key is 0x55

Byte 7 of the key is 0x66

Byte 8 of the key is 0x77

Byte 9 of the key is 0x88

Byte 10 of the key is 0x99

Byte 11 of the key is 0xAA

Byte 12 of the key is 0xBB

Byte 13 of the key is 0xCC

Byte 14 of the key is 0xDD

Byte 15 of the key is 0xEE

Byte 16 of the key is 0xFF

Αυτό που μπορούμε να παρατηρήσουμε στα παραπάνω αποτελέσματα είναι ότι κατά την συσχέτιση βγαίνει και μια τιμή που όσο πλησιάζει προς το 1 είναι μεγαλύτερη η πιθανότητα να είναι σωστό το κλειδί. Στο τέλος έχουμε και τα 16 byte κωδικοποίησης και δίπλα τις τιμές που είχαν την μεγαλύτερη πιθανότητα και υπερίσχυσαν και έτσι βγαίνει το μυστικό κλειδί.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Nicolas Sklavos & Ricardo Chaves & Giorgio Di Natale & Francesco Regazzoni, Hardware Security & Trust, 2017

2. Mohammad Tehranipoor & Cliff Wang, Introduction to hardware security and trust, 2012

3. Stefan Mangard & Elisabeth Oswald & Thomas Popp, Power Analysis Attacks, 2007

4. Paul Kocher & Joshua Jae & Benjamin Jun & Pankaj Rohatgi, Introduction to differential power analysis, 2011

5. https://en.wikipedia.org/wiki/S-box
6. https://en.wikipedia.org/wiki/Power_analysis#Differential_power_analysis