Πανεπιστήμιο Αιγαίου

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τεχνικές κρυπτογράφησης υλικού

Νικόλαος Καρούσος

Επιβλέπων Καθηγητής: Μανόλης Καλλίγερος

Καρλόβασι, Μάρτιος 2016

Πρόλογος

Στις μέρες μας, οι περισσότερες εταιρίες σχεδίασης ηλεκτρονικών ψηφιακών κυκλωμάτων δεν διαθέτουν ιδιόκτητο εργοστάσιο παραγωγής των κυκλωμάτων τους. Αυτό συμβαίνει εξαιτίας του υψηλού κόστους κατασκευής και συντήρησης των εργοστασίων αυτών. Έτσι τα σχέδια των κυκλωμάτων αποστέλλονται σε εξωτερικά εργοστάσια, τα οποία και τα κατασκευάζουν. Αυτός ο τρόπος σχεδίασης και παραγωγής των κυκλωμάτων έχει δυστυχώς δημιουργήσει μία σειρά από «επιθέσεις» στο υλικό. Για τον λόγο αυτόν πρέπει οι εταιρίες σχεδίασης να λαμβάνουν μέτρα προστασίας των κυκλωμάτων τους, πριν τα στείλουν για παραγωγή σε κάποιο μη έμπιστο εργοστάσιο.

Στο πρώτο κεφάλαιο αυτής της εργασίας θα περιγράψουμε αναλυτικά το συγκεκριμένο πρόβλημα και θα αναφέρουμε διάφορες τεχνικές αντιμετώπισής του. Μία κατηγορία τέτοιων τεχνικών είναι και αυτή της κρυπτογράφησης υλικού (logic encryption). Στο δεύτερο κεφάλαιο θα περιγράψουμε διεξοδικά την πιο αποδοτική μέθοδο της βιβλιογραφίας για κρυπτογράφηση ψηφιακών κυκλωμάτων, με χρήση πυλών XOR και XNOR. Στο τρίτο κεφάλαιο θα περιγράψουμε τα προγράμματα και τα εργαλεία που θα χρησιμοποιήσουμε για να υλοποιήσουμε τη συγκεκριμένη μέθοδο καθώς και άλλες που προτείνονται στην παρούσα διπλωματική. Στη συνέχεια, στο τέταρτο κεφάλαιο θα εξηγήσουμε τη διαδικασία υλοποίησης των διαφόρων μεθόδων. Στα υπόλοιπα κεφάλαια, πέμπτο, έκτο, έβδομο και όγδοο, θα εξετάσουμε νέες εναλλακτικές τεχνικές, που έχουν σαν στόχο τη μείωση του αριθμού των απαιτούμενων πυλών κρυπτογράφησης ενός κυκλώματος ή την επίτευξη μεγαλύτερου ποσοστού εσφαλμένων εξόδων του κυκλώματος με τον ίδιο αριθμό πυλών κρυπτογράφησης. Τέλος, στο ένατο κεφάλαιο θα συγκρίνουμε όλες τις μεθόδους και θα εξάγουμε συμπεράσματα.

Κατάλογος Περιεχομένων

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Ευχαριστίες

Την εκπόνηση μίας διπλωματικής εργασίας θα μπορούσα να την παρομοιάσω με ένα περπάτημα στο βουνό σε ένα άγνωστο μονοπάτι, που όταν ξεκινάς στην αρχή δεν ξέρεις πού φτάνει και εάν η διαδρομή και το τέλος θα σε ικανοποιήσουν. Πολλές φορές συναντάς δύο ή περισσότερες διαδρομές, όπου εάν πάρεις τη λάθος, θα πρέπει να γυρίσεις πίσω και να επιλέξεις τη σωστή. Τελικά, μετά από αρκετό περπάτημα καταφέρνεις και φτάνεις στον προορισμό σου. Μπορεί να έχεις κουραστεί αλλά σε ανταμείβει το θέαμα που αντικρίζεις και όλα όσα έχεις δει στη διαδρομή αυτή. Στο γυρισμό, το μόνο που σκέφτεσαι είναι πότε θα ξαναπερπατήσεις στο βουνό για να εξερευνήσεις μία νέα διαδρομή, φτάνοντας σε έναν νέο προορισμό.

Την περιήγηση αυτή και την επιτυχή κατάληξή της δεν θα μπορούσα να ολοκληρώσω χωρίς την πολύτιμη βοήθεια του επιβλέποντα καθηγητή της διπλωματικής μου κ. Μανόλη Καλλίγερου, Επίκουρου Καθηγητή του Τμήματος Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου. Τον ευχαριστώ πάρα πολύ για τις συμβουλές και την καθοδήγηση που μου προσέφερε σε όλη τη διάρκεια της εκπόνησης της εργασίας. Επίσης θα ήθελα να ευχαριστήσω για τη συμμετοχή τους στην τριμελή επιτροπή τον κ. Χαράλαμπο Σκιάνη, Αναπληρωτή Καθηγητή, Πρόεδρο του Τμήματος και Διευθυντή του Προγράμματος Μεταπτυχιακών Σπουδών, καθώς και τον κ. Δημοσθένη Βουγιούκα Αναπληρωτή Καθηγητή του Τμήματος.

1 Εισαγωγή

Στις μέρες μας, οι ηλεκτρονικές συσκευές είναι παρούσες σε πολλούς τομείς της ζωής μας, όπως για παράδειγμα στις τηλεπικοινωνίες, στις οικιακές συσκευές, στα μεταφορικά μέσα και φυσικά, οπουδήποτε χρησιμοποιείται οποιασδήποτε μορφής υπολογιστής (σταθερός, φορητός, ταμπλέτα κ.τ.λ.). Η εξάπλωση αυτή της χρήσης των ηλεκτρονικών συσκευών οφείλεται, κατά κύριο λόγο, στις ολοένα και αυξανόμενες δυνατότητες των ψηφιακών κυκλωμάτων που ενσωματώνουν. Δυστυχώς η μεγάλη πλειοψηφία των εταιριών που σχεδιάζει τέτοια κυκλώματα δεν διαθέτει εργοστάσια για την κατασκευή τους μίας και το κόστος ενός τέτοιου εργοστασίου είναι πολύ υψηλό. Αυτό έχει ως αποτέλεσμα να αναθέτουν την κατασκευή των σχεδιασμών τους σε άλλες εταιρίες που έχουν εξειδικευμένα εργοστάσια για τον σκοπό αυτό.

Με βάση τον νόμο του Moore, σύμφωνα με τον οποίο ο αριθμός των τρανζίστορ σε ένα πυκνό ολοκληρωμένο κύκλωμα θα διπλασιάζεται κάθε 18 μήνες (εξαιτίας κατά κύριο λόγο της μείωσης του μεγέθους των τρανζίστορ), τα ψηφιακά κυκλώματα γίνονται όλο και πιο πυκνά, με αποτέλεσμα να απαιτούνται συνεχείς αναβαθμίσεις της διαδικασίας κατασκευής τους. Επίσης, ένα ακόμα δεδομένο είναι ότι ο δίσκος πυριτίου πάνω στον οποίο φτιάχνονται τα κυκλώματα αυτά (wafer) είχε διάμετρο 300mm το 2011, η οποία προβλέπεται να φτάσει στα 450mm μέχρι το 2018 [1]. Έτσι, ένα εργοστάσιο παραγωγής ψηφιακών κυκλωμάτων πρέπει συνέχεια να συντηρείται, ώστε να μπορεί, ανά τακτά χρονικά διαστήματα, να παράγει πιο πυκνά και άρα πιο ισχυρά κυκλώματα.

Δεδομένου, λοιπόν, ότι οι περισσότερες εταιρίες σχεδίασης δεν διαθέτουν εργοστάσια κατασκευής, αποστέλλουν τους σχεδιασμούς των κυκλωμάτων τους στα εξειδικευμένα εργοστάσια, τα οποία προχωρούν στην τελική παραγωγή τους. Επιπλέον, η ανάγκη για γρήγορη μετάβαση ενός προϊόντος, από τη φάση σχεδίασης στην αγορά (time-to-market), αναγκάζει τις εταιρίες να αγοράζουν αρκετές προ-σχεδιασμένες μονάδες, ώστε να τις χρησιμοποιήσουν στα συστήματά τους. Οι μονάδες αυτές μπορεί να προέρχονται από οπουδήποτε στον κόσμο.

Αυτή η παγκοσμιοποίηση της βιομηχανίας σχεδίασης ολοκληρωμένων κυκλωμάτων, έχει οδηγήσει σε ένα πλήθος νέων «επιθέσεων» στο υλικό. Ένας «εισβολέας», σε οποιαδήποτε φάση της σχεδίασης ενός ολοκληρωμένου κυκλώματος, μπορεί να προσπαθήσει να ανακαλύψει τη δομή και τη λειτουργία του κυκλώματος, χρησιμοποιώντας τεχνικές αντίστροφης μηχανικής (reverse engineering). Με την αντίστροφη μηχανική, ο εισβολέας αρχικά αφαιρεί το κάλυμμα του ολοκληρωμένου και στην συνέχεια φωτογραφίζει και αφαιρεί ένα – ένα τα επίπεδά του. Τέλος, χρησιμοποιώντας τις απεικονίσεις όλων των επιπέδων προσπαθεί να εξάγει τη δομή του κυκλώματος. Στόχος του είναι η κλοπή και η παράνομη κατοχύρωση της πνευματικής ιδιοκτησίας του κυκλώματος.

Ένα άλλος κίνδυνος που υπάρχει είναι να προστεθεί υλικό trojan σε ένα κύκλωμα. Με τον όρο υλικό trojan εννοούμε την προσθήκη επιπλέον κυκλώματος ή την τροποποίηση του ήδη υπάρχοντος ώστε να επιτελεί λειτουργίες που δε επιθυμεί ο σχεδιαστής. Ένα παράδειγμα μίας μη επιθυμητής λειτουργίας είναι η διαρροή ενός κωδικού σε τρίτους, όταν τον εισάγει ο χρήστης σε ένα κύκλωμα με υλικό trojan.

Επίσης, υπάρχει ο κίνδυνος ένα μη αξιόπιστο εργοστάσιο, από τη στιγμή που έχει τα σχέδια του κυκλώματος, να κατασκευάσει περισσότερα ολοκληρωμένα από αυτά που έχει συμφωνήσει με τον ιδιοκτήτη και να τα πουλήσει το ίδιο, χωρίς την έγκριση του.

Από τις παραπάνω μη επιθυμητές ενέργειες έχει υπολογιστεί ότι η βιομηχανία των κυκλωμάτων ημιαγωγών χάνει κάθε χρόνο 4 δισεκατομμύρια δολάρια. Για αυτόν τον λόγο θα πρέπει με κάποιες μεθόδους να προστατεύονται τα κυκλώματα από τους προαναφερθέντες κινδύνους. Υπάρχουν διάφορες μέθοδοι, οι οποίες εφαρμόζονται πριν την αποστολή των σχεδιασμών στα εργοστάσια κατασκευής και άλλες που εφαρμόζονται μετά την παραλαβή τους. Οι περισσότερες μέθοδοι δεν αντιμετωπίζουν όλους τους κινδύνους, αλλά μερικούς από αυτούς. Τέτοιες μέθοδοι είναι η κρυπτογράφηση υλικού (logic encryption), η διαίρεση βιομηχανικής κατασκευής (split manufacturing), το καμουφλάρισμα κυκλώματος (IC camouflaging) και η ενεργοποίηση trojan (trojan activation).

1.1 Μέθοδοι προστασίας κυκλωμάτων

1.1.1 Κρυπτογράφηση υλικού

Με αυτήν τη μέθοδο κρυπτογραφείται ένα κύκλωμα προσθέτοντάς επιπλέον υλικό σε αυτό. Το επιπλέον υλικό (το οποίο ονομάζεται κύκλωμα κρυπτογράφησης) μπορεί να αποτελείται από πύλες XOR και XNOR, πολυπλέκτες και γενικά, από οποιαδήποτε κύκλωμα επιβάλει κάθε μέθοδος κρυπτογράφησης. Η προσθήκη του κυκλώματος κρυπτογράφησης στο αρχικό κύκλωμα οδηγεί στην αύξηση των εισόδων του τελευταίου. Οι νέες είσοδοι που προστίθενται ονομάζονται είσοδοι κλειδιού. Όπως όταν κρυπτογραφούμε ένα αρχείο ή ένα μήνυμα, για να μπορούμε να το διαβάσουμε στη συνέχεια θα πρέπει να εισάγουμε ένα κλειδί, έτσι και σε ένα κρυπτογραφημένο κύκλωμα, για να λειτουργήσει, θα πρέπει να του εισάγουμε το κλειδί. Το κλειδί είναι μία δυαδική λέξη (αποτελείται από 0 και 1). Εάν δεν εισαχθεί το σωστό κλειδί στις σχετικές εισόδους του κυκλώματος, τότε θα αντιστραφούν κάποιες από τις εξόδους του, με αποτέλεσμα το κύκλωμα να μην παράγει σωστά αποτελέσματα.

Έτσι, εισάγοντας το επιπλέον κύκλωμα κρυπτογράφησης, καθιστούμε την αντιγραφή και μη εγκεκριμένη παραγωγή του κυκλώματος άχρηστη, αφού η εξαγωγή της δομής του παρότι εφικτή, δεν θα έχει νόημα χωρίς τη γνώση του σωστού κλειδιού. Η μέθοδος κρυπτογράφησης υλικού με χρήση πυλών XOR και XNOR θα αναλυθεί σε επόμενο κεφάλαιο της παρούσας διπλωματικής εργασίας.

1.1.2 Διαίρεση βιομηχανικής κατασκευής

Ένα τσιπ αποτελείται από πολλά επίπεδα υλικών (τρανζίστορ και γραμμές «επίπεδα» μετάλλου), τα οποία κατασκευάζονται το ένα πάνω στο άλλο. Σύμφωνα με τη διαδικασία διαίρεσης βιομηχανικής κατασκευής, ο φυσικός σχεδιασμός (layout) ενός ολοκληρωμένου διαχωρίζεται στα δύο: στα χαμηλότερα επίπεδα (επίπεδα front end of line - FEOL) και στα υψηλότερα επίπεδα (επίπεδα back end of line - BEOL), τα οποία κατασκευάζονται σε διαφορετικά εργοστάσια. Τα επίπεδα FEOL αποτελούνται από τα τρανζίστορ και τα χαμηλότερα επίπεδα μετάλλου ενός ολοκληρωμένου, ενώ τα επίπεδα BEOL περιλαμβάνουν τα ανώτερα επίπεδα μετάλλου του ολοκληρωμένου.

Για την παραγωγή του τελικού ολοκληρωμένου υπάρχουν δύο επιλογές. Σύμφωνα με την πρώτη, στα δύο εργοστάσια κατασκευάζονται δύο διαφορετικοί δίσκοι πυριτίου, οι οποίοι, στη συνέχεια, συνενώνονται με χρήση ηλεκτρικών, μηχανικών ή οπτικών μεθόδων ευθυγράμμισης από μία τρίτη εταιρία. Έτσι, κανένα εργοστάσιο δεν έχει όλο το κύκλωμα και άρα δεν μπορεί να επέμβει σε αυτό εισάγοντας υλικό trojan, ενώ επίσης δεν μπορεί και να κατασκευάσει επιπλέον κυκλώματα. Η δεύτερη επιλογή επιτρέπει την κατασκευή των επιπέδων BEOL σε ένα έμπιστο αλλά όχι τόσο εξελιγμένο εργοστάσιο, πάνω στον δίσκο πυριτίου, στον οποίο έχουν κατασκευαστεί τα επίπεδα FEOL από ένα μη έμπιστο αλλά περισσότερο εξελιγμένο εργοστάσιο. Κάτι τέτοιο είναι δυνατό εξαιτίας των χαρακτηριστικών των επιπέδων FEOL και BEOL. Τα επίπεδα BEOL περιλαμβάνουν στοιχεία (γραμμές μετάλλου) μεγαλύτερων διαστάσεων από αυτά των επιπέδων FEOL, με αποτέλεσμα να μπορούν να κατασκευαστούν και από λιγότερο εξελιγμένα εργοστάσια.

1.1.3 Καμουφλάρισμα κυκλώματος

Οι πύλες που υπάρχουν σε ένα ψηφιακό κύκλωμα αποτελούνται από διάφορα τρανζίστορ, των οποίων η συνδεσμολογία καθορίζει και το είδος της πύλης (NAND, NOR, XOR κ.τ.λ.). Η τεχνική του καμουφλαρίσματος προσπαθεί να αποτρέψει έναν επιτιθέμενο από το να εξάγει τη δομή του κυκλώματος με εφαρμογή αντίστροφης μηχανικής. Ένας τρόπος για να γίνει αυτό είναι μέσω της εφαρμογής ψεύτικων συνδέσεων ή αλλιώς επαφών (dummy contacts), στον φυσικό σχεδιασμό του κυκλώματος. Χρησιμοποιώντας έναν συνδυασμό πραγματικών και ψεύτικων επαφών, το φυσικό σχέδιο (layout) μίας λογικής πύλης μπορεί να καμουφλαριστεί έτσι ώστε να μην αναγνωρίζονται οι πραγματικές συνδέσεις μεταξύ των τρανζίστορ της και άρα να μην είναι σαφές σε ποια πύλη αντιστοιχεί (π.χ. NAND ή NOR). Αυτό έχει ως επακόλουθο ο εισβολέας να μην μπορεί να εξάγει την πλήρη δομή του κυκλώματος. Καμουφλαρισμένες πύλες θα πρέπει να εισαχθούν σε διάφορα σημεία του κυκλώματος, έτσι ώστε όταν ο επιτιθέμενος δοκιμάσει να ανακαλύψει τη λειτουργία τους εφαρμόζοντας διάφορες εισόδους στο πραγματικό, κύκλωμα κάτι τέτοιο να μην καταστεί εφικτό λόγω της τοποθέτησης των πυλών αυτών στο κύκλωμα. Φυσικά, η μέθοδος του καμουφλαρίσματος δεν μπορεί να αποτρέψει ένα μη έμπιστο εργοστάσιο από το να κατασκευάσει περισσότερα κυκλώματα και να τα πουλήσει χωρίς την άδεια του σχεδιαστή.

1.1.4 Ενεργοποίηση Trojan

Η συγκεκριμένη μεθοδολογία δεν προσπαθεί να αποτρέψει την αντιγραφή ενός κυκλώματος αλλά να ανιχνεύσει την πιθανή προσθήκη υλικού trojan σε αυτό από κάποιον κακόβουλο σχεδιαστή ή από κάποιο μη έμπιστο εργοστάσιο. Η προσθήκη κακόβουλου υλικού μπορεί να αναγνωριστεί είτε από τη μη αναμενόμενη συμπεριφορά του κυκλώματος, είτε από την αυξημένη κατανάλωση αυτού, όταν το υλικό trojan ενεργοποιηθεί. Το πρόβλημα είναι ότι η ενεργοποίηση ενός κυκλώματος trojan γίνεται από συγκεκριμένες ακολουθίες εισόδων, οι οποίες εμφανίζονται σπάνια. Η μεθοδολογία της ενεργοποίησης trojan στοχεύει στην εισαγωγή δομών στο κύκλωμα, οι οποίες επιτρέπουν την ανάθεση συγκεκριμένων τιμών στο εσωτερικό του, μόνο κατά τη διαδικασία ελέγχου του κυκλώματος για ανίχνευση κακόβουλου υλικού. Έτσι, αν έχει προστεθεί κύκλωμα trojan θα καταναλώσει επιπλέον ενέργεια σε σχέση με αυτή που έχει προβλέψει ο σχεδιαστής, με αποτέλεσμα ο τελευταίος να μπορεί να ελέγξει εάν το αρχικό κύκλωμα έχει παραποιηθεί μέσω της προσθήκης σε αυτό υλικού trojan.

1.2 Περίληψη της διπλωματικής εργασίας

Σε αυτήν τη διπλωματική εργασία μελετούμε αρχικά τη βασική μέθοδο κρυπτογράφησης υλικού με πύλες XOR και XNOR [2], [3] μέσω προσομοιώσεων με χρήση σχετικού κώδικα που αναπτύχθηκε. Μετά εξετάζουμε κάποιες εναλλακτικές στον τρόπο που ελέγχονται οι πύλες κρυπτογράφησης (XOR/XNOR) για να επιτύχουμε το επιθυμητό ποσοστό εσφαλμένων εξόδων, του κρυπτογραφημένου κυκλώματος με ένα τυχαίο κλειδί. Αυτό το κάνουμε για να μειώσουμε τον αριθμό των πυλών κρυπτογράφησης ή για να πετύχουμε καλύτερο ποσοστό εσφαλμένων εξόδων με τον ίδιο αριθμό πυλών με τη βασική μέθοδο. Το ποσοστό εσφαλμένων εξόδων που αναφέραμε ισούται με την απόσταση Hamming (Hamming Distance) των σωστών εξόδων ενός κρυπτογραφημένου κυκλώματος, από τις εξόδους που προκύπτουν όταν δεν χρησιμοποιείται το σωστό κλειδί στο κύκλωμα αλλά κάποιο τυχαίο. Η διαδικασία αυτή θα αναλυθεί στο επόμενο κεφάλαιο.

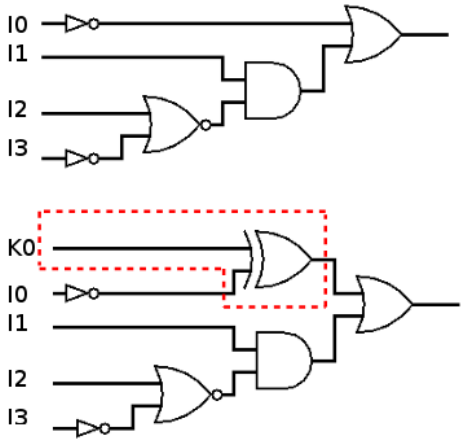
Όπως ήδη αναφέραμε, για να μελετήσουμε τη βασική μέθοδο και τις προτεινόμενες εναλλακτικές ελέγχου των πυλών κρυπτογράφησης αναπτύξουμε ένα πρόγραμμα. Η γλώσσα προγραμματισμού που επιλέξαμε ήταν η Python. Το πρόγραμμα αυτό αρχικά υπολογίζει το σημείο του κυκλώματος στο οποίο πρέπει να τοποθετηθεί μία πύλη κρυπτογράφησης. Τα κριτήρια για την επιλογή του σημείου θα αναλυθούν στο επόμενο κεφάλαιο. Μόλις τελειώσει αυτή η διαδικασία και το πρόγραμμα εντοπίσει το κατάλληλο σημείο, τότε τοποθετεί σε αυτό τη σχετική πύλη. Σε περίπτωση που εξετάζεται κάποια από τις προτεινόμενες εναλλακτικές στο κύκλωμα τοποθετείται επιπλέον και το απαιτούμενο κύκλωμα ελέγχου. Στη συνεχεία υπολογίζεται το Hamming Distance με χρήση του κρυπτογραφημένου κυκλώματος που προέκυψε. Βάση της τιμής του Hamming Distance αποφασίζεται εάν θα επαναληφθεί η παραπάνω διαδικασία ή εάν η μέθοδος έχει ολοκληρωθεί.

2 Βασική μέθοδος κρυπτογράφησης υλικού

Η μέθοδος που θεωρούμε ως βασική περιγράφεται στις εργασίες [2] και [3]. Σε ένα κύκλωμα προσθέτει επιπλέον πύλες, με τη μία από τις δύο εισόδους κάθε τέτοιας πύλης να αποτελεί μία νέα είσοδο του κυκλώματος. Οι νέες αυτές είσοδοι χρησιμοποιούνται για να εισαχθεί το κλειδί του κυκλώματος, το οποίο, όπως έχουμε αναφέρει, είναι μία δυαδική λέξη (αποτελούμενη από 0 και 1). Εάν το κλειδί είναι εσφαλμένο, το κύκλωμα στις εξόδους του δεν θα παράγει το επιθυμητό αποτέλεσμα.

Οι πύλες κρυπτογράφησης που προστίθενται από τη βασική μέθοδο είναι XOR και XNOR. Αρχικά επιλέγεται το κατάλληλο σημείο του κυκλώματος, στο οποίο θα τοποθετηθεί μία νέα τέτοια πύλη. το σημείο αυτό θα συνδεθεί στη μία είσοδο της πύλης κρυπτογράφησης, ενώ η έξοδός της θα οδηγεί όλα εκείνα τα σημεία του κυκλώματος που συνδέονταν αρχικά στο σημείο τοποθέτησης της πύλης. Η άλλη είσοδος της πύλης κρυπτογράφησης θα χρησιμοποιηθεί σαν είσοδος κλειδιού του κυκλώματος. Ο λόγος που επιλέγουμε πύλες XOR για κρυπτογράφηση είναι ότι εάν μία τέτοια πύλη, στην είσοδο που χρησιμοποιείται για το κλειδί, λάβει την τιμή 1, έχει στην έξοδο της την αντεστραμμένη τιμή της άλλης εισόδου. Εάν όμως στην είσοδο για το κλειδί τεθεί η τιμή 0, τότε στην έξοδο θα έχει την ίδια τιμή με την άλλη είσοδο, με αποτέλεσμα να μην μεταβάλλεται σε αυτήν την περίπτωση η λειτουργία του κυκλώματος. Αντίστοιχα λειτουργεί και η πύλη XNOR, με τη διαφορά ότι με την τιμή 1 στην είσοδο κλειδιού θα έχει στην έξοδό της την τιμή της άλλης εισόδου (περίπτωση μη μεταβολής), ενώ με την τιμή 0 στην είσοδο κλειδιού, θα έχει στην έξοδο την αντεστραμμένη τιμή της άλλης εισόδου. Εάν μία πύλη κρυπτογράφησης έχει στην είσοδό κλειδιού την τιμή που προκαλεί την αντίστροφη της τιμής της άλλης της εισόδου, τότε θα επηρεάσει και τις πύλες που οδηγεί, οπότε είναι πιθανό να επηρεαστούν και οι έξοδοι του κυκλώματος.

Στην παρακάτω εικόνα παρουσιάζεται ένα κύκλωμα, το οποίο να προστίθεται μία πύλη XOR πριν από έναν αντιστροφέα, με αποτέλεσμα να δημιουργείται μία νέα είσοδος κλειδιού (η K0) στο αρχικό κύκλωμα.



Σχήμα 2.1: Προσθήκη πύλης XOR για κρυπτογράφηση

Με αυτόν τον τρόπο θα υπάρχει μία δυαδική λέξη, η οποία εάν τοποθετεί στις εισόδους του κυκλώματος που προορίζονται για το κλειδί, δεν θα επηρεάζονται εσωτερικά οι τιμές των σημείων που επιλέχθηκαν κατά την προαναφερθείσα διαδικασία και έτσι το κύκλωμα θα έχει στις εξόδους του το σωστό αποτέλεσμα. Αυτή η δυαδική λέξη θα είναι και το κλειδί του κυκλώματος. Κάθε άλλη δυαδική λέξη θα «ενεργοποιεί» κάποιες από τις πύλες κρυπτογράφησης, με αποτέλεσμα να αντιστρέφονται οι αντίστοιχες τιμές μέσα στο κύκλωμα, αντιστρέφοντας έτσι και κάποιες από τις εξόδους του κυκλώματος. Η πύλη κρυπτογράφησης που θα τοποθετηθεί σε κάποιο σημείο του κυκλώματος προσδιορίζει και την τιμή του αντίστοιχου bit κλειδιού (0 για πύλη XOR και 1 για XNOR). Το αν σε ένα σημείο θα τοποθετήσει μία πύλη XOR ή XNOR αποφασίζεται τυχαία.

Το πιο κρίσιμο σημείο αυτής της μεθόδου είναι ο τρόπος επιλογής των σημείων του κυκλώματος που θα τοποθετηθούν οι πύλες κρυπτογράφησης. Εάν όλες οι πύλες τοποθετηθούν κοντά στις εισόδους ή στις εξόδους του κυκλώματος μπορεί ένας εισβολέας να αντιληφθεί εύκολα ότι αυτές οι πύλες προορίζονται για την κρυπτογράφηση του κυκλώματος, με αποτέλεσμα παρακάμπτοντας 'τες να μπορεί να εξάγει τη δομή του κυκλώματος, αφαιρώντας εντελώς το κύκλωμα κρυπτογράφησης. Ένα άλλο πρόβλημα είναι ότι υπάρχουν σημεία που εάν τοποθετηθούν εκεί οι πύλες και "ενεργοποιηθούν", δεν επηρεάζουν αρκετές εξόδους του κυκλώματος. Ο στόχος είναι να βρεθούν τα σημεία εκείνα, όπου οι πύλες κρυπτογράφησης επηρεάζουν τις περισσότερες δυνατές εξόδους του κυκλώματος.

Ένας τρόπος για να εντοπίσουμε αυτά τα σημεία είναι να χρησιμοποιήσουμε έναν εξομοιωτή απλών σφαλμάτων μόνιμης τιμής (single stuck-at-0 fault και single stuck-at-1 fault - θα τα αναφέρουμε σαν s-a-0 και s-a-1 για ευκολία). Συγκεκριμένα, ο εξομοιωτής, με χρήση κάποιων τυχαίων εισόδων (διανυσμάτων), ελέγχει εάν ένα σφάλμα s-a-0 ή s-a-1 ανιχνεύεται σε μία είσοδο ενός κυκλώματος ή στην έξοδο κάποιας πύλης αυτού. Για κάθε σφάλμα που ανιχνεύεται καταγράφονται επίσης και οι έξοδοι του κυκλώματος, οι οποίες διαφέρουν σε σχέση με την κανονική του λειτουργία (απουσία του σφάλματος). Η διαδικασία αυτή εκτελείται για όλες τις εισόδους και τις εξόδους των πυλών του κυκλώματος, για 1.000 τυχαία διανύσματα εισόδου. Για κάθε ένα από τα σημεία αυτά (είσοδοι και έξοδοι των πυλών του κυκλώματος) υπολογίζουμε μία μετρική που ονομάζεται Fault Impact [2], [3] και επιλέγουμε το σημείο με το μεγαλύτερο Fault Impact για να του προσθέσουμε την πύλη κρυπτογράφησης. Με αυτόν τον τρόπο εντοπίζουμε ένα σημείο κάθε φορά και μετά επαναλαμβάνουμε τη διαδικασία. Φυσικά, πριν από κάθε επανάληψη, θα πρέπει να προστεθεί στο κύκλωμα η νέα πύλη κρυπτογράφησης.

Το Fault Impact μίας εισόδου ή εξόδου πύλης ενός κυκλώματος υπολογίζουμε με τη βοήθεια της ακόλουθης σχέσης:

$$\text{Fault Impact} = NoP_0 \cdot NoO_0 + NoP_1 \cdot NoO_1$$

Το NoP_0 είναι το πλήθος των διανυσμάτων (από τα 1.000 που εξομοιώνουμε) που ανιχνεύουν το σφάλμα s-a-0 στο σημείο που εξετάζουμε.

Το NoO_0 είναι το συνολικό πλήθος των εξόδων, στις οποίες ανιχνεύεται το συγκεκριμένο σφάλμα s-a-0, για όλα τα διανύσματα που εξομοιώνουμε.

Το NoP_1 είναι το πλήθος των διανυσμάτων (από τα 1.000 που εξομοιώνουμε) που ανιχνεύουν το σφάλμα s-a-1 στο σημείο που εξετάζουμε.

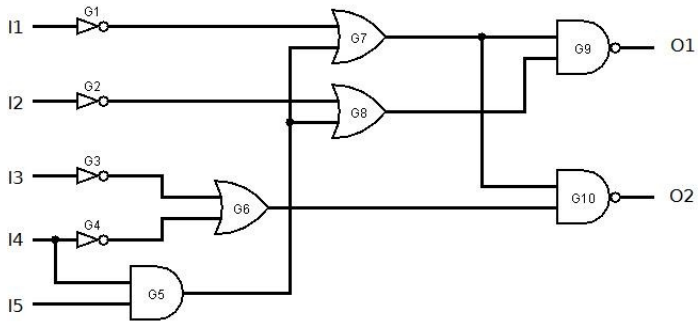
Το NoO_1 είναι το συνολικό πλήθος των εξόδων, στις οποίες ανιχνεύεται το συγκεκριμένο σφάλμα s-a-1, για όλα τα διανύσματα που εξομοιώνουμε.

Κάθε φορά που προσθέτουμε μία πύλη κρυπτογράφησης υπολογίζουμε και το Hamming Distance του κυκλώματος. Το Hamming Distance, είναι όπως αναφέραμε προηγουμένως,0 το ποσοστό των εξόδων του κυκλώματος έχουν εσφαλμένη τιμή, σε περίπτωση που το κλειδί είναι

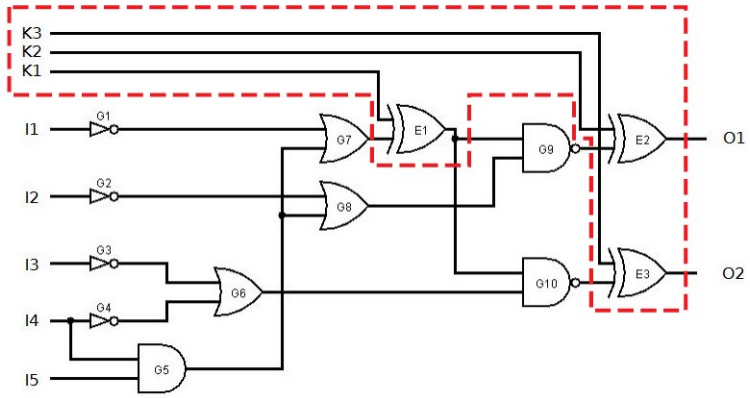
λάθος. Θα πρέπει να σταματήσουμε να τοποθετούμε πύλες κρυπτογράφησης στο κύκλωμα όταν το Hamming Distance φτάσει περίπου στο 50%. Εάν το Hamming Distance είναι 0%, τότε όλες οι έξοδοι είναι σωστές και άρα η κρυπτογράφηση που πραγματοποιούμε είναι αναποτελεσματική. Εάν το Hamming Distance είναι 100%, τότε όλες οι έξοδοι του κυκλώματος είναι λάθος το οποίο επίσης δεν είναι επιθυμητό, αφού με μία απλή αντιστροφή θα έχουμε και πάλι το σωστό αποτέλεσμα. Με Hamming Distance ίσο με 50% οι μισές έξοδοι θα έχουν το σωστό αποτέλεσμα και οι άλλες μισές λάθος, χωρίς όμως να γνωρίζουμε ποιες έξοδοι λειτουργούν σωστά και ποιες όχι (σημειώνουμε ότι ανάλογα με το διάνυσμα εισόδου, διαφορετικές έξοδοι δίνουν κάθε φορά λάθος αποτέλεσμα και διαφορετικές το σωστό). Έτσι, κάποιος εισβολέας εάν δεν έχει το σωστό κλειδί δεν θα έχει τη δυνατότητα να χρησιμοποιήσει σωστά το κύκλωμα. Μόλις το Hamming Distance φτάσει στο 50% σταματάμε να τοποθετούμε πύλες κρυπτογράφησης στο κύκλωμα και θεωρούμε ότι έχει ολοκληρωθεί η κρυπτογράφηση του.

Για να υπολογίσουμε το Hamming Distance κάνουμε τις ακόλουθες ενέργειες. Αφού, προσθέσουμε μία πύλη κρυπτογράφησης, εφαρμόζουμε 1.000 τυχαία διανύσματα με το σωστό κλειδί στο κύκλωμα και υπολογίζουμε τις εξόδους του. Στη συνέχεια, με τα ίδια διανύσματα, αλλά με τυχαία κλειδιά, υπολογίζουμε εκ νέου τις εξόδους του. Συγκρίνουμε αποτελέσματα και των δύο εξομοιώσεων (αυτής με το σωστό κλειδί και αυτής με τα τυχαία κλειδιά) και μετράμε το συνολικό πλήθος των διαφορετικών bits, συγκρίνοντας τις εξόδους για το ίδιο διάνυσμα εισόδου με σωστό και με τυχαίο κλειδί. Αυτό το διαιρούμε αρχικά με το 1.000 ώστε να βρούμε τον μέσο αριθμό των bit εξόδου που διαφέρουν ανά διάνυσμα που εφαρμόσαμε, ενώ στην συνέχεια το διαιρούμε με το πλήθος των εξόδων του κυκλώματος ώστε να υπολογίσουμε το Hamming Distance.

Ένα παράδειγμα εφαρμογής της βασικής μεθόδου κρυπτογράφησης κυκλωμάτων παρουσιάζεται στα Σχήματα 2.2 και 2.3 για το κύκλωμα αναφοράς c17 (περισσότερες λεπτομέρειες για τα κυκλώματα αναφοράς θα δοθούν στο επόμενο κεφάλαιο). Στο Σχήμα 2.2 παρουσιάζουμε το c17 όπως είναι κανονικά (χωρίς την κρυπτογράφηση), ενώ στο Σχήμα 2.3 φαίνεται το c17 κρυπτογραφημένο χρησιμοποιώντας, για λόγους απλότητας, μόνο πύλες XOR. Όταν εφαρμόσαμε τον αλγόριθμο των εργασιών [2], [3] που αναλύθηκε στο κεφάλαιο αυτό, το Hamming Distance έφτασε στο 50% τοποθετώντας μόνο τρεις πύλες κρυπτογράφησης στο κύκλωμα. Στην αρχή ο αλγόριθμος επέλεξε την έξοδο της πύλης G7, στη συνέχεια της G9 και τέλος της G10. Φυσικά, για κάθε πύλη κρυπτογράφησης που τοποθετήθηκε στο κύκλωμα, προέκυψε και η αντίστοιχη είσοδος κλειδιού (είναι οι είσοδοι K1, K2 και K3 στο Σχήμα 2.3). Αν η είσοδος K1 έχει την τιμή 0, τότε η πύλη E1 δεν αντιστρέφει την τιμή της εξόδου της πύλης G7, με αποτέλεσμα να μην επηρεάζεται η λειτουργία του κυκλώματος. Στην περίπτωση που η είσοδος K1 έχει την τιμή 1, τότε η πύλη E1 θα αντιστρέψει τη τιμή σε αυτό το σημείο του κυκλώματος, με αποτέλεσμα να επηρεαστεί όλο το υπόλοιπο κύκλωμα. Αντίστοιχα λειτουργούν η είσοδος K2 με την πύλη E2 και η είσοδος K3 με την πύλη E3.



Σχήμα 2.2: Το κύκλωμα αναφοράς c17



Σχήμα 2.3: Το κύκλωμα αναφοράς c17 μετά την εφαρμογή της μεθόδου κρυπτογράφησης των εργασιών [2], [3]

3 Εργαλεία, προγράμματα και γλώσσες προγραμματισμού που χρησιμοποιήθηκαν στη διπλωματική εργασία

Για να υλοποιήσουμε τη βασική μέθοδο κρυπτογράφησης κυκλωμάτων και τις προτεινόμενες εναλλακτικές, χρησιμοποιήσαμε το πρόγραμμα εξομοίωσης απλών σφαλμάτων μόνιμης τιμή Hope [4] καθώς και τη γλώσσα προγραμματισμού Python. Τα κυκλώματα που χρησιμοποιήσαμε ήταν σε μορφή διασυνδεδεμένων πυλών (netlist). Συγκεκριμένα, χρησιμοποιήθηκε η αναπαράσταση bench (bench-format – αρχεία τύπου bench), την οποία δέχεται ως είσοδο ο εξομοιωτής Hope που αποτέλεσε και το βασικό μας εργαλείο. Το πρόγραμμα που υλοποιήσαμε σε Python καλεί το Hope ορίζοντας το κατάλληλο αρχείο εισόδου τύπου bench, καθώς και τις παραμέτρους της εξομοίωσης. Τα αποτελέσματα της εξομοίωσης εξετάζονται ακολούθως από το πρόγραμμα, το οποίο υπολογίζει το Fault Impact σε όλα τα σημεία του κυκλώματος που μας ενδιαφέρουν, παράγει το νέο αρχείο bench που περιέχει μία επιπλέον πύλη κρυπτογράφησης στο σημείο με το μεγαλύτερο Fault Impact, και κατόπιν υπολογίζει το Hamming Distance για το κύκλωμα αυτό.

3.1 Το πρόγραμμα εξομοίωσης Hope

Το Hope είναι ένας εξομοιωτής απλών σφαλμάτων μόνιμης τιμής. Ένας τέτοιος εξομοιωτής εξετάζει αν ανιχνεύονται κάποια ή όλα τα απλά σφάλματα μόνιμης τιμής (s-a-0 και s-a-1) ενός κυκλώματος, εφαρμόζοντας σε αυτό ένα πλήθος διανυσμάτων εισόδου. Τα κυκλώματα που επεξεργάζεται είναι σε μορφή bench. Είναι γραμμένο σε γλώσσα προγραμματισμού C και ο κώδικάς του είναι ανοικτός. Μπορεί να μεταγλωττιστεί σε λειτουργικά συστήματα UNIX και Linux καθώς σε περιβάλλον cygwin κάτω από Windows. Δεν έχει γραφικό περιβάλλον και εκτελείται από τη γραμμή εντολών χρησιμοποιώντας τις κατάλληλες παραμέτρους. Εμφανίζει κάποια συνοπτικά αποτελέσματα στην οθόνη, ενώ περισσότερες πληροφορίες παρέχει σε κατάλληλα αρχεία που δημιουργεί. Τα αρχεία που δέχεται ως είσοδο είναι απλού κειμένου (text), αλλά σε μορφή UNIX (υπάρχει διαφοροποίηση σε σχέση με τα Windows ως προς το πώς σηματοδοτείται το τέλος μίας γραμμής). Επειδή οι εξομοιώσεις μας πραγματοποιήθηκαν σε περιβάλλον Windows, χρησιμοποιήσαμε το πρόγραμμα dos2unix, το οποίο εκτελείται και αυτό από τη γραμμή εντολών και μετατρέπει τα αρχεία απλού κειμένου από μορφή Windows σε μορφή UNIX. Το Hope μπορεί να δεχθεί αρκετές παραμέτρους. Ενδεικτικά θα αναφέρουμε όσες χρησιμοποιήσαμε στη διπλωματική εργασία.

-t filename Διαβάζει ένα αρχείο με όνομα filename, το οποίο περιλαμβάνει τα διανύσματα εισόδου που θα χρησιμοποιηθούν κατά την εξομοίωση του κυκλώματος. Ένα παράδειγμα με τρία διαφορετικά διανύσματα, υποθέτοντας ότι το κύκλωμα έχει πέντε εισόδους είναι το εξής:

1: 00000
2: 10101
3: 01010

-f filename Διαβάζει ένα αρχείο με όνομα filename, το οποίο περιλαμβάνει όλα τα απλά σφάλματα μόνιμης τιμής που θέλουμε να εξετάσουμε. Για κάθε σημείο ενδιαφέροντος (είσοδο ή έξοδο πύλης) του κυκλώματος, θα πρέπει να συμπεριλάβουμε στο αρχείο τόσο το αντίστοιχο s-a-0 σφάλμα (συμβολίζεται /0), όσο και το s-a-1 (συμβολίζεται /1). Ένα παράδειγμα με τρία διαφορετικά σημεία (G1, G2 και G3) είναι το εξής:

G1 /0
G1 /1
G2 /0
G2 /1
G3 /0
G3 /1

-N Η παράμετρος αυτή αναγκάζει το Hope να μην αγνοεί τα σφάλματα που ανιχνεύτηκαν από τα προηγούμενα διανύσματα (fault dropping). Έτσι, όλα τα σφάλματα που δηλώθηκαν στο σχετικό αρχείο (παράμετρος -f) εξετάζονται για κάθε διάνυσμα εισόδου.

-F filename Δημιουργεί ένα αρχείο με το όνομα filename, στο οποίο καταγράφονται τόσο η σωστή όσο και οι εσφαλμένες έξοδοι του κυκλώματος, για κάθε ένα από τα εξεταζόμενα σφάλματα και για όλα τα εφαρμοζόμενα διανύσματα εισόδου. Ένα παράδειγμα με είσοδο ένα μόνο διάνυσμα των έξι bit (010101), έξι εξεταζόμενα σφάλματα, τέσσερα bit εξόδου (σωστή έξοδος: 1010) και δύο ανιχνευόμενα σφάλματα (οι εσφαλμένες έξοδοι για τα σφάλματα αυτά σημειώνουμε με τον χαρακτήρα *), φαίνεται παρακάτω:

test 1: 010101 1010
G1 /0: 1010
G1 /1: * 1011
G2 /0: * 1111
G2 /1: 1010
G3 /0: 1010
G3 /1: 1010

3.2 Python

Η Python είναι μία open-source γλώσσα προγραμματισμού υψηλού επιπέδου, γενικής χρήσης και πολύ διαδεδομένη σήμερα, η οποία αναπτύχθηκε από τον Guido van Rossum τη δεκαετία του 1990. Ενσωματώνει δυνατότητες του αντικειμενοστραφούς, του συναρτησιακού και του διαδικαστικού προγραμματισμού. Είναι διερμηνευόμενη, δηλαδή για να εκτελεστεί δεν μεταγλωττίζεται σε δυαδικό αρχείο, αλλά εκτελείται απευθείας από τον πηγαίο κώδικα. Το χαρακτηριστικό αυτό έχει το μειονέκτημα ότι η εκτέλεση ενός κώδικα Pyhon είναι πιο αργή από την εκτέλεση του αντίστοιχου κώδικα άλλων μεταγλωττιζόμενων γλωσσών, όπως για παράδειγμα η C. Το μειονέκτημα αυτό όμως, στους σύγχρονους επεξεργαστές που έχουν μεγάλη υπολογιστική ισχύ, δεν γίνεται εύκολα αντιληπτό σε μικρές και μεσαίες εφαρμογές. Η Python έχει τη δυνατότητα να συνδεθεί και με άλλες γλώσσες προγραμματισμού με τη χρήση κατάλληλων διεπαφών, όπως είναι το Pyhon C API. Έτσι, σε κώδικα Python μπορούν να χρησιμοποιηθούν αντικείμενα που έχουν δημιουργηθεί με C ή C++. Η Python εύκολη στην εκμάθηση γιατί συντακτικά μοιάζει πολύ με ψευδοκώδικα και είναι συμβατή με αρκετά λειτουργικά συστήματα όπως τα Windows, το Linux και το Mac Os.

3.3 Αρχεία bench και κυκλώματα αναφοράς

Τα αρχεία τύπου bench είναι αρχεία κειμένου που περιγράφουν κυκλώματα σαν ένα σύνολο (netlist) από διασυνδεδεμένες πύλες και στοιχεία μνήμης (D flip-flop). Παρακάτω παρουσιάζεται ένα παράδειγμα ενός πολυπλέκτη 2-σε-1 σε αναπαράσταση διασυνδεδεμένων πυλών μορφής bench (τα INPUT, OUTPUT, NOT, AND και OR είναι δεσμευμένες λέξεις της αναπαράστασης):

```
INPUT(I0)
INPUT(I1)
INPUT(S)

OUTPUT(O)

S_N = NOT(S)
G0 = AND(I0, S_N)
G1 = AND(I1, S)
O = OR(G0, G1)
```

Για τον έλεγχο των διαφόρων μεθόδων, στην διπλωματική εργασία χρησιμοποιήθηκαν μερικά από τα κυκλώματα αναφοράς ISCAS '85 [5] και ISCAS '89 [6]. Συγκεκριμένα, στον Πίνακα 3.1 σημειώνονται τα κυκλώματα αναφοράς που χρησιμοποιήσαμε στα πειράματα που εκτελέσαμε, καθώς και το πλήθος των εισόδων, των εξόδων και πυλών που αυτά έχουν.

Πίνακας 3.1: Κυκλώματα αναφοράς ISCAS '85 και ISCAS '89 που χρησιμοποιήθηκαν στα πειράματα της διπλωματικής

Όνομα	Είσοδοι	Έξοδοι	Πύλες
c432	36	7	160
c499	41	32	202
c880	60	26	409
c1355	41	32	578
c1908	33	25	1.042
c3540	50	22	1.892
c5315	178	123	2.620
c6288	32	32	2.416
c7552	207	108	3.512
s1196	32	32	529
s1238	32	32	509
s5378	214	228	2.779
s9234	247	250	5.597
s13207	700	790	7.951
s15850	611	684	9.772

Σημειώνουμε ότι όσον αφορά τα τελευταία 6 κυκλώματα, των οποίων το όνομα αρχίζει από τον χαρακτήρα 's', ανήκουν στα ISCAS '89 και είναι ακολουθιακά, στα πειράματα μας χρησιμοποιήσαμε το συνδυαστικό τους τμήμα (και σε αυτό αντιστοιχούν και τα στοιχεία του Πίνακα 3.1).

4 Υλοποίηση της βασικής μεθόδου και των προτεινόμενων εναλλακτικών

4.1 Υλοποίηση της βασικής μεθόδου

Στα πλαίσια της διπλωματικής εργασίας αναπτύχθηκε ένα πρόγραμμα σε γλώσσα προγραμματισμού Python, το οποίο εκτελεί τις παρακάτω ενέργειες

1. Στην αρχή το πρόγραμμα διαβάζει το αρχείο bench του προς κρυπτογράφηση κυκλώματος και εντοπίζει τα ονόματα των εισόδων καθώς και των εξόδων όλων των πυλών αυτού. Με τα ονόματα αυτά, φτιάχνει ένα αρχείο σφαλμάτων για το Hope, το οποίο περιλαμβάνει όλα τα s-a-0 και s-a-1 σφάλματα των σημείων του κυκλώματος που αναφέρθηκαν. Σημειώνουμε ότι όταν επαναλαμβάνεται η διαδικασία, αφού έχει προστεθεί μία πύλη κρυπτογράφησης, το πρόγραμμα φτιάχνει πάλι το παραπάνω αρχείο αφαιρώντας όμως τα σημεία που επιλέχθηκαν στα προηγούμενα βήματα καθώς και τις εξόδους των πυλών κρυπτογράφησης. Αυτό γίνεται γιατί, μετά από πειράματα, παρατηρήσαμε ότι εάν έμενε στο αρχείο ένα σημείο που είχε ήδη επιλεγεί ή η έξοδος της αντίστοιχης πύλης κρυπτογράφησης, τότε τις περισσότερες φορές, η χρήση της μετρικής (Fault Impact) θα οδηγούσε στην επιλογή εκ νέου του ίδιου σημείου, με αποτέλεσμα να δημιουργείται ένα δέντρο από πύλες XOR ή XNOR. Δυστυχώς όμως, αυτό δεν αυξάνει το Hamming Distance.
2. Στη συνέχεια το πρόγραμμα δημιουργεί το αρχείο με τα διανύσματα που θα εξομοιωθούν από το Hope. Σε περίπτωση που στο κύκλωμα έχουν προστεθεί πύλες κρυπτογράφησης, σε κάθε διάνυσμα προστίθεται και το κλειδί. Σύμφωνα με τη μεθοδολογία των εργασιών [2], [3] το κλειδί αυτό είναι τυχαίο, αρκεί να μην είναι το σωστό, κάτι που ελέγχεται από το πρόγραμμα που υλοποιήθηκε. Αν και στη δημοσίευση της βασικής μεθόδου εξομοιώνονταν 1.000 διανύσματα εισόδου για τον υπολογισμό του Fault Impact σε κάθε επανάληψη, παρατηρήσαμε ότι εάν μειώσουμε το πλήθος των διανυσμάτων σε 100 παίρνουμε αντίστοιχα αποτέλεσμα, με τη διαφορά ότι κερδίζουμε σημαντικά σε χρόνο εκτέλεσής. Έτσι αποφασίσαμε, σε κάθε επανάληψη, να χρησιμοποιήσουμε 100 διανύσματα.
3. Το επόμενο βήμα είναι το πρόγραμμα να καλέσει το Hope με είσοδο τα δύο παραπάνω αρχεία αλλά και με το αρχείο bench του κυκλώματος. Πριν όμως τρέξει το Hope, θα πρέπει τα αρχεία αυτά να μετατραπούν με τη βοήθεια της εφαρμογής dos2unix σε μορφή αρχείων κειμένου UNIX για να έχει τη δυνατότητα το Hope να τα διαβάσει. Παρακάτω παρουσιάζεται ένα παράδειγμα κλήσης του Hope από το πρόγραμμα που αναπτύχθηκε, μετά τη δημιουργία και μετατροπή των σχετικών αρχείων εισόδου: hope -t c880oSimulationKey.vec -f c880o.fl -N -F c880o_faulty_outs.log c880o.bench
4. Από το αρχείο εξόδου (Log) που δημιουργεί το Hope, το πρόγραμμα υπολογίζει για κάθε σημείο ενδιαφέροντος το Fault Impact και στο τέλος επιλέγει αυτό με το μεγαλύτερο Fault Impact. Ο τρόπος υπολογισμού του Fault Impact έχει εξηγηθεί στο Κεφάλαιο 2.

5. Αφού επιλεγεί το σημείο εισαγωγής της νέας πύλης κρυπτογράφησης, το πρόγραμμα τροποποιεί το αρχείο bench του κυκλώματος, τοποθετώντας στο σημείο αυτό μία πύλη XOR καθώς και την αντίστοιχη είσοδό κλειδιού. Για λόγους καλύτερης κατανόησης των τεχνικών που θα παρουσιαστούν, στα κυκλώματα δεν προσθέτουμε XOR και XNOR, αλλά μόνο πύλες XOR. Συνεπώς, το σωστό κλειδί είναι η λέξη που περιλαμβάνει μόνο 0. Σε συνθήκες κανονικής χρήσης της μεθόδου το βήμα τοποθέτησης των πυλών XOR διαδέχεται ένα δεύτερο βήμα, το οποίο μετατρέπει τυχαία κάποιες από αυτές σε XNOR ή σε XOR με αντιστροφέα (ώστε ο αντιστροφέας να ενσωματωθεί από το εργαλείο της σύνθεσης στη λογική που ακολουθεί και να αποτραπεί έτσι ένας εισβολέας από το να ανακαλύψει το κλειδί, αν αναγνωρίσει της πύλες κρυπτογράφησης). Φυσικά, στα σημεία αντιστροφής, το αντίστοιχο bit κλειδιού αλλάζει από 0 σε 1. Το δεύτερο αυτό βήμα αυτό είναι απλό, πολύ γρήγορο και ανεξάρτητο της μεθόδου κρυπτογράφησης που εφαρμόστηκε στο κύκλωμα. Στη συγκεκριμένη εργασία όμως μας ενδιαφέρει η βελτίωση της απόδοσης της βασικής μεθόδου κρυπτογράφησης και έτσι, για την καλύτερη κατανόηση των μεθόδων, εξηγούμε μόνο το κύριο βήμα, αυτό της τοποθέτησης των πυλών XOR. Σημειώνουμε ότι το δεύτερο βήμα, απλά τροποποιεί το κλειδί, χωρίς να αλλάζει σε καμία περίπτωση την απόδοση της κρυπτογράφησης Τα σημεία, στα οποία το πρόγραμμα προσθέτει τις πύλες κρυπτογράφησης, αποθηκεύονται επιπλέον σε ένα ξεχωριστό αρχείο, το οποίο θα μας χρησιμεύσει αργότερα, στις εναλλακτικές μεθόδους που θα μελετήσουμε.
6. Αφού το πρόγραμμα προσθέσει τη νέα πύλη κρυπτογράφησης, υπολογίζει το Hamming Distance του νέου κυκλώματος. Για τον υπολογισμό αυτόν θα πρέπει πρώτα να δημιουργηθούν τα αρχεία με τα κατάλληλα διανύσματα για τις εισόδους του κυκλώματος (με τα σωστά και τα τυχαία κλειδιά). Η εξομοίωση πραγματοποιείται και πάλι με τη βοήθεια του Hope, χωρίς όμως αυτή τη φορά να εξετάζονται σφάλματα μόνιμης τιμής (συνεπώς, εκτελείται απλή λογική εξομοίωση). Η διαδικασία υπολογισμού του Hamming Distance έχει περιγραφεί στο Κεφάλαιο 2.

Το πρόγραμμα επαναλαμβάνει όλα τα παραπάνω βήματα μέχρις ότου το Hamming Distance να φτάσει στο 50%. Υπάρχουν όμως κυκλώματα στα οποία το Hamming Distance είναι δύσκολο να φτάσει σε αυτήν την τιμή. Σε τέτοιες περιπτώσεις, το πρόγραμμα σταματάει μετά την προσθήκη 128 πυλών κρυπτογράφησης (εύρος κλειδιού = 128bit).

Παρατηρήσαμε ότι όταν επιχειρούσαμε διαφορετικές κρυπτογραφήσεις του ίδιου κυκλώματος, δεν επιλέγονταν πάντα τα ίδια σημεία για την τοποθέτησης των πυλών κρυπτογράφησης. Αυτό συμβαίνει γιατί όταν υπολογίζουμε το Fault Impact δεν δοκιμάζουμε όλα τα δυνατά διανύσματα εισόδου αλλά μόνο 100 τυχαία. Όλοι οι συνδυασμοί των εισόδων είναι πάρα πολλοί και άρα αδύνατον να δοκιμαστούν. Ακόμα και το πιο μικρό κύκλωμα αναφοράς από αυτά που χρησιμοποιήσαμε στα πειράματά μας, έχει 32 εισόδους, με 2^{32} διαφορετικούς συνδυασμούς, οι οποίοι είναι αδύνατον να ελεγχθούν όλοι. Για αυτόν τον λόγο εκτελέσαμε 20 διαφορετικές εξομοιώσεις για κάθε κύκλωμα και κάθε διαφορετική μέθοδο. Σε κάθε βήμα κάθε τέτοιας εξομοίωσης χρησιμοποιήσαμε διαφορετικά τυχαία διανύσματα, για τον υπολογισμό τόσο του Fault Impact όσο και του Hamming Distance. Βρίσκοντας τον μέσο όρο των αποτελεσμάτων των 20 αυτών εξομοιώσεων μπορούμε να εξάγουμε μία ρεαλιστική εικόνα της απόδοσης της εξεταζόμενης μεθόδου στο υπό κρυπτογράφηση κύκλωμα.

4.2 Υλοποίηση των προτεινόμενων εναλλακτικών μεθόδων

Σκοπός των προτεινόμενων εναλλακτικών μεθόδων είναι είτε η μείωση των πυλών κρυπτογράφησης που απαιτούνται για να επιτευχθεί 50% Hamming Distance σε ένα κύκλωμα, είτε η αύξηση της τιμής του Hamming Distance με τον ίδιο αριθμό πυλών, όταν ο στόχος του

50% δεν είναι εφικτός. Αυτό μπορεί να γίνει αλλάζοντας τον τρόπο που ελέγχονται οι πύλες κρυπτογράφησης, ώστε εάν ένα εσφαλμένο bit κλειδιού «ενεργοποιεί» μία πύλη κρυπτογράφησης, να ενεργοποιεί και άλλες. Έτσι σε ένα κύκλωμα, στο οποίο μπορεί να επιτευχθεί Hamming Distance ίσο με 50%, αυτό γίνεται με λιγότερες πύλες κρυπτογράφησης, αφού συμβαίνει ταυτόχρονη ενεργοποίηση περισσότερων πυλών σε σχέση με τη βασική μέθοδο, ενώ για τον ίδιο λόγο, σε ένα κύκλωμα με Hamming Distance μικρότερο του 50% μπορεί να επιτευχθεί αύξηση του ποσοστού αυτού με το ίδιο αριθμό πυλών, σε σχέση πάντα με τη βασική μέθοδο.

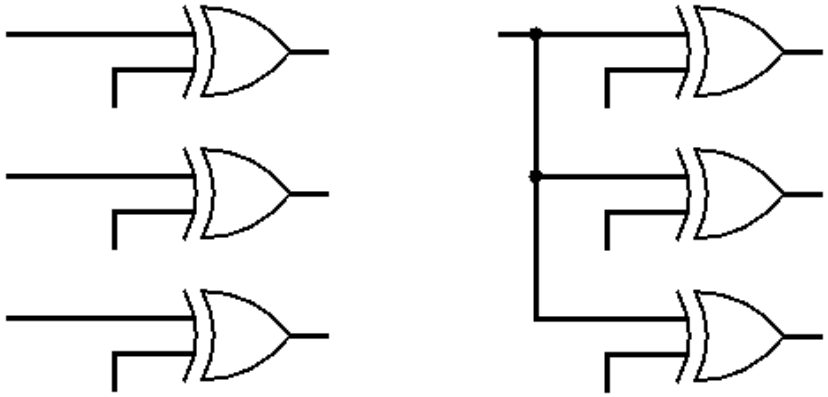
Σε κάθε μία νέα μέθοδο που δοκιμάσαμε, δεν ξαναυπολογίζαμε το Fault Impact, αλλά χρησιμοποιήσαμε τα ίδια σημεία των κυκλωμάτων που είχαν εντοπιστεί από τις εξομοιώσεις της βασικής μεθόδου και είχαν αποθηκευτεί για τον σκοπό αυτό, όπως εξηγήθηκε στο βήμα 5 της προηγούμενης παραγράφου. Βέβαια, μετά την τοποθέτηση κάθε νέας πύλης κρυπτογράφησης και του σχετικού κυκλώματος που τη συνόδευε, ακολουθούσε η πλήρης διαδικασία υπολογισμού του Hamming Distance.

Για να βρούμε την πιο αποδοτική μέθοδο, μετρούσαμε το πλήθος των πυλών κρυπτογράφησης που απαιτούνταν για να γίνει το Hamming Distance ίσο με 50%, για ένα κύκλωμα. Για όσα κυκλώματα το Hamming Distance δεν έφτασε στο 50% με 128 πύλες κρυπτογράφησης, φτιάξαμε διαγράμματα για να συγκρίνουμε τις διάφορες μεθόδους. Στον οριζόντιο άξονα κάθε τέτοιου διαγράμματος φαινόταν ο αριθμός των πυλών κρυπτογράφησης που είχαμε προσθέσει στο κύκλωμα και στον κατακόρυφο το Hamming Distance. Επίσης στα διαγράμματα υπήρχε επιπλέον και μία οριζόντια γραμμή, η οποία έδειχνε την τιμή του μέγιστου Hamming Distance για το κύκλωμα αυτό. Για να υπολογίσουμε το μέγιστο Hamming Distance αντικαθιστούσαμε τα τυχαία κλειδιά της δεύτερης λογικής εξομοίωσης, με ένα κλειδί που έχει όλα τα bit του λάθος (δηλαδή 1, για την περίπτωση που οι πύλες κρυπτογράφησης είναι XOR). Με αυτόν τον τρόπο ενεργοποιούσαμε ταυτόχρονα όλες τις πύλες, οπότε αναμέναμε το Hamming Distance να προσεγγίσει τη μέγιστη τιμή του (για τις συγκεκριμένες πύλες κρυπτογράφησης που είχαν τοποθετηθεί, φυσικά).

5 Πρώτη εναλλακτική μέθοδος

Σκοπός της πρώτης εναλλακτικής μεθόδου, όπως και των υπολοίπων, είναι ένα εσφαλμένο bit κλειδιού να επηρεάζει περισσότερες πύλες κρυπτογράφησης σε ένα κύκλωμα. Σε αυτήν τη μέθοδο απλώς συνδέσαμε μία είσοδο κλειδιού με περισσότερες από μία πύλες κρυπτογράφησης. Πίο συγκεκριμένα, δοκιμάσαμε τέσσερις παραλλαγές. Στην πρώτη παραλλαγή κάθε μία είσοδος κλειδιού συνδεόταν με δύο πύλες κρυπτογράφησης. Αντίστοιχα, στη δεύτερη παραλλαγή συνδεόταν με τρεις, στην τρίτη παραλλαγή συνδεόταν με τέσσερις και τέλος, στην τέταρτη παραλλαγή συνδεόταν πέντε πύλες κρυπτογράφησης.

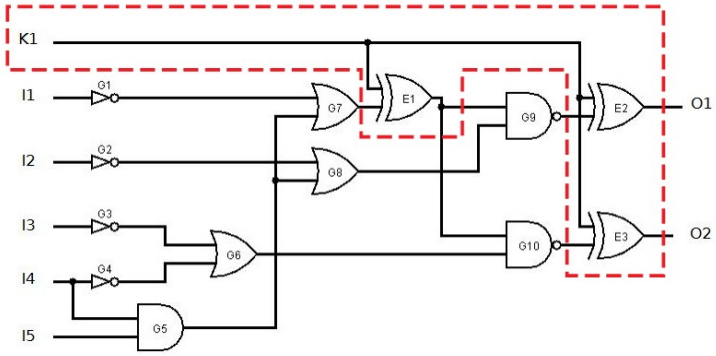
Στην αριστερή πλευρά του Σχήματος 5.1 παρουσιάζονται τρεις πύλες XOR που χρησιμοποιούνται για την κρυπτογράφηση ενός κυκλώματος και έχουν η κάθε μία τη δική της είσοδο για το κλειδί, όπως προτείνεται από τη βασική μέθοδο. Στα δεξιά του Σχήματος 5.1 παρουσιάζεται ο τρόπος που αυτές οι τρεις πύλες συνδέονται με μία κοινή είσοδο κλειδιού. Αντίστοιχα, και οι υπόλοιπες πύλες κρυπτογράφησης του κυκλώματος θα συνδεθούν με τον ίδιο τρόπο και πάντα θα είναι σε ομάδες των τριών πυλών, αφού υποθέτουμε ομαδοποίηση τριών πυλών ανά είσοδο κλειδιού (εκτός βέβαια από την τελευταία ομάδα η οποία θα αποτελείται από μία ή δύο πύλες, ανάλογα με το πόσες έχουν απομείνει). Ο ίδιος τρόπος θα χρησιμοποιηθεί για την πρώτη, τρίτη και τέταρτη παραλλαγή αυτής της μεθόδου.



(α) *(β)*

Σχήμα 5.1: Συνδεσμολογία των πυλών κρυπτογράφησης: (α) της βασικής μεθόδου (β) της πρώτης εναλλακτικής μεθόδου με ομαδοποίηση τριών πυλών ανά είσοδο κλειδιού

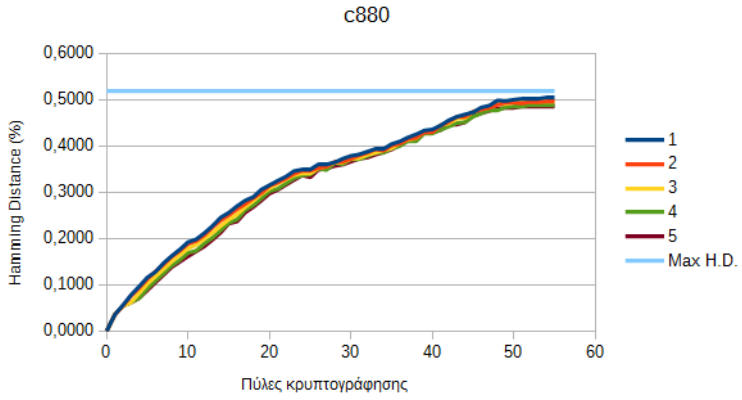
Ένα παράδειγμα για το πως εφαρμόζεται αυτή η μέθοδος στο κύκλωμα αναφοράς c17 παρουσιάζεται στο Σχήμα 5.2. Τα σημεία που τοποθετούνται οι πύλες κρυπτογράφησης είναι τα ίδια με τη βασική μέθοδο (δηλαδή οι έξοδοι των πυλών G7, G9 και G10). Η διαφορά είναι ότι σε κάθε πύλη κρυπτογράφησης δεν αντιστοιχεί μία ξεχωριστή είσοδος κλειδιού, αλλά όλες οι πύλες συνδέονται σε μία κοινή είσοδο, την K1. Αυτό έχει ως αποτέλεσμα εάν η είσοδος K1 έχει την τιμή 0 (σωστό κλειδί) να μην υπάρχει αντιστροφή σε κανένα από τα επιλεγμένα σημεία, ενώ εάν έχει την τιμή 1 (λάθος κλειδί) να πραγματοποιείται αντιστροφή και στα τρία σημεία.



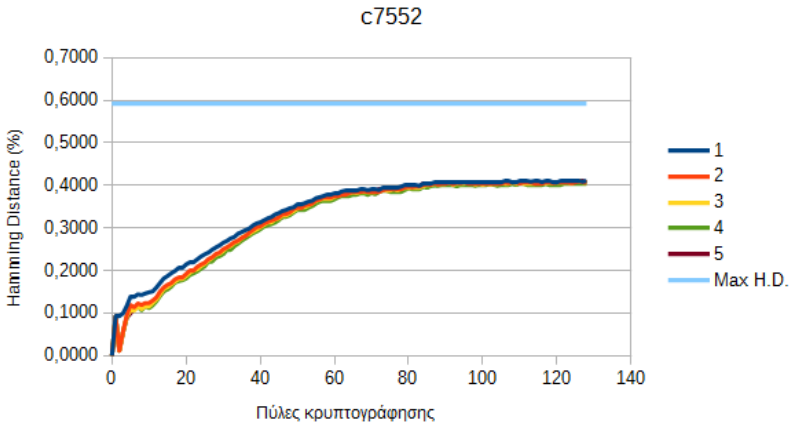
Σχήμα 5.2: Εφαρμογή της πρώτης εναλλακτικής μεθόδου στο κύκλωμα c17

5.1 Αποτελέσματα

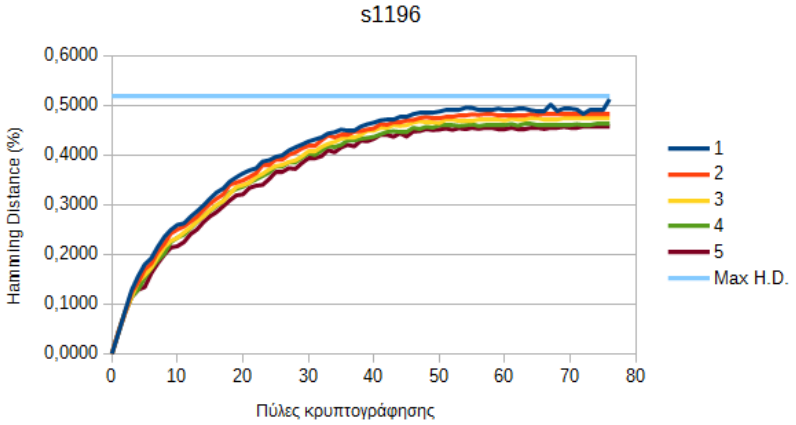
Η παραπάνω μέθοδος δοκιμάστηκε σε έξι κυκλώματα. Αυτά είναι τα c880, c7552, s1196, s1238, s5378 και s9234. Δεν καταφέραμε σε κανένα επιτύχουμε 50% Hamming Distance με 128 πύλες κρυπτογράφησης. Έτσι δημιουργήσαμε τα παρακάτω διαγράμματα, ένα για κάθε κύκλωμα. Στα διαγράμματα αυτά, η σκούρα μπλε καμπύλη (1) αντιστοιχεί στη βασική μέθοδο, η πορτοκαλί καμπύλη (2) αφορά την παραλλαγή με ομαδοποίηση δύο πυλών κρυπτογράφησης ανά είσοδο κλειδιού, η κίτρινη καμπύλη (3) αντιστοιχεί στην ομαδοποίηση τριών πυλών κρυπτογράφησης ανά bit κλειδιού, η πράσινη (4) στην ομαδοποίηση τεσσάρων πυλών και η μοβ (5) στην ομαδοποίηση πέντε πυλών. Η γαλάζια γραμμή (Max H.D.) δείχνει το μέγιστο Hamming Distance του κυκλώματος, με κρυπτογράφηση του σύμφωνα με την βασική μέθοδο. Υπενθυμίζουμε ότι στα διαγράμματα που ακολουθούν, όπως και σε όλα τα αντίστοιχα διαγράμματα των άλλων μεθόδων οι καμπύλες που παρουσιάζονται αντιστοιχούν στο μέσο όρο των αποτελεσμάτων των 20 εξομοιώσεων που εκτελέσαμε για κάθε κύκλωμα. Σημειώνουμε ότι κάποια από τα κυκλώματα που εξετάζουμε (c880, s1196 και s1238), η βασική μέθοδος οδήγησε σε 50% Hamming Distance ίσο με 50%, με λιγότερες από 128 πύλες κρυπτογράφησης. Για τα κυκλώματα αυτά δεν προχωρήσαμε στην εύρεση περισσοτέρων σημείων εισαγωγής πυλών, για χρήση τους με την πρώτη εναλλακτική, καθώς ενδιαφερόμαστε για τη σύγκριση των προτεινόμενων εναλλακτικών με τη βασική μέθοδο, κάτω από τις ίδιες συνθήκες κρυπτογράφησης.



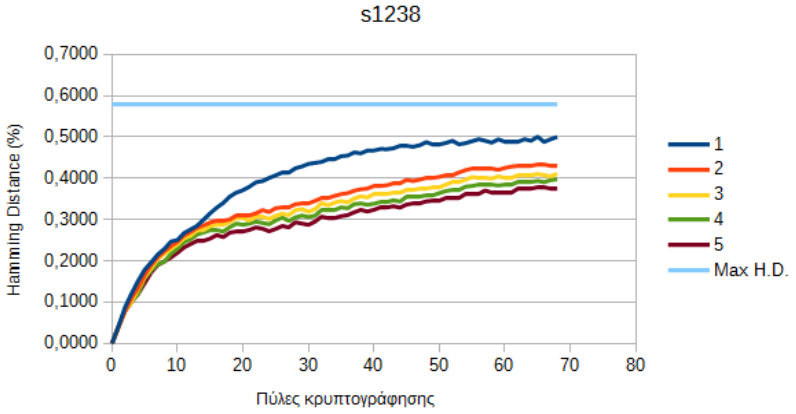
Σχήμα 5.3: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του c880 σύμφωνα με την πρώτη εναλλακτική μέθοδο



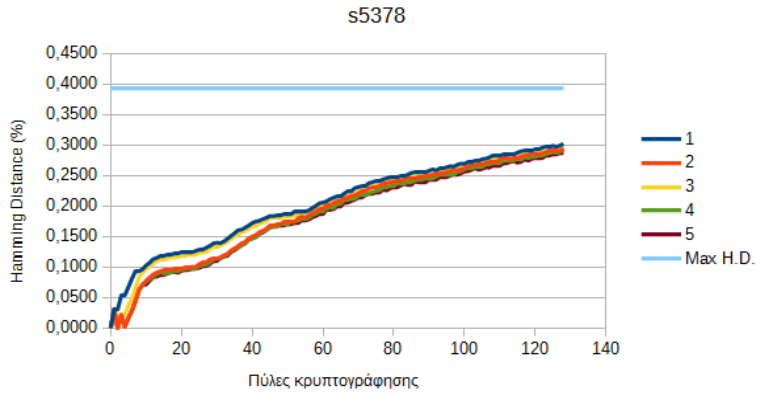
Σχήμα 5.4: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του c7552 σύμφωνα με την πρώτη εναλλακτική μέθοδο



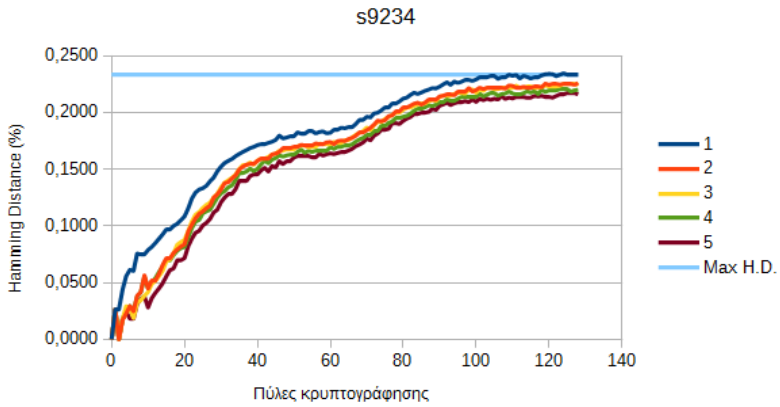
Σχήμα 5.5: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του s1196 σύμφωνα με την πρώτη εναλλακτική μέθοδο



Σχήμα 5.6: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του s1238 σύμφωνα με την πρώτη εναλλακτική μέθοδο



Σχήμα 5.7: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του s5378 σύμφωνα με την πρώτη εναλλακτική μέθοδο



Σχήμα 5.8: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του s9234 σύμφωνα με την πρώτη εναλλακτική μέθοδο

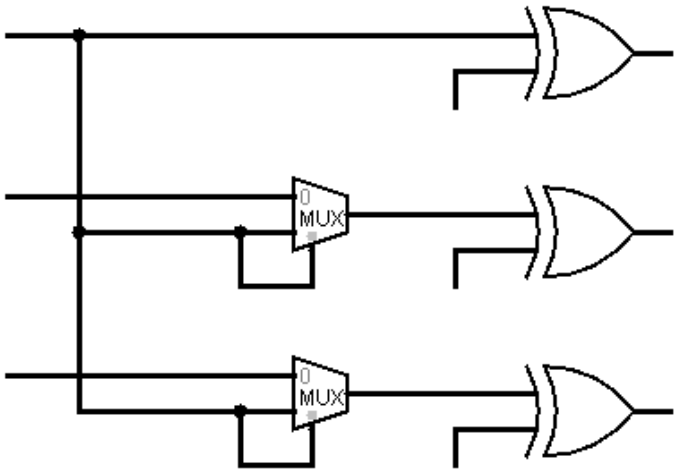
5.2 Σχολιασμός των αποτελεσμάτων

Όπως παρατηρούμε σε όλα τα διαγράμματα, όλες οι παραλλαγές της πρώτης μεθόδου δυστυχώς οδήγησαν σε χειρότερο (δηλαδή μικρότερο) Hamming Distance σε σχέση με τη βασική μέθοδο. Πίο συγκεκριμένα, όσο αυξάναμε τις πύλες κρυπτογράφησης, τόσο αυξάνονταν και το Hamming Distance του κυκλώματος, αλλά πάντα οι τιμές του ήταν μικρότερες από αυτές της βασικής μεθόδου. Ο λόγος είναι ότι ναι μεν κάθε λάθος bit κλειδιού επηρεάζει περισσότερες από μία πύλες κρυπτογράφησης του κυκλώματος, το οποίο είναι επιθυμητό, αλλά δυστυχώς το ίδιο συμβαίνει και για κάθε σωστό bit κλειδιού. Δηλαδή, μία σωστή είσοδος κλειδιού επιτρέπει τη διάδοση της σωστής τιμής του κυκλώματος μέσα από όλες τις πύλες κρυπτογράφησης που συνδέεται. Το γεγονός αυτό αναιρεί την επίδραση των εσφαλμένων εισόδων κλειδιού στη συνολική τιμή του Hamming Distance.

Παρατηρώντας το παραπάνω πρόβλημα, βγάλαμε το εξής συμπέρασμα: κάθε μία πύλη κρυπτογράφησης, θα πρέπει να έχει τη δική της είσοδο κλειδιού, αλλά θα πρέπει να μπορεί να επηρεάζεται και από κάποια άλλη είσοδο, εφόσον η τελευταία έχει λάθος τιμή. Κατά αυτόν τον τρόπο θα καταλήγουν στις πύλες κρυπτογράφησης περισσότερα εσφαλμένα bit, με αποτέλεσμα την επίτευξη υψηλότερων τιμών για το Hamming Distance.

6 Δεύτερη εναλλακτική μέθοδος

Σκοπός της δεύτερης εναλλακτικής μεθόδου είναι η επίδραση μίας εισόδου κλειδιού σε πολλαπλά σημεία κρυπτογράφησης ενός κυκλώματος να πραγματοποιείται υπό συνθήκη και συγκεκριμένα, μόνο όταν η τιμή της εισόδου αυτής είναι εσφαλμένη. Με αυτόν τον τρόπο θα αποφύγουμε το πρόβλημα που εμφανίστηκε στην πρώτη μέθοδο που παρουσιάσαμε. Τη λειτουργία αυτή μπορούμε να την επιτύχουμε τοποθετώντας πολυπλέκτες στο κύκλωμα. Συγκεκριμένα πραγματοποιούμε και πάλι ομαδοποιήσεις των πυλών κρυπτογράφησης, αλλά η κάθε πύλη διατηρεί και μία ξεχωριστή είσοδο κλειδιού. Η συνδεσμολογία της πρώτης πύλης κάθε ομάδας είναι ίδια με αυτή της βασικής μεθόδου, με τη διαφορά ότι η είσοδος κλειδιού της δεν συνδέεται απευθείας με άλλες πύλες κρυπτογράφησης αλλά διαμέσου ενός πολυπλέκτη 2-σε-1 (απαιτείται ένας πολυπλέκτης για κάθε διασυνδεόμενη πύλη). Συγκεκριμένα, η είσοδος κλειδιού της πρώτης πύλης μίας ομάδας συνδέεται σε δύο σημεία κάθε πολυπλέκτη: στην είσοδο επιλογής καθώς και σε μία κανονική είσοδο αυτού (σε αυτή που οδηγείται στην έξοδο με τη γραμμή επιλογής ίση με 1, αν η πύλη κρυπτογράφησης είναι XOR, ή σε αυτή που οδηγείται στην έξοδο με 0 στη γραμμή επιλογής, αν η πύλη κρυπτογράφησης είναι XNOR). Στην άλλη είσοδο του πολυπλέκτη συνδέεται η είσοδος κλειδιού που αντιστοιχεί σε κάθε μία από τις διασυνδεόμενες πύλες. Στο Σχήμα 6.1 παρουσιάζονται τρεις πύλες κρυπτογράφησης συνδεδεμένες με αυτόν τον τρόπο (ομαδοποίηση πυλών ανά τρείς).



Σχήμα 6.1: Συνδεσμολογία των πυλών κρυπτογράφησης της δεύτερης εναλλακτικής μεθόδου με ομαδοποίηση τριών πυλών ανά είσοδο κλειδιού

Σύμφωνα με τη μέθοδο αυτή, αν υποθέσουμε ίση πιθανότητα εμφάνισης της τιμής 0 ή 1 σε μία είσοδο κλειδιού, η πιθανότητα ενεργοποίησης της πρώτης πύλης (αυτής, στην οποία συνδέεται απευθείας η είσοδος κλειδιού) είναι 1/2. Οι υπόλοιπες πύλες κρυπτογράφησης όμως λαμβάνουν την είσοδο κλειδιού της πρώτης, όταν αυτή είναι εσφαλμένη, ενώ διαφορετικά οδηγούνται από την τιμή της δικής τους εισόδου κλειδιού (αυτός είναι και ο λόγος ύπαρξης των πολυπλεκτών που τοποθετούνται σε αυτές). Άρα, κάθε μία από τις πύλες αυτές μπορεί να οδηγηθεί από δύο

διαφορετικές εισόδους κλειδιού. Συνεπώς υπάρχουν τέσσερις διαφορετικοί συνδυασμοί αυτών των δυο εισόδων και μόνο για έναν δεν ενεργοποιείται η πύλη (δηλ. δεν αντιστρέφει την τιμή του καλύμματος στο σημείο τοποθέτησης της). Άρα, η πιθανότητα να αντιστραφεί η τιμή του κυκλώματος στο συγκεκριμένο σημείο είναι 3/4. Στον Πίνακα 6.1 παρουσιάζονται οι συνδυασμοί τιμών της εισόδου κλειδιού της πρώτης πύλης κρυπτογράφησης μίας ομάδας (A) και της εισόδου κλειδιού μίας οποιαδήποτε άλλης πύλης κρυπτογράφησης (B), της ίδιας ομάδας.

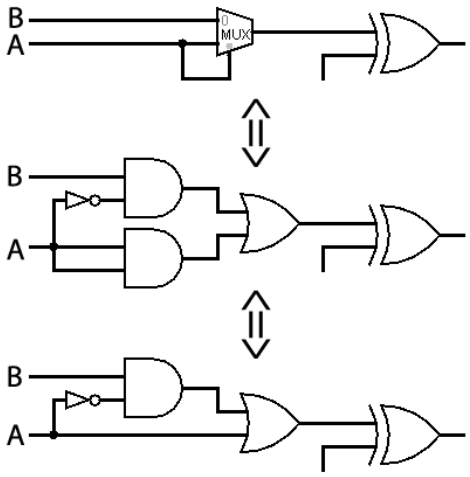
Πίνακας 6.1: Συνδυασμοί εισόδων κλειδιού της πρώτης (A) και μίας οποιασδήποτε άλλης πύλης (B) μίας ομάδας

A	B	Ενεργοποίηση της πύλης που αντιστοιχεί στην είσοδο B
0	0	Όχι
0	1	Ναι (λόγω της εισόδου B)
1	0	Ναι (λόγω της εισόδου A)
1	1	Ναι (λόγω της εισόδου A)

Παρατηρούμε ότι για να μην ενεργοποιηθεί η πύλη κρυπτογράφησης που αντιστοιχεί στην είσοδο B πρέπει να έχουν σωστή τιμή και οι δύο είσοδοι κλειδιού που την επηρεάζουν.

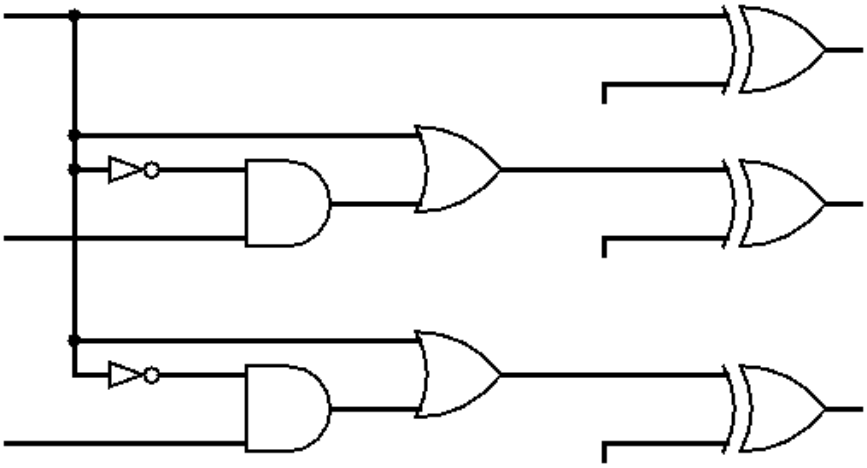
Μπορούμε να απλοποιήσουμε το κύκλωμά μας με τον εξής τρόπο: σε έναν πολυπλέκτη 2-σε-1, εάν μία είσοδος είναι και είσοδος επιλογής, έχουμε μία πύλη AND, στις δύο εισόδους της οποίας συνδέεται η ίδια γραμμή. Έστω ότι με I_0 και I_1 συμβολίζουμε τις δυο κανονικές εισόδους του πολυπλέκτη και με S την είσοδο επιλογής. Η αλγεβρική σχέση που περιγράφει τον πολυπλέκτη 2-σε-1 είναι η $Y = I_0 \cdot S' + I_1 \cdot S$, όπου Y είναι η έξοδος του πολυπλέκτη. Ακολουθώντας την ονοματολογία με τις εισόδους κλειδιού A και B που χρησιμοποιήσαμε μέχρι τώρα, για ένα πολυπλέκτη μίας ομάδας πυλών κρυπτογράφησης θα ισχύει $S = I_1 = A$ και $I_0 = B$. Συνεπώς, η αλγεβρική έκφραση ενός τέτοιου πολυπλέκτη μετατρέπεται ως εξής:
$Y = B \cdot A' + A \cdot A \Rightarrow Y = B \cdot A' + A$

Στο Σχήμα 6.2 παρουσιάζουμε τη συγκεκριμένη απλοποίηση σε επίπεδο πυλών.



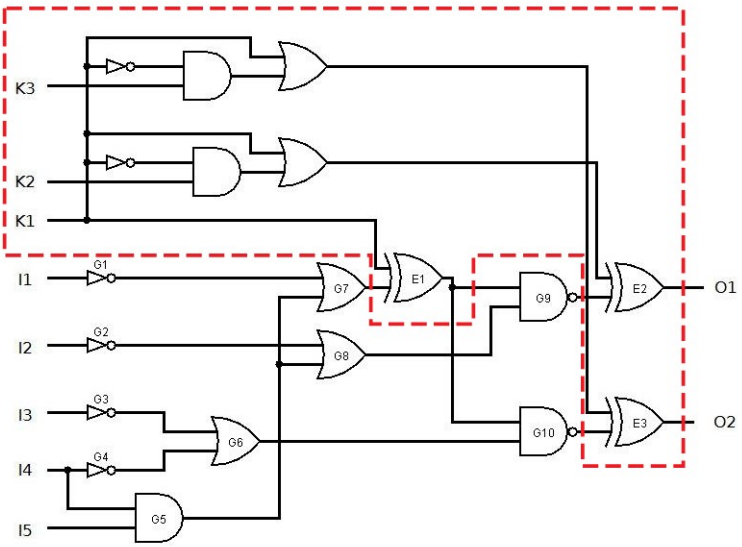
Σχήμα 6.2: Απλοποίηση πολυπλέκτη για τη δεύτερη εναλλακτική μέθοδος κρυπτογράφησης κυκλωμάτων

Στο Σχήμα 6.3 παρουσιάζεται η ομαδοποίηση τριών πυλών κρυπτογράφησης σύμφωνα με τη δεύτερη εναλλακτική μέθοδο (ακριβώς η ίδια με αυτή του Σχήματος 6.1), έχοντας τοποθετήσει τους απλοποιημένους πολυπλέκτες.



Σχήμα 6.3: Η ομαδοποίηση του Σχήματος 6.1 με απλοποιημένους πολυπλέκτες

Ένα παράδειγμα του πώς εφαρμόζεται η δεύτερη εναλλακτική μέθοδος στο κύκλωμα αναφοράς c17 παρουσιάζεται στο Σχήμα 6.4. Η πύλη E1 συνδέεται κατευθείαν στην είσοδο K1 και εξαρτάται μόνο από αυτήν. Οι πύλες E2 και E3 θα συνδεθούν και με τις εισόδους K2 και K3 αντίστοιχα αλλά και με την είσοδο K1 μέσω πολυπλεκτών. Για να αντιστρέψουν τις τιμές των πυλών G9 και G10 αντίστοιχα θα πρέπει ή να λάβουν την τιμή 1 από την είσοδο K1 ή, αν K1 = 0, να λάβουν 1 από τη δική τους είσοδο κλειδιού (K2 και K3 αντίστοιχα). Για να μην αντιστρέψουν τις τιμές των G9 και G10 θα πρέπει, για την πύλη E2, να τεθεί στην τιμή 0 τόσο η είσοδος K1 όσο και η K2. Αντίστοιχα, για την E3, θα πρέπει να τεθεί στην τιμή 0 η K1 και η K3.



Σχήμα 6.4: Εφαρμογή της δεύτερης εναλλακτικής μεθόδου στο κύκλωμα c17

Θα εξετάσουμε και πάλι τέσσερις παραλλαγές της δεύτερης εναλλακτικής μεθόδου. Στην πρώτη παραλλαγή, η είσοδος κλειδιού της πρώτης πύλης θα συνδέεται μέσω πολυπλέκτη με μόνο άλλη μία πύλη κρυπτογράφησης (ομαδοποίηση δύο πυλών). Αντίστοιχα στις υπόλοιπες παραλλαγές θα εξετάσουμε ομαδοποιήσεις τριών (όπως στο Σχήμα 6.1), τεσσάρων και πέντε πυλών.

6.1 Αποτελέσματα

Η μέθοδος που αναλύσαμε δοκιμάστηκε στα ίδια κυκλώματα αναφοράς που χρησιμοποιήθηκαν για την εκτίμηση της πρώτης εναλλακτικής μεθόδου (c880, c7552, s1196, s1238, s5378 και s9234). Στα c880, s1196 και s1238 καταφέραμε να επιτύχουμε Hamming Distance ίσο ή και λίγο μεγαλύτερο από 50% με λιγότερες από 128 πύλες. Για τα κυκλώματα αυτά θα παρουσιάσουμε πίνακες με το πλήθος των πυλών που χρειαστήκαμε για να φτάσει το Hamming Distance στην επιθυμητή τιμή (50%). Επειδή εκτελέσαμε 20 εξομοιώσεις για κάθε κύκλωμα και κάθε διαφορετική ομαδοποίηση, θα παρουσιάσουμε, τις λιγότερες πύλες που χρειαστήκαμε σε ένα πείραμα (ΜΙΚ.), τις περισσότερες (ΜΕΓ.), καθώς και τον μέσο όρο (Μ.Ο.) των 20 εξομοιώσεων. Για τα υπόλοιπα κυκλώματα που το Hamming Distance δεν έφτασε στο 50%, φτιάξαμε διαγράμματα αντίστοιχα με αυτά του Κεφαλαίου 5. Τα χρώματα των καμπυλών αφορούν την ίδια ακριβώς ομαδοποίηση με το Κεφάλαιο 5, ενώ για λόγους σύγκρισης, συνεχίζουμε στα διαγράμματα να παρουσιάζουμε και τα αποτελέσματα της βασικής μεθόδου (είναι η σκούρα μπλε καμπύλη που σημειώνεται με τον αριθμό 1).

Πίνακας 6.2: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του c880 σύμφωνα με τη δεύτερη εναλλακτική μέθοδο (αριθμός πυλών κρυπτογράφησης)

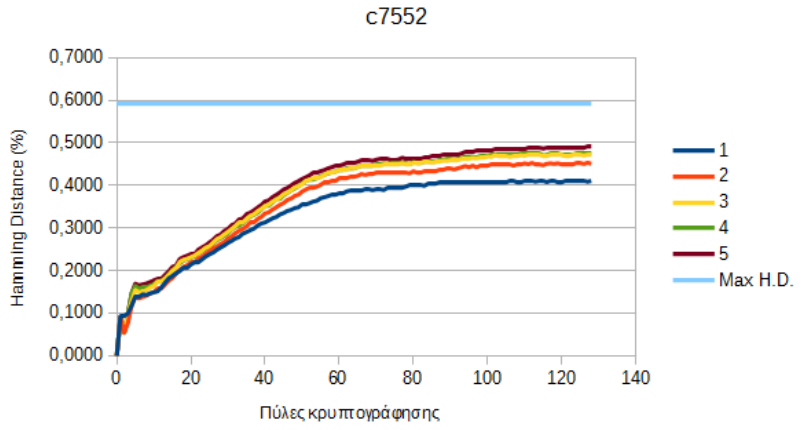
	Βασική μέθοδος	Ομαδοποίηση 2 πυλών	Ομαδοποίηση 3 πυλών	Ομαδοποίηση 4 πυλών	Ομαδοποίηση 5 πυλών
Μ.Ο.	48,7	38,3	36,3	35,2	34,2
ΜΕΓ.	52	43	40	40	40
ΜΙΚ.	46	33	32	31	31

Πίνακας 6.3: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του s1196 σύμφωνα με τη δεύτερη εναλλακτική μέθοδο (αριθμός πυλών κρυπτογράφησης)

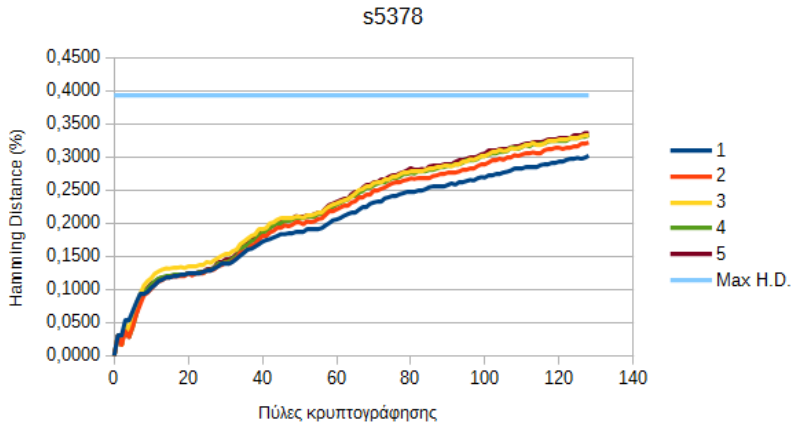
	Βασική μέθοδος	Ομαδοποίηση 2 πυλών	Ομαδοποίηση 3 πυλών	Ομαδοποίηση 4 πυλών	Ομαδοποίηση 5 πυλών
Μ.Ο.	53,0	36,3	33,3	33,0	31,5
ΜΕΓ.	76	48	42	39	36
ΜΙΚ.	46	30	30	28	28

Πίνακας 6.4: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του s1238 σύμφωνα με τη δεύτερη εναλλακτική μέθοδο (αριθμός πυλών κρυπτογράφησης)

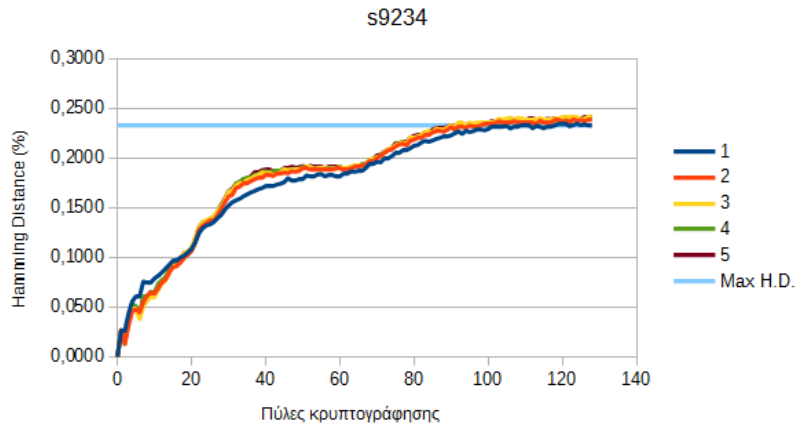
	Βασική μέθοδος	Ομαδοποίηση 2 πυλών	Ομαδοποίηση 3 πυλών	Ομαδοποίηση 4 πυλών	Ομαδοποίηση 5 πυλών
Μ.Ο.	53,3	34,6	31,1	29,8	29,2
ΜΕΓ.	68	42	38	40	39
ΜΙΚ.	46	29	24	24	22



Σχήμα 6.5: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του c7552 σύμφωνα με τη δεύτερη εναλλακτική μέθοδο



Σχήμα 6.6: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του s5378 σύμφωνα με τη δεύτερη εναλλακτική μέθοδο



Σχήμα 6.7: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του s9234 σύμφωνα με τη δεύτερη εναλλακτική μέθοδο

6.2 Σχολιασμός των αποτελεσμάτων

Καταρχήν, σε σχέση με τη πρώτη εναλλακτική μέθοδο, υπάρχει σαφής βελτίωση των αποτελεσμάτων. Σε τρία κυκλώματα επιτυγχάνεται Hamming Distance ίσο ή μεγαλύτερο από 50%, κάτι το οποίο δεν είχε συμβεί με την πρώτη μέθοδο, ενώ για όλα τα υπό σύγκριση κυκλώματα πήραμε καλύτερα αποτελέσματα ως προς το Hamming Distance. Επίσης, και πάλι για όλα τα κυκλώματα, τα αποτελέσματα της μεθόδου αυτής είναι καλύτερα από αυτά της βασικής μεθόδου. Η σημαντική αυτή βελτίωση οφείλεται στην αυξημένη πιθανότητα ενεργοποίησης των περισσότερων εκ των πυλών κρυπτογράφησης (όλων, πλην των πρώτων κάθε ομάδας).

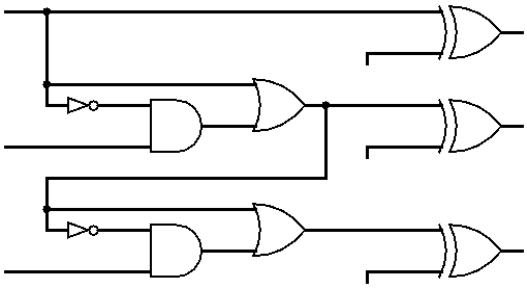
Όπως αναμενόταν, όσο πιο πολλές πύλες κρυπτογράφησης έχουμε σε μία ομάδα και άρα όσο λιγότερες ομάδες, τόσο λιγότερες είναι και οι πύλες που έχουν χαμηλό ποσοστό ενεργοποίησης (= 1/2). Συνεπώς, τα αποτελέσματα είναι καλύτερα όσο αυξάνεται ο βαθμός ομαδοποίησης των πυλών. Τα θετικά αποτελέσματα της συγκεκριμένης εναλλακτικής μας δείχνουν ότι αν καταφέρουμε να αυξήσουμε περαιτέρω τα ποσοστά ενεργοποίησης των πυλών κρυπτογράφησης, θα επιτύχουμε ακόμα καλύτερα αποτελέσματα είτε ως προς το πλήθος των πυλών που απαιτούνται για να επιτευχθεί Hamming Distance ίσο με 50%, είτε ως προς την τιμή αυτού, όταν είναι μικρότερη του 50%.

7 Τρίτη εναλλακτική μέθοδος

Με τη δεύτερη εναλλακτική μέθοδο καταφέραμε να επιτύχουμε μεγαλύτερο Hamming Distance στα κρυπτογραφημένα κυκλώματα σε σχέση με τη βασική μέθοδο. Ο λόγος ήταν ότι στις ομαδοποιήσεις των πυλών κρυπτογράφησης, κάποιες πύλες επηρεάζονταν και από μία δεύτερη είσοδο κλειδιού, όταν αυτή ήταν εσφαλμένη. Η πρώτη πύλη κρυπτογράφησης μίας ομάδας είχε πιθανότητα ίση με 1/2 να αλλάξει την τιμή του κυκλώματος στο σημείο τοποθέτησής της (θεωρώντας ότι όλες οι είσοδοι κλειδιού μπορούν να πάρουν τιμή 0 ή 1 με την ίδια πιθανότητα), ενώ οι υπόλοιπες πύλες της ομάδας είχαν πιθανότητα ίση με 3/4, γεγονός το οποίο είχε ως επακόλουθο την αύξηση του Hamming Distance. Σκοπός στην τρίτη εναλλακτική μέθοδο είναι να αυξήσουμε την πιθανότητα αντιστροφής στις πύλες που ανήκουν σε μία ομάδα.

Ένας τρόπος για να γίνει αυτό είναι να χρησιμοποιήσουμε και πάλι πολυπλέκτες, όπως και στη δεύτερη εναλλακτική μέθοδο, με τη συνδεσμολογία τους όμως τροποποιημένη ως εξής: η πρώτη είσοδος κλειδιού δεν θα συνδέεται με όλους τους πολυπλέκτες μίας ομάδας, αλλά η έξοδος κάθε πολυπλέκτη θα οδηγεί τον επόμενο πολυπλέκτη. Έτσι η κάθε πύλη κρυπτογράφησης, πέρα από τη δική της είσοδο κλειδιού, δεν θα επηρεάζεται μόνο από την πρώτη είσοδο κλειδιού κάθε ομάδας, (όπως συνέβαινε στην δεύτερη εναλλακτική μέθοδο), αλλά και από όλες τις προηγούμενες εισόδους της ομάδας. Έτσι θα έχουμε πύλες κρυπτογράφησης με μεγαλύτερη πιθανότητα αντιστροφής της τιμής του κυκλώματος στο σημείο τοποθέτησης τους.

Στο Σχήμα 7.1 παρουσιάζεται μία ομάδα με τρεις πύλες κρυπτογράφησης, στις οποίες εφαρμόζουμε την τρίτη εναλλακτική μέθοδο (στους πολυπλέκτες έχουν γίνει οι σχετικές απλοποιήσεις, όπως και στη δεύτερη εναλλακτική μέθοδο). Η συνδεσμολογία της πρώτης και της δεύτερης πύλης κρυπτογράφησης είναι η ίδια με αυτή της δεύτερης εναλλακτικής μεθόδου. Ο πολυπλέκτης της τρίτης πύλης κρυπτογράφησης όμως δεν συνδέεται με την είσοδο κλειδιού της πρώτης πύλης, αλλά με την έξοδο του δεύτερου πολυπλέκτη.



Σχήμα 7.1: Συνδεσμολογία των πυλών κρυπτογράφησης της τρίτης εναλλακτικής μεθόδου με ομαδοποίηση τριών πυλών ανά είσοδο κλειδιού

Η πιθανότητα αντιστροφής της τιμής του κυκλώματος στην πρώτη πύλη κρυπτογράφησης μίας ομάδας είναι 1/2 και στη δεύτερη 3/4, όπως ακριβώς συνέβαινε και στη δεύτερη εναλλακτική μέθοδο. Στην τρίτη πύλη όμως το ποσοστό αυτό αυξάνεται, επειδή, για να αντιστρέψει την τιμή του κυκλώματος η πύλη αυτή, αρκεί να υπάρχει εσφαλμένη τιμή σε μία μόνο από τις εισόδους κλειδιού που αντιστοιχούν στην πρώτη, στη δεύτερη ή στην τρίτη πύλη κρυπτογράφησης (σε κάποια δηλαδή από τις εισόδους που συνδέονται μεταξύ τους, μέσω των πολυπλεκτών, μέχρι τη

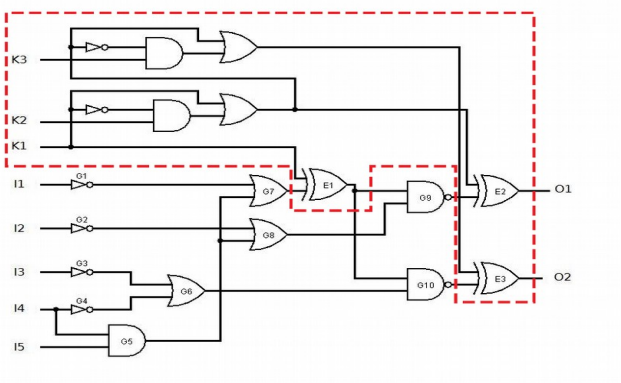
συγκεκριμένη πύλη). Παρακάτω παρουσιάζονται οι συνδυασμοί των εισόδων κλειδιού που αντιστοιχούν στην πρώτη (Α), δεύτερη (Β) και τρίτη (Γ) πύλη κρυπτογράφησης μίας ομάδας.

Πίνακας 7.1: Συνδυασμοί εισόδων κλειδιού για μία ομάδα με τρεις πύλες κρυπτογράφησης

Είσοδος κλειδιού της Α	Είσοδος κλειδιού της Β	Είσοδος κλειδιού της Γ	Ενεργοποίηση της πύλης Γ
0	0	0	Όχι
0	0	1	Ναι
0	1	0	Ναι
0	1	1	Ναι
1	0	0	Ναι
1	0	1	Ναι
1	1	0	Ναι
1	1	1	Ναι

Παρατηρούμε ότι η πιθανότητα αντιστροφής της τιμής του κυκλώματος από την τρίτη πύλη κρυπτογράφησης είναι 7/8 και ισούται με τον λόγο του πλήθους των εσφαλμένων συνδυασμών των τριών εισόδων κλειδιού προς το σύνολο των συνδυασμών αυτών. Επειδή το πλήθος των διαφορετικών συνδυασμών n εισόδων κλειδιού είναι 2^n και από αυτούς μόνο ένας είναι σωστός, γενικά, για την πύλη n μίας ομαδοποίησης ισχύει ότι η πιθανότητα ενεργοποίησης της και συνεπώς αντιστροφής της τιμής του κυκλώματος στο σημείο τοποθέτησής της ισούται με $(2^n-1)/2^n$. Έτσι η τέταρτη πύλη μίας ομαδοποίησης έχει πιθανότητα ενεργοποίησης $(2^4-1)/2^4 = 15/16$, ενώ για την πέμπτη πύλη η πιθανότητα αυτή είναι $(2^5-1)/2^5 = 31/32$. Οι πιθανότητες 7/8, 15/16 και 31/32 είναι πολύ μεγαλύτερες από το 3/4 (ή από το 1/2 της βασικής μεθόδου), πράγμα που σημαίνει ότι αυξάνεται σημαντικά η συχνότητα ενεργοποίησης των πυλών κρυπτογράφησης, παρουσία ενός εσφαλμένου κλειδιού. Με απλά λόγια, ενώ στη βασική μέθοδο μία πύλη κρυπτογράφησης επηρεάζεται μόνο από την εσφαλμένη τιμή της αντίστοιχης εισόδου κλειδιού, στην δεύτερη και τρίτη εναλλάκτη που εξετάστηκαν, μία τέτοια πύλη επηρεάζεται και από επιπλέον εισόδους (μία στη δεύτερη εναλλακτική και μία ή περισσότερες στην τρίτη).

Ένα παράδειγμα για το πως εφαρμόζεται η τρίτη εναλλακτική μέθοδος στο κύκλωμα αναφορας c17 παρουσιάζεται στο Σχήμα 7.2. Η συνδεσμολογία είναι παρόμοια με τη συνδεσμολογία της δεύτερης εναλλακτικής μεθόδου με τη διαφορά ότι στον πολυπλέκτη που οδηγεί την πύλη E3 δεν συνδέεται η είσοδος K1 αλλά η έξοδος του πολυπλέκτη της πύλης E2. Αυτό έχει ως επακόλουθο, η αντιστροφή της τιμής της G10 από την E3 να πραγματοποιείται όταν οποιαδήποτε από τις εισόδους κλειδιού K1, K2 και K3 λάβει την τιμή 1, ενώ μόνο όταν και οι τρεις έχουν την τιμή 0 (σωστό κλειδί) δεν ενεργοποιείται η πύλη E3.



Σχήμα 7.2: Εφαρμογή της τρίτης εναλλακτικής μεθόδου στο κύκλωμα c17

Για τη συγκεκριμένη μέθοδο θα εξετάσουμε τρεις παραλλαγές. Στην πρώτη παραλλαγή οι πύλες κρυπτογράφησης θα ομαδοποιούνται ανά τρεις (όπως και στο Σχήμα 7.1), στη δεύτερη παραλλαγή θα ομαδοποιούνται ανά τέσσερις ενώ στην τρίτη παραλλαγή θα ομαδοποιούνται ανά πέντε. Για την εναλλακτική του κεφαλαίου αυτού δεν θα εξετάσουμε την παραλλαγή με ομαδοποίηση δύο πυλών κρυπτογράφησης, καθώς είναι η ίδια με τη δεύτερη παραλλαγή της δεύτερης εναλλακτικής μεθόδου.

7.1 Αποτελέσματα

Η παραπάνω μέθοδος δοκιμάστηκε, όπως και οι προηγούμενες, στα κυκλώματα αναφοράς c880, c7552, s1196, s1238, s5378 και s9234. Στα c880, s1196 και s1238 επιτύχαμε Hamming Distance ίσο με 50% με λιγότερες από 128 πύλες. Για τα κυκλώματα αυτά θα παρουσιάσουμε πίνακες με το πλήθος των πυλών που χρειαστήκαμε για να φτάσουμε στην επιθυμητή τιμή του Hamming Distance. Ο τρόπος εμφάνισης των πινάκων είναι ίδιος με αυτόν του Κεφαλαίου 6. Στα υπόλοιπα κυκλώματα που δεν επετεύχθη Hamming Distance ίσο με 50%, φτιάξαμε διαγράμματα αντίστοιχα με αυτά των προηγούμενων κεφαλαίων (για τις διάφορες καμπύλες χρησιμοποιήθηκαν ακριβώς τα ίδια χρώματα με τα Κεφάλαια 5 και 6).

Πίνακας 7.2: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του c880 σύμφωνα με την τρίτη εναλλακτική μέθοδο (αριθμός πυλών κρυπτογράφησης)

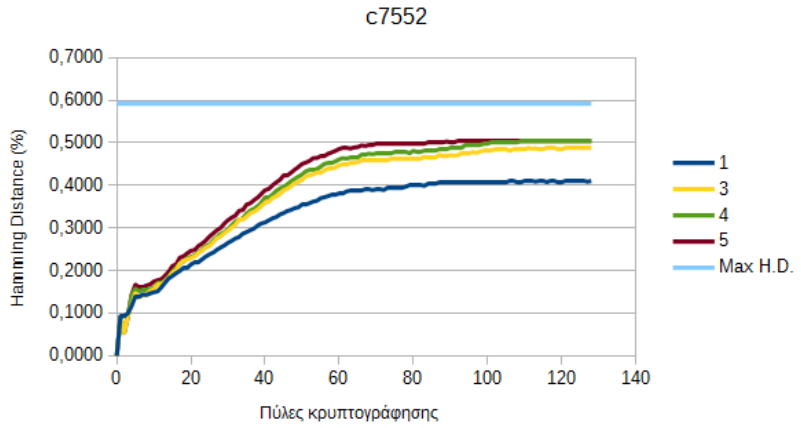
	Βασική μέθοδος	Ομαδοποίηση 3 πυλών	Ομαδοποίηση 4 πυλών	Ομαδοποίηση 5 πυλών
Μ.Ο.	48,7	34,0	30,2	26,3
ΜΕΓ.	52	39	37	35
ΜΙΚ.	46	27	24	22

Πίνακας 7.3: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του s1196 σύμφωνα με την τρίτη εναλλακτική μέθοδο (αριθμός πυλών κρυπτογράφησης)

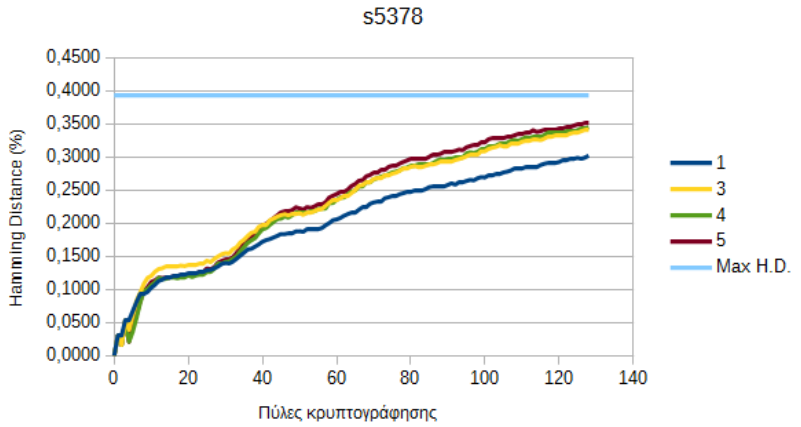
	Βασική μέθοδος	Ομαδοποίηση 3 πυλών	Ομαδοποίηση 4 πυλών	Ομαδοποίηση 5 πυλών
Μ.Ο.	53,0	30,7	28,3	26,6
ΜΕΓ.	76	39	36	32
ΜΙΚ.	46	27	24	23

Πίνακας 7.4: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του s1238 σύμφωνα με την τρίτη εναλλακτική μέθοδο (αριθμός πυλών κρυπτογράφησης)

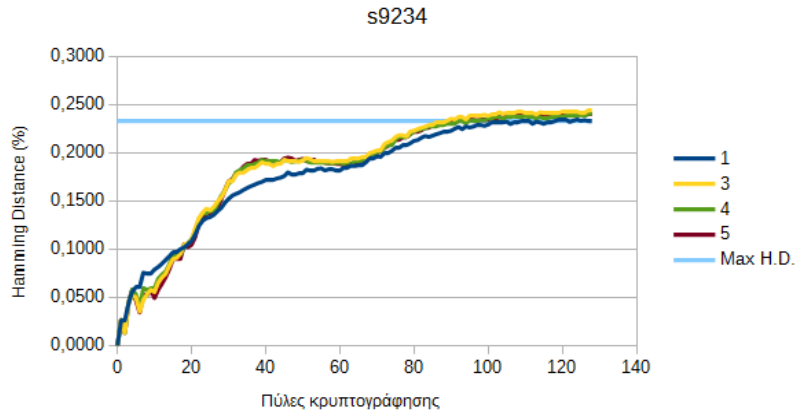
	Βασική μέθοδος	Ομαδοποίηση 3 πυλών	Ομαδοποίηση 4 πυλών	Ομαδοποίηση 5 πυλών
Μ.Ο.	53,3	27,2	25,2	23,9
ΜΕΓ.	68	35	31	29
ΜΙΚ.	46	21	19	19



Σχήμα 7.3: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του c7552 σύμφωνα με την τρίτη εναλλακτική μέθοδο



Σχήμα 7.4: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του s5378 σύμφωνα με την τρίτη εναλλακτική μέθοδο



Σχήμα 7.5: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του s9234 σύμφωνα με την τρίτη εναλλακτική μέθοδο

7.2 Σχολιασμός των αποτελεσμάτων

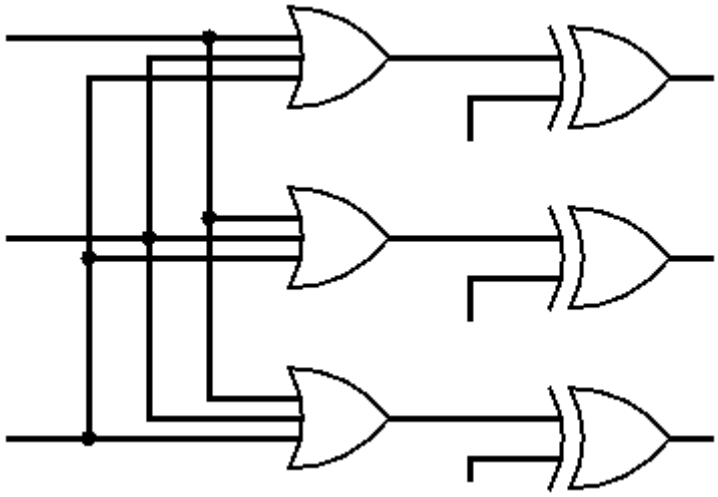
Όπως μπορούμε να παρατηρήσουμε, στα κυκλώματα αναφοράς c880, s1196 και s1238, καταφέραμε να επιτύχουμε Hamming Distance ίσο με 50%, με λιγότερες πύλες σε σχέση με την προηγούμενη μέθοδο, ενώ στα κυκλώματα c7552, s5378 και s9234, για τα οποία δεν επετεύχθη το αποτέλεσμα αυτό με εισαγωγή 128 πυλών κρυπτογράφησης, καταφέραμε να αυξήσουμε τις τιμές του Hamming Distance συγκριτικά με τη δεύτερη εναλλακτική. Αυτό συνέβη γιατί στις διάφορες ομαδοποιήσεις που εξετάσαμε, υπήρχαν πύλες κρυπτογράφησης με μεγαλύτερη πιθανότητα αντιστροφής της τιμής του κυκλώματος στο σημείο τοποθέτησής τους, σε σχέση με τη δεύτερη εναλλακτική μέθοδο.

Από τα αποτελέσματα παρατηρούμε ότι, όσο αυξάνουμε το μέγεθος των ομάδων, τόσο βελτιώνονται τα αποτελέσματα που παίρνουμε. Αυτό είναι λογικό, καθώς με μεγαλύτερες ομάδες έχουμε πύλες κρυπτογράφησης με αυξημένη πιθανότητα αντιστροφής της τιμής του κυκλώματος στο σημείο τοποθέτησής τους. Το πρόβλημα της συγκεκριμένης εναλλακτικής είναι ότι δεν μπορούμε να ομαδοποιήσουμε μεγάλο αριθμό πυλών, γιατί κάτι τέτοιο θα δημιουργούσε μονοπάτια μεγάλης καθυστέρησης μέσα στο κύκλωμα, γεγονός που πιθανώς θα οδηγούσε σε μείωση της συχνότητας ρολογιού του συνολικού ακολουθιακού κυκλώματος, στο οποίο θα εντάσσονταν το κρυπτογραφημένο συνδυαστικό. Θα πρέπει λοιπόν να βρούμε και άλλους τρόπους αύξησης της πιθανότητας ενεργοποίησης των πυλών κρυπτογράφησης, οι οποίοι θα επιβαρύνουν σε μικρότερο βαθμό την καθυστέρηση του υπό κρυπτογράφηση κυκλώματος.

8 Τέταρτη εναλλακτική μέθοδος (τελική προτεινόμενη)

Στην τρίτη εναλλακτική μέθοδο, χρησιμοποιώντας πολυπλέκτες όπως και στη δεύτερη εναλλακτική, καταφέραμε, για τις περισσότερες πύλες κρυπτογράφησης (αν και όχι για όλες), να αυξήσουμε την πιθανότητα αντιστροφής της τιμής του κυκλώματος, στο σημείο τοποθέτησης τους. Αυτό είχε ως επακόλουθο να αυξηθεί το Hamming Distance στα κρυπτογραφημένα κυκλώματα ή να μειωθεί το πλήθος των πυλών κρυπτογράφησης όταν σε ένα κύκλωμα επιτυγχάνονται 50% Hamming Distance. Σκοπός της τέταρτης (και τελευταίας) εναλλακτικής μεθόδου είναι να αυξήσουμε την πιθανότητα αυτή σε όλες τις πύλες κρυπτογράφησης και όχι σε μερικές όπως στην τρίτη εναλλακτική μέθοδο, καθώς επίσης και να μειώσουμε την επιβάρυνση σε καθυστέρηση που η μέθοδος αυτή επιβάλει.

Τους στόχους αυτούς μπορούμε να τους πετύχουμε αν συνδέσουμε άμεσα τις πύλες κρυπτογράφησης, με περισσότερες από μία εισόδους κλειδιού του κυκλώματος. Κάθε μία πύλη κρυπτογράφησης θα ενεργοποιείται από τον συνδυασμό δυο, τριών, τεσσάρων ή πέντε διαφορετικών εισόδων κλειδιού. Η τιμή των εισόδων αυτών θα αποκωδικοποιείται με τη βοήθεια μίας επιπλέον πύλης, η έξοδος της οποίας θα συνδέεται με την πύλη κρυπτογράφησης. Στην περίπτωση που εξετάζουμε, όπου όλες οι πύλες κρυπτογράφησης είναι XOR και η σωστή τιμή όλων των bit κλειδιού είναι 0, η απαιτούμενη αποκωδικοποίηση μπορεί να πραγματοποιηθεί με τη βοήθεια πυλών OR. Ένα λάθος bit κλειδιού (με τιμή 1) προκαλεί ενεργοποίηση της πύλης κρυπτογράφησης, αφού η έξοδος της OR ισούται με 1, ενώ μόνο όταν όλα τα bit κλειδιού έχουν τη σωστή τιμή (0), η έξοδος της OR είναι τέτοια (0) που να μην προκαλεί την ενεργοποίηση της πύλης κρυπτογράφησης. Στο Σχήμα 8.1 παρουσιάζονται τρεις πύλες κρυπτογράφησης, οι οποίες ελέγχονται από τρεις διαφορετικές εισόδους κλειδιού η κάθε μία.

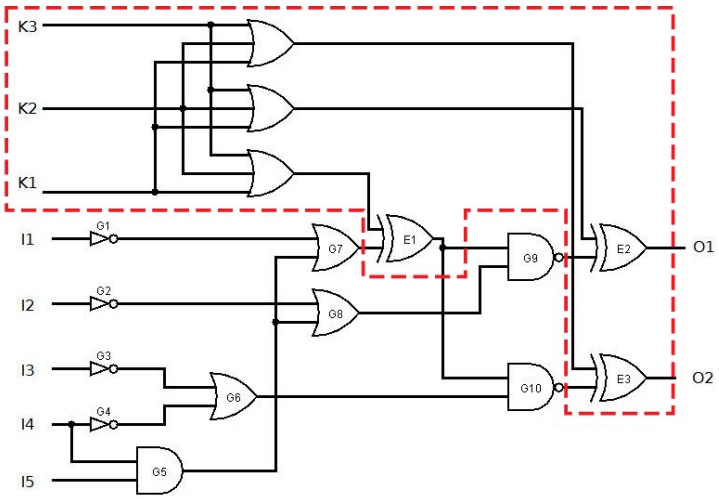


Σχήμα 8.1: Συνδεσμολογία των πυλών κρυπτογράφησης σύμφωνα με την τέταρτη εναλλακτική μέθοδο, με την κάθε πύλη να ελέγχεται από τρεις διαφορετικές εισόδους κλειδιού

Η τέταρτη εναλλακτική μέθοδος προσφέρει τη μέγιστη πιθανότητα αντιστροφής της τρίτης εναλλακτικής σε όλες τις πύλες κρυπτογράφησης, με σαφώς μικρότερη καθυστέρηση (ένα ή

δύο, το πολύ, επίπεδα πυλών πριν την πύλη κρυπτογράφησης). Έτσι, εάν μία πύλη κρυπτογράφησης ελέγχεται από δύο εισόδους κλειδιού (μέσω της σχετικής πύλης OR), η πιθανότητα αντιστροφής της τιμής του κυκλώματος στο σημείο που έχει τοποθετηθεί είναι 3/4, ενώ αν ελέγχεται από τρεις, τέσσερις ή πέντε εισόδους κλειδιού, η πιθανότητα αυτή ανεβαίνει στα 7/8, 15/16 και 31/32 αντίστοιχα. Αυτές ακριβώς είναι και οι παραλλαγές τις συγκεκριμένης μεθόδου που εξετάσαμε μέσω πειραμάτων.

Στο Σχήμα 8.2 παρουσιάζεται ένα παράδειγμα εφαρμογής της τέταρτης εναλλακτικής μεθόδου στο κύκλωμα αναφοράς c17, θεωρώντας ότι κάθε πύλη κρυπτογράφησης ελέγχεται από τρεις εισόδους κλειδιού. Όλες οι πύλες κρυπτογράφησης (E1, E2 και E3) ελέγχονται και από τις τρεις εισόδους κλειδιού του κυκλώματος (K1, K2 και K3). Για να αντιστρέψουν οι πύλες την τιμή του κυκλώματος στα αντίστοιχα σημεία, αρκεί τουλάχιστον μία είσοδος από τις K1, K2, K3 να έχει τη λάθος τιμή (1), ενώ για να μην πραγματοποιηθούν αντιστροφές και το κύκλωμα να συνεχίσει να λειτουργεί κανονικά, θα πρέπει σε όλες τις εισόδους κλειδιού να τεθεί η σωστή τιμή (0).



Σχήμα 8.2: Εφαρμογή της τέταρτης εναλλακτικής μεθόδου στο κύκλωμα c17

8.1 Αποτελέσματα

Αφού η τέταρτη εναλλακτική μέθοδος αποτελεί και την τελική προτεινόμενη μέθοδο της παρούσας διπλωματικής εργασίας, την εφαρμόσαμε σε δεκατέσσερα κυκλώματα αναφοράς. Αυτά ήταν τα c432, c499, c880, c1355, c1908, c3540, c5315, c7552, s1196, s1238, s5378, s9234, s13207 και s15850. Στα c432, c499, c880, c1355, c1908, c3540, c7552, s1196 και s1238 καταφέραμε να επιτύχουμε Hamming Distance ίσο με 50% με λιγότερες από 128 πύλες. Για τα κυκλώματα αυτά παρουσιάζουμε τα αποτελέσματα σε πίνακες, οι οποίοι έχουν ακριβώς την ίδια μορφή με αυτούς των δύο προηγούμενων κεφαλαίων. Για τα υπόλοιπα κυκλώματα που το Hamming Distance δεν έφτασε στο 50%, παρουσιάζουμε τα αποτελέσματα σε διαγράμματα (ένα για κάθε ένα κύκλωμα). Τα χρώματα των καμπυλών είναι ακριβώς τα ίδια με αυτά των προηγούμενων κεφαλαίων, με τη διαφορά ότι στην μέθοδο αυτή, ο βαθμός ομαδοποίησης (2, 3, 4 ή 5) αναφέρεται στο πλήθος των διαφορετικών εισόδων κλειδιού που ελέγχουν μία πύλη κρυπτογράφησης. Επιπλέον, για το s9234 πραγματοποιήσαμε και μία εξομοίωση επιτρέποντας την εισαγωγή 1.024 πυλών κρυπτογράφησης στο κύκλωμα. Ο λόγος που μας οδήγησε στην δοκιμή αυτή είναι ότι θέλαμε να παρατηρήσουμε εάν η τιμή του Hamming Distance, μετά την εισαγωγή ενός μεγάλου αριθμού πυλών κρυπτογράφησης σταθεροποιείται ή συνεχίζει να αυξάνει.

Πίνακας 8.1: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του c432 σύμφωνα με την τέταρτη εναλλακτική μέθοδο (αριθμός πυλών κρυπτογράφησης)

	Βασική μέθοδος	2 είσοδοι κλειδιού / πύλη κρυπτ.	3 είσοδοι κλειδιού / πύλη κρυπτ.	4 είσοδοι κλειδιού / πύλη κρυπτ.	5 είσοδοι κλειδιού / πύλη κρυπτ.
Μ.Ο.	8,6	5,5	5,5	6,5	7,7
ΜΕΓ.	9	8	6	7	8
ΜΙΚ.	6	3	4	5	6

Πίνακας 8.2: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του c499 σύμφωνα με την τέταρτη εναλλακτική μέθοδο (αριθμός πυλών κρυπτογράφησης)

	Βασική μέθοδος	2 είσοδοι κλειδιού / πύλη κρυπτ.	3 είσοδοι κλειδιού / πύλη κρυπτ.	4 είσοδοι κλειδιού / πύλη κρυπτ.	5 είσοδοι κλειδιού / πύλη κρυπτ.
Μ.Ο.	43,2	19,1	15,4	14,5	13,9
ΜΕΓ.	52	22	18	18	17
ΜΙΚ.	37	17	14	13	13

Πίνακας 8.3: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του c880 σύμφωνα με την τέταρτη εναλλακτική μέθοδο (αριθμός πυλών κρυπτογράφησης)

	Βασική μέθοδος	2 είσοδοι κλειδιού / πύλη κρυπτ.	3 είσοδοι κλειδιού / πύλη κρυπτ.	4 είσοδοι κλειδιού / πύλη κρυπτ.	5 είσοδοι κλειδιού / πύλη κρυπτ.
Μ.Ο.	48,7	28,7	22,1	20,4	20,0
ΜΕΓ.	52	32	25	23	22
ΜΙΚ.	46	26	19	17	17

Πίνακας 8.4: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του c1355 σύμφωνα με την τέταρτη εναλλακτική μέθοδο (αριθμός πυλών κρυπτογράφησης)

	Βασική μέθοδος	2 είσοδοι κλειδιού / πύλη κρυπτ.	3 είσοδοι κλειδιού / πύλη κρυπτ.	4 είσοδοι κλειδιού / πύλη κρυπτ.	5 είσοδοι κλειδιού / πύλη κρυπτ.
Μ.Ο.	42,1	19,4	15,6	14,8	14,1
ΜΕΓ.	52	21	18	17	16
ΜΙΚ.	36	17	14	13	13

Πίνακας 8.5: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του c1908 σύμφωνα με την τέταρτη εναλλακτική μέθοδο (αριθμός πυλών κρυπτογράφησης)

	Βασική μέθοδος	2 είσοδοι κλειδιού / πύλη κρυπτ.	3 είσοδοι κλειδιού / πύλη κρυπτ.	4 είσοδοι κλειδιού / πύλη κρυπτ.	5 είσοδοι κλειδιού / πύλη κρυπτ.
Μ.Ο.	29,6	14,4	12,1	11,2	10,9
ΜΕΓ.	47	16	14	13	13
ΜΙΚ.	20	12	10	9	9

Πίνακας 8.6: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του c3540 σύμφωνα με την τέταρτη εναλλακτική μέθοδο (αριθμός πυλών κρυπτογράφησης)

	Βασική μέθοδος	2 είσοδοι κλειδιού / πύλη κρυπτ.	3 είσοδοι κλειδιού / πύλη κρυπτ.	4 είσοδοι κλειδιού / πύλη κρυπτ.	5 είσοδοι κλειδιού / πύλη κρυπτ.
Μ.Ο.	108,8	86,6	80,5	76,2	68,1
ΜΕΓ.	121	99	89	89	87
ΜΙΚ.	83	81	73	40	20

Πίνακας 8.7: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του c7552 σύμφωνα με την τέταρτη εναλλακτική μέθοδο (αριθμός πυλών κρυπτογράφησης)

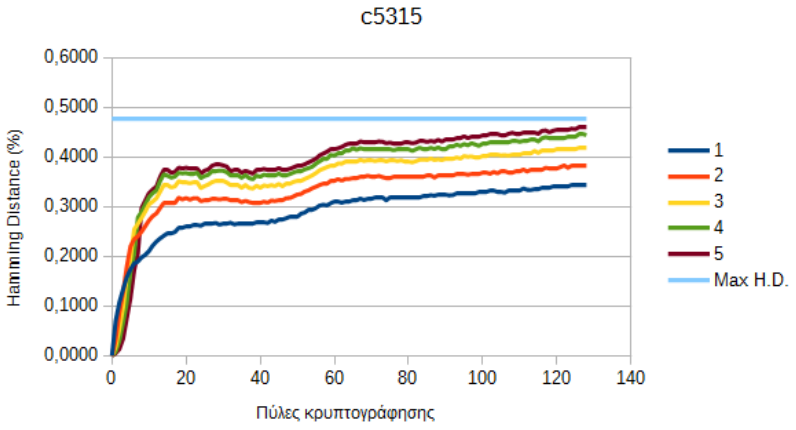
	Βασική μέθοδος	2 είσοδοι κλειδιού / πύλη κρυπτ.	3 είσοδοι κλειδιού / πύλη κρυπτ.	4 είσοδοι κλειδιού / πύλη κρυπτ.	5 είσοδοι κλειδιού / πύλη κρυπτ.
Μ.Ο.	-	93,8	59,4	54,5	52,9
ΜΕΓ.	-	109	63	60	57
ΜΙΚ.	-	80	54	49	48

Πίνακας 8.8: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του s1196 σύμφωνα με την τέταρτη εναλλακτική μέθοδο (αριθμός πυλών κρυπτογράφησης)

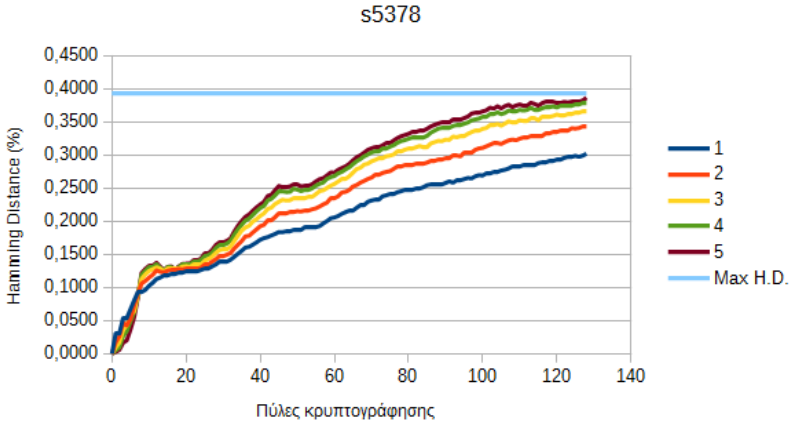
	Βασική μέθοδος	2 είσοδοι κλειδιού / πύλη κρυπτ.	3 είσοδοι κλειδιού / πύλη κρυπτ.	4 είσοδοι κλειδιού / πύλη κρυπτ.	5 είσοδοι κλειδιού / πύλη κρυπτ.
Μ.Ο.	53,0	26,3	22,6	21,6	20,9
ΜΕΓ.	76	29	26	26	26
ΜΙΚ.	46	23	18	17	17

Πίνακας 8.9: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του s1238 σύμφωνα με την τέταρτη εναλλακτική μέθοδο (αριθμός πυλών κρυπτογράφησης)

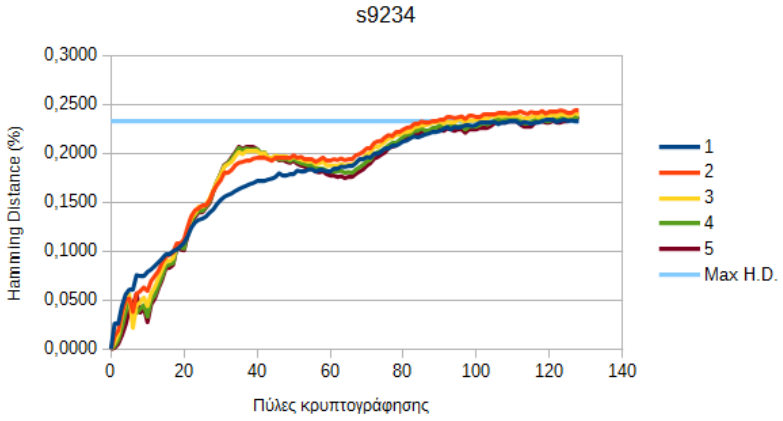
	Βασική μέθοδος	2 είσοδοι κλειδιού / πύλη κρυπτ.	3 είσοδοι κλειδιού / πύλη κρυπτ.	4 είσοδοι κλειδιού / πύλη κρυπτ.	5 είσοδοι κλειδιού / πύλη κρυπτ.
Μ.Ο.	53,3	24,7	20,2	18,9	18,3
ΜΕΓ.	68	30	29	24	20
ΜΙΚ.	46	21	17	17	17



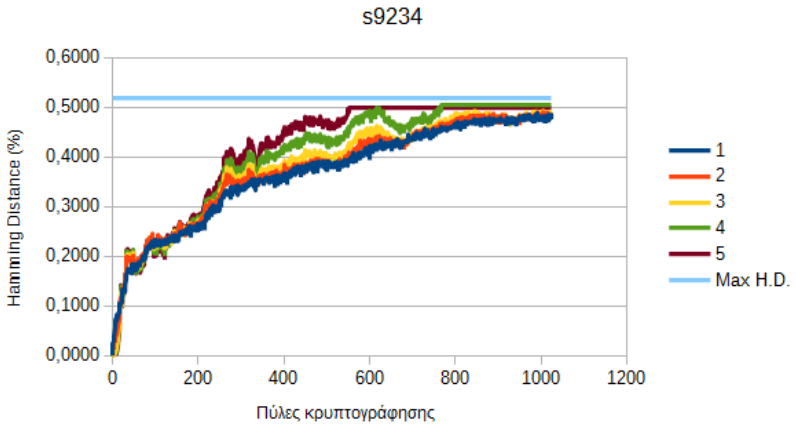
Σχήμα 8.3: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του c5315 σύμφωνα με την τέταρτη εναλλακτική μέθοδο



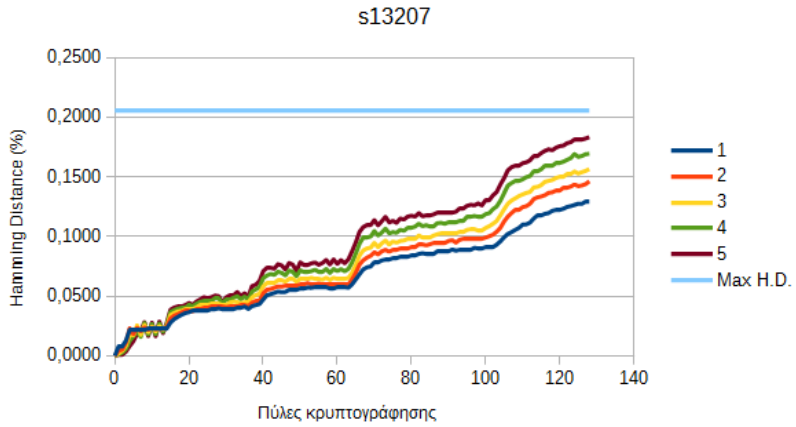
Σχήμα 8.4: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του s5378 σύμφωνα με την τέταρτη εναλλακτική μέθοδο



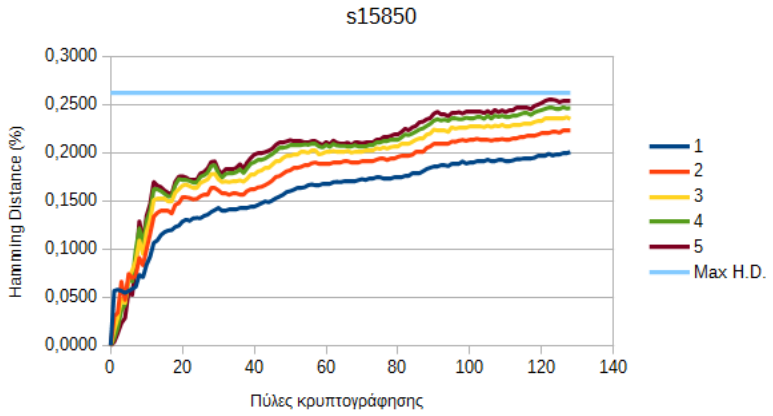
Σχήμα 8.5: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του s9234 σύμφωνα με την τέταρτη εναλλακτική μέθοδο (με 128 πύλες κρυπτογράφησης)



Σχήμα 8.6: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του s9234 σύμφωνα με την τέταρτη εναλλακτική μέθοδο (με 1.024 πύλες κρυπτογράφησης)



Σχήμα 8.7: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του s13207 σύμφωνα με την τέταρτη εναλλακτική μέθοδο



Σχήμα 8.8: Αποτελέσματα εξομοιώσεων για την κρυπτογράφηση του s15850 σύμφωνα με την τέταρτη εναλλακτική μέθοδο

8.2 Σχολιασμός των αποτελεσμάτων

Όπως παρατηρούμε, στα κυκλώματα c432, c499, c880, c1355, c1908, c3540, c7552, s1196 και s1238 καταφέραμε να επιτύχουμε Hamming Distance ίσο με 50%, με λιγότερες από 128 πύλες. Στα c880, c7552, s1196 και s1238, τα οποία χρησιμοποιήθηκαν, μαζί με τα s5378 και s9234, για σύγκριση των διάφορων μεθόδων, ο αριθμός των πυλών ήταν μικρότερος από τις προηγούμενες εναλλακτικές. Στα κυκλώματα c5315, s5378, s9234, s13207 και s15850 δεν καταφέραμε να πετύχουμε Hamming Distance ίσο με 50% με χρήση 128 πυλών κρυπτογράφησης (για το s9234, αυτό έγινε εφικτό με 767 και 551 πύλες, για τις περιπτώσεις ελέγχου μίας πύλης κρυπτογράφησης από 4 και 5 εισόδους κλειδιού αντίστοιχα), αλλά καταφέραμε να αυξήσουμε την τιμή του σε σχέση με τις υπόλοιπες μεθόδους, ενώ στα περισσότερα κυκλώματα πλησιάσαμε κοντά στην τιμή του μέγιστου Hamming Distance. Αυτό συνέβη γιατί όλες οι πύλες κρυπτογράφησης είχαν τη μέγιστη δυνατή πιθανότητα να αντιστρέψουν την τιμή του κυκλώματος στο σημείο που τοποθετούνταν, σύμφωνα πάντα με το πλήθος των εισόδων κλειδιού που χρησιμοποιήθηκαν για τον έλεγχο τους.

9 Συμπεράσματα

Σκοπός της παρούσας διπλωματικής εργασίας ήταν η μελέτη της βασικής μεθόδου κρυπτογράφησης ψηφιακών κυκλωμάτων που παρουσιάστηκε στις εργασίες [2], [3] και η ανάπτυξη νέων μεθόδων κρυπτογράφησης με καλύτερη απόδοση. Όπως εξηγήσαμε, καλύτερη απόδοση σημαίνει επίτευξη απόστασης Hamming ίσης με 50% με λιγότερες πύλες κρυπτογράφησης από τη βασική μέθοδο ή επίτευξη μεγαλύτερης απόστασης Hamming, όταν η τιμή της τελευταίας είναι μικρότερη του 50%, με τον ίδιο αριθμό πυλών με τη βασική μέθοδο. Σε όλες τις εναλλακτικές μεθόδους που προτείναμε δεν εξετάσαμε τον τρόπο επιλογής του σημείου τοποθέτησης των πυλών κρυπτογράφησης, αλλά διαφοροποιήσαμε τον τρόπο ελέγχου τους, ομαδοποιώντας τις πύλες ως προς μία ή περισσότερες εισόδους κλειδιού που μπορούν να τις ενεργοποιήσουν, ή ομαδοποιώντας τις εισόδους κλειδιού που ελέγχουν μία πύλη. Δοκιμάστηκαν ομαδοποιήσεις δυο, τριών, τεσσάρων και πέντε πυλών καθώς και δυο, τριών, τεσσάρων και πέντε εισόδων κλειδιού ανά πύλη κρυπτογράφησης. Δεν δοκιμάστηκαν μεγαλύτερες ομαδοποιήσεις ώστε να μην δημιουργηθούν μονοπάτια μεγάλης καθυστέρησης στο κύκλωμα.

Στην πρώτη εναλλακτική μέθοδο, σε μία είσοδο κλειδιού συνδέσαμε περισσότερες από μία πύλες κρυπτογράφησης. Τα αποτελέσματα ήταν χειρότερα από τη βασική μέθοδο (υπήρξε μείωση του Hamming Distance). Όσο πιο πολλές πύλες κρυπτογράφησης ομαδοποιούσαμε, τόσο μίκραινε και το ποσοστό του Hamming Distance. Αυτό συνέβαινε γιατί κάθε λάθος bit κλειδιού επηρέαζε περισσότερες από μία πύλες κρυπτογράφησης του κυκλώματος (επιθυμητό), το ίδιο όμως συνέβαινε και για κάθε σωστή είσοδο κλειδιού (μη επιθυμητό). Το συνολικό αποτέλεσμα ήταν ελαφρώς χειρότερο σε σχέση με τη βασική μέθοδο.

Στη δεύτερη εναλλακτική μέθοδο που εξετάσαμε, χρησιμοποιήσαμε πολυπλέκτες 2-σε-1 και τα αποτελέσματα ήταν καλύτερα από τη βασική μέθοδο. Αυτό επετεύχθη γιατί κάποιες από τις εισόδους κλειδιού επηρέαζαν περισσότερες από μία πύλες κρυπτογράφησης μόνο εάν είχαν λάθος τιμή, ενώ, σε αντίθετη περίπτωση οι πύλες αυτές ελέγχονταν από άλλη είσοδο κλειδιού.

Στην τρίτη εναλλακτική μέθοδο, στην οποία χρησιμοποιήσαμε και πάλι πολυπλέκτες 2-σε-1, αλλά με διαφορετική συνδεσμολογία, τα αποτέλεσμα ήταν ακόμη καλύτερα. Αυτό συνέβη γιατί η χρησιμοποιούμενη συνδεσμολογία επέτρεπε, με την αύξηση του βαθμού ομαδοποίησης των πυλών, να αυξάνεται και η πιθανότητα μία πύλη κρυπτογράφησης να αντιστρέφει την τιμή του κυκλώματος, όταν κάποια από τις εισόδους κλειδιού που ελέγχουν τις πύλες της ομάδας είχε λάθος τιμή. Σε αυτή τη μέθοδο δεν εξετάστηκε η περίπτωση ομαδοποίησης δύο πυλών γιατί ήταν ίδια με την αντίστοιχη περίπτωση της δεύτερης μεθόδου.

Στην τέταρτη εναλλακτική μέθοδο χρησιμοποιήσαμε πύλες OR και τα αποτέλεσμα ήταν πολύ καλύτερα από όλες τις άλλες μεθόδους. Σε μερικά κυκλώματα μάλιστα φτάσαμε αρκετά κοντά στη μέγιστη απόσταση Hamming, η οποία θεωρήσαμε ότι προκύπτει όταν όλες οι πύλες κρυπτογράφησης αντιστρέψουν την τιμή του κυκλώματος στο σημείο τοποθέτησής τους. Ο λόγος της συνολικά καλύτερης απόδοσης της τελευταίας εναλλακτικής είναι ότι, λόγω της ομαδοποίησης των εισόδων κλειδιού που ελέγχουν μία πύλη κρυπτογράφησης μέσω των πυλών OR, όλες οι πύλες κρυπτογράφησης είχαν μεγάλο ποσοστό αντιστροφής της τιμής του κυκλώματος.

Στους πίνακες 9.1 – 9.6 παρουσιάζουμε τα συγκριτικά αποτελέσματα των τεσσάρων εναλλακτικών μεθόδων που εξετάσαμε, για τα κυκλώματα αναφοράς c880, c7552, s1196, s1238, s5378 και s9234. Στους πίνακες φαίνεται ο μέσος όρος των αποτελεσμάτων των 20 πειραμάτων που εκτελέσαμε για κάθε βαθμό ομαδοποίησης των προτεινόμενων εναλλακτικών, καθώς και για τη βασική μέθοδο. Σημειώνεται επίσης και η μεγίστη τιμή του Hamming Distance, υπολογισμένη όπως εξηγήθηκε προηγουμένως. Για όσα πειράματα επετεύχθη απόσταση Hamming ίση με 50% καταγράφεται στους πίνακες ο απαιτούμενος αριθμός πυλών κρυπτογράφησης (σαν καθαρός αριθμός), ενώ για όσα πειράματα το Hamming Distance δεν ξεπέρασε το 50% παρουσιάζουμε το σχετικό ποσοστό (σημειώνεται ως "% (HD)").

Πίνακας 9.1: Συγκριτικά αποτελέσματα όλων των μεθόδων κρυπτογράφησης για το κύκλωμα c880

	c880			
	Βαθμός ομαδοποίησης των πυλών κρυπτογράφησης ή των εισόδων κλειδιού που τις ελέγχουν (4η εναλλακτική)			
	2	3	4	5
Βασική μέθοδος	48,7			
Max Hamming Distance	0,5172% (HD)			
Πρώτη εναλλακτική μέθοδος	0,4958% (HD)	0,4960% (HD)	0,4894% (HD)	0,4860% (HD)
Δεύτερη εναλλακτική μέθοδος	38,3	36,3	35,2	34,2
Τρίτη εναλλακτική μέθοδος	-	34,0	30,2	26,3
Τέταρτη εναλλακτική μέθοδος	28,7	22,1	20,4	20,0

Πίνακας 9.2: Συγκριτικά αποτελέσματα όλων των μεθόδων κρυπτογράφησης για το κύκλωμα c7552

	c7552			
	Βαθμός ομαδοποίησης των πυλών κρυπτογράφησης ή των εισόδων κλειδιού που τις ελέγχουν (4η εναλλακτική)			
	2	3	4	5
Βασική μέθοδος	0,4105% (HD)			
Max Hamming Distance	0,5935% (HD)			
Πρώτη εναλλακτική μέθοδος	0,4086% (HD)	0,4079% (HD)	0,4035% (HD)	0,4073% (HD)
Δεύτερη εναλλακτική μέθοδος	0,4510% (HD)	0,4708% (HD)	0,4747% (HD)	0,4903% (HD)
Τρίτη εναλλακτική μέθοδος	-	0,4871% (HD)	96,0	71,1
Τέταρτη εναλλακτική μέθοδος	93,8	59,4	54,5	52,9

Πίνακας 9.3: Συγκριτικά αποτελέσματα όλων των μεθόδων κρυπτογράφησης για το κύκλωμα s1196

	s1196			
	Βαθμός ομαδοποίησης των πυλών κρυπτογράφησης ή των εισόδων κλειδιού που τις ελέγχουν (4η εναλλακτική)			
	2	3	4	5
Βασική μέθοδος	53,0			
Max Hamming Distance	0,5172% (HD)			
Πρώτη εναλλακτική μέθοδος	0,4820% (HD)	0,4753% (HD)	0,4621% (HD)	0,4570% (HD)
Δεύτερη εναλλακτική μέθοδος	36,3	33,3	33,0	31,5
Τρίτη εναλλακτική μέθοδος	-	30,7	28,3	26,6
Τέταρτη εναλλακτική μέθοδος	26,3	22,6	21,6	20,9

Πίνακας 9.4: Συγκριτικά αποτελέσματα όλων των μεθόδων κρυπτογράφησης για το κύκλωμα s1238

	s1238			
	Βαθμός ομαδοποίησης των πυλών κρυπτογράφησης ή των εισόδων κλειδιού που τις ελέγχουν (4η εναλλακτική)			
	2	3	4	5
Βασική μέθοδος	53,3			
Max Hamming Distance	0,5784% (HD)			
Πρώτη εναλλακτική μέθοδος	0,4302% (HD)	0,4108% (HD)	0,3976% (HD)	0,3738% (HD)
Δεύτερη εναλλακτική μέθοδος	34,6	31,1	29,8	29,2
Τρίτη εναλλακτική μέθοδος	-	27,2	25,2	23,9
Τέταρτη εναλλακτική μέθοδος	24,7	20,2	18,9	18,3

Πίνακας 9.5: Συγκριτικά αποτελέσματα όλων των μεθόδων κρυπτογράφησης για το κύκλωμα s5378

	s5378			
	Βαθμός ομαδοποίησης των πυλών κρυπτογράφησης ή των εισόδων κλειδιού που τις ελέγχουν (4η εναλλακτική)			
	2	3	4	5
Βασική μέθοδος	0,3019% (HD)			
Max Hamming Distance	0,3926% (HD)			
Πρώτη εναλλακτική μέθοδος	0,2946% (HD)	0,2977% (HD)	0,2929% (HD)	0,2873% (HD)
Δεύτερη εναλλακτική μέθοδος	0,3219% (HD)	0,3321% (HD)	0,3331% (HD)	0,3358% (HD)
Τρίτη εναλλακτική μέθοδος	-	0,3404% (HD)	0,3450% (HD)	0,3521% (HD)
Τέταρτη εναλλακτική μέθοδος	0,3440% (HD)	0,3666% (HD)	0,3781% (HD)	0,3866% (HD)

Πίνακας 9.6: Συγκριτικά αποτελέσματα όλων των μεθόδων κρυπτογράφησης για το κύκλωμα s9234

	s9234			
	Βαθμός ομαδοποίησης των πυλών κρυπτογράφησης ή των εισόδων κλειδιού που τις ελέγχουν (4η εναλλακτική)			
	2	3	4	5
Βασική μέθοδος	0,2335% (HD)			
Max Hamming Distance	0,2330% (HD)			
Πρώτη εναλλακτική μέθοδος	0,2261% (HD)	0,2246% (HD)	0,2202% (HD)	0,2159% (HD)
Δεύτερη εναλλακτική μέθοδος	0,2387% (HD)	0,2421% (HD)	0,2405% (HD)	0,2417% (HD)
Τρίτη εναλλακτική μέθοδος	-	0,2440% (HD)	0,2403% (HD)	0,2406% (HD)
Τέταρτη εναλλακτική μέθοδος	0,2434% (HD)	0,2393% (HD)	0,2370% (HD)	0,2349% (HD)

Από όλους του πίνακες είναι εμφανής η βελτίωση της απόδοσης της κρυπτογράφησης καθώς βελτιώνουμε τον έλεγχο των πυλών κρυπτογράφησης (από τη πρώτη στην τέταρτη εναλλακτική), αλλά και καθώς αυξάνουμε τον βαθμό ομαδοποίησης των πυλών ή των εισόδων κλειδιού. Μόνο στα αποτελέσματα του s9234 όλες οι μέθοδοι βρίσκονται κοντά στο μέγιστο Hamming Distance, οπότε οι διαφοροποιήσεις στα διανύσματα εισόδου μεταξύ των διαφορετικών πειραμάτων, οδήγησαν σε μικρές αποκλίσεις μεταξύ των συγκρινόμενων μεθόδων και έδωσαν αποτελέσματα ακόμα και ελαφρώς μεγαλύτερα από το μέγιστο Hamming

Distance (υπενθυμίζουμε ότι ο υπολογισμός του είναι πειραματικός, με χρήση τυχαίων διανυσμάτων). Παρόλα αυτά, η τιμή της μέγιστης απόστασης Hamming για κάθε κύκλωμα δείχνει ποια είναι τα όρια των δυνατοτήτων κρυπτογράφησης των μεθόδων που χρησιμοποιούν τα κριτήρια τοποθέτησης πυλών κρυπτογράφησης που προτείνονται από τους συγγραφείς των εργασιών της βασικής μεθόδου. Έτσι, για να πάρουμε ακόμα καλύτερα αποτελέσματα και για να επιτύχουμε το επιθυμητό Hamming Distance για όσα κυκλώματά δεν το κατορθώσαμε, θα πρέπει να εξετάσουμε νέα κριτήρια τοποθέτησης των πυλών κρυπτογράφησης, τα οποία θα οδηγήσουν σε αυξημένα ποσοστά της μέγιστης απόστασης Hamming. Τα κριτήρια αυτά, σε συνδυασμό με τη διαδικασία ελέγχου των πυλών που προτάθηκε στην τέταρτη εναλλακτική μέθοδο θα οδηγήσουν στα επιζητούμενα καλύτερα αποτελέσματα κρυπτογράφησης των ψηφιακών κυκλωμάτων. Η αναζήτηση τέτοιων κριτηρίων θα αποτελέσει ένα από τα αντικείμενα της μελλοντική ερευνητικής μας δραστηριότητας.

10 Βιβλιογραφία

[1] J. Rajendran, O. Sinanoglu, and R. Karri, “Regaining Trust in VLSI Design: Design-for-Trust Techniques”, Proceedings of the IEEE, vol. 102, pp. 1266-1282, Aug. 2014.

[2] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, “Logic Encryption: A Fault Analysis Perspective”, in Proc. of Design Automation and Test in Europe (DATE) Conference, March 2012, pp. 953-958.

[3] J. Rajendran, H. Zhang, C. Zhang, G. S. Rose, Y. Pino, O. Sinanoglu, and R. Karri, “Fault Analysis-based Logic Encryption”, IEEE Transactions on Computers, vol. 64, pp. 410-424, Feb. 2015.

[4] H. K. Lee and D. S. Ha, "HOPE: An Efficient Parallel Fault Simulator for Synchronous Sequential Circuits", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 15, Sept. 1996, pp. 1048-1058.

[5] F. Brglez, P. Pownall and R. Hum, "Accelerated ATPG and Fault Grading via Testability Analysis", in Proc. of IEEE International Symposium on Circuits and Systems (ISCAS), June 1985, pp. 695-698.

[6] F. Brglez, D. Bryan and K. Kozminski, "Combinational Profiles of Sequential Benchmark Circuits", in Proc. of IEEE International Symposium on Circuits and Systems (ISCAS), May 1989, pp. 1929-1934.