ΠΑΝΕΠΙΣΤΗΜΙΟ
ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Θέμα Διπλωματικής Εργασίας

Ανάλυση Απόδοσης Συμμετρικών Αλγορίθμων Κρυπτογραφίας για ενσωματωμένα συστήματα
Performance Analysis of Symmetric Cryptography Algorithms for Embedded Systems

Επιβλέπων: Δρ. Μηνάς Δασυγένης (mdasyg **(at)** ieee .org**) -http://arch.icte.uowm.gr**

Αναπόσπαστο κομμάτι της ανθρώπινης ιστορίας είναι η ανάγκη για ασφαλή αποθήκευση και μετάδοση πληροφορίας. Η ανάγκη αυτή δημιουργήθηκε αρχικά, λόγω της διαφορετικότητας των ανθρώπων σε επίπεδο κοινωνικό, πολιτικό, στρατιωτικό ή ακόμη και θρησκευτικών πεποιθήσεων. Η ραγδαία ανάπτυξη των επικοινωνιακών συστημάτων σήμερα, προσφέρει σε ένα μεγάλο ποσοστό ανθρώπων, πρόσβαση σε μία τεράστια ποσότητα πληροφορίας και μία ποικιλία από ηλεκτρονικά μέσα με σκοπό την ανταλλαγή προσωπικών δεδομένων. Επομένως, κάθε πληροφορία που μεταδίδεται χρειάζεται να μετατραπεί σε μία μη αναγνωρίσιμη μορφή έτσι ώστε να διασφαλιστεί η ασφάλεια της.

Η επεξεργασία και κρυπτογράφηση των δεδομένων είναι αναγκαίο να συμβεί σε πραγματικό χρόνο. Για αυτό το λόγο έχουν αναπτυχθεί αρκετοί αλγόριθμοι κρυπτογράφησης και συγκεκριμένα αλγόριθμοι κρυπτογράφησης συμμετρικού κλειδιού. Το βασικό πλεονέκτημα των αλγορίθμων συμμετρικού κλειδιού είναι ότι η διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης είναι πολύ γρήγορη και δεν καταναλώνει σημαντική υπολογιστική ισχύ. Βασικός άξονας της θεματικής περιοχής είναι η ανάλυση των χαρακτηριστικών λειτουργίας και απόδοσης, των αλγορίθμων κρυπτογραφίας συμμετρικού κλειδιού που έχουν προταθεί σε διεθνής διαγωνισμούς τυποποίησης, για κρυπτογραφική πιστοποίηση. Οι πιο γνωστοί αλγόριθμοι αυτού του είδους είναι οι DES, Triple DES, IDEA, RC2, RC4, AES.

Σκοπός της πτυχιακής εργασίας είναι η ανάλυση αυτών των αλγορίθμων, στα κύρια κριτήρια σχεδιασμού: ασφάλειας, δυνατότητας εφαρμογής, ευρωστίας, καθώς και ο αναλυτικός προσδιορισμός των χαρακτηριστικών απόδοσης τους. Στην παρούσα εργασία θα γίνει θεωρητική ανάλυση των αλγορίθμων με βάση το πρότυπο που τους περιγράφει καθώς και χρήση παραδειγμάτων πάνω σε αυτό. Στο τέλος, θα γίνει προσομοίωση του αλγόριθμου με τις καλύτερες επιδόσεις, σε προγραμματιζόμενο ολοκληρωμένο κύκλωμα γενικής χρήσης (Field Programmable Gate Array – FPGA) χρησιμοποιώντας τη γλώσσα περιγραφής υλικού VHDL. Τα αποτελέσματα της παραπάνω έρευνας θα αποτυπωθούν σε σύγχρονες εφαρμογές κρυπτογραφίας και ασφάλειας δεδομένων.

Απαιτήσεις: Ψηφιακή σχεδίαση, Προγραμματισμός VHDL, Αρχιτεκτονική FPGA, Πρωτόκολλά ασφάλειας.

Πλεονεκτήματα: Με την παρούσα διπλωματική εργασία ο φοιτητής θα αποκομίσει καλή γνώση σχεδιασμού ψηφιακών συστημάτων, προγραμματισμού με VHDL και την εμπειρία της υλοποίησης σύγχρονων κρυπτογραφικών εφαρμογών για την προστασία της πληροφορίας σε επίπεδο υλικού. Σχεδίαση Ενσωματωμένων Εφαρμογών σε SoC που περιλαμβάνεται η ανάπτυξη κώδικα στον ενσωματωμένο επεξεργαστή (embedded firmware).

Ενδεικτική βιβλιογραφία

1. Potlapally, N. R., Ravi, S., Raghunathan, A., & Jha, N. K. (2003, August). Analyzing the energy consumption of security protocols. In Proceedings of the 2003 international symposium on Low power electronics and design (pp. 30-35). ACM.
2. Manifavas, C., Hatzivasilis, G., Fysarakis, K., & Rantos, K. (2014). Lightweight cryptography for embedded systems–A comparative analysis. In Data Privacy Management and Autonomous Spontaneous Security (pp. 333-349). Springer, Berlin, Heidelberg.
3. Potlapally, N. R., Ravi, S., Raghunathan, A., & Jha, N. K. (2006). A study of the energy consumption characteristics of cryptographic algorithms and security protocols. IEEE Transactions on mobile computing, 5(2), 128-143.