Σχεδίαση και υλοποίηση αντιμέτρων ενάντια σε επιθέσεις υλικού σε FPGA με σύνθεση υψηλού επιπέδου (High Level Synthesis) για εφαρμογές ασφάλειας

Περιγραφή

Η πλειοψηφία των σύγχρονων ψηφιακών εφαρμογών (IoT, τραπεζικές εφαρμογές κλπ.) βασίζονται σε κρυπτογραφικές υλοποιήσεις για την παροχή ικανοποιητικών επιπέδων ασφάλειας. Η ύπαρξη επιθέσεων υλικού όπως για παράδειγμα οι επιθέσεις πλευρικού καναλιού (Side Channel Analysis attacks) και οι επιθέσεις εισαγωγής σφαλμάτων (Fault Injection attacks) είναι δυνατόν να υποβαθμίσουν σημαντικά και έως να εξαλείψουν το επιθυμητό επίπεδο ασφάλειας [1, 2]. Η παρούσα πτυχιακή εργασία θα αφορά την σχεδίαση και υλοποίηση αντιμέτρων ενάντια σε επιθέσεις υλικού. Αρχικά θα μελετηθούν επιθέσεις υλικού και έπειτα θα σχεδιαστούν αντίμετρα με χρήση εργαλείων σύνθεσης υψηλού επιπέδου, όπου η περιγραφές των κυκλωμάτων γίνονται με χρήση της γλώσσας C και η υλοποίηση τους γίνεται με εργαλεία σύνθεσης υψηλού επιπέδου (HLS) για σύγχρονα FPGAs [3]. Θα αποκτηθεί εμπειρία με το σύνολο των εργαλείων σύνθεσης για Xilinx FPGAs (Vivado HLS ή Vitis HLS) καθώς και με τη σχεδίαση αντιμέτρων επιθέσεων υλικού με χρήση γλωσσών υψηλού επιπέδου. Η μέγιστη διάρκεια ολοκλήρωσης της πτυχιακής είναι ένα ημερολογιακό έτος.

Παραδοτέα

- Ο C κώδικας περιγραφής των κρυπτογραφικών αλγορίθμων
- Οι υλοποιήσεις τους με χρήση του Vivado HLS και το επίπεδο ασφάλειας μέσω διεξαγωγής πειραμάτικών επιθέσεων υλικού
- Αναφορά πτυχιακής εργασίας

Απαραίτητες και επιθυμητές γνώσεις

Η γνώση της C ή C++ είναι απαραίτητη για την ανάληψη της εργασίας. Επιθυμητή η γνώση σχεδίασης κυκλωμάτων με χρήση VHDL ή Verilog και του λογισμικού Vivado.

Βιβλιογραφία και αναφορές

[1] Mangard, Stefan, Elisabeth Oswald, and Thomas Popp. Power analysis attacks: Revealing the secrets of smart cards. Vol. 31. Springer Science & Business Media, 2008.

[2] Barenghi, Alessandro, Luca Breveglieri, Israel Koren, and David Naccache. "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures." Proceedings of the IEEE 100, no. 11 (2012): 3056-3076.

[3] https://www.xilinx.com/support/documentation-navigation/design-hubs/dh0012-vivado-high-level-synthesis-hub.html

Πλήθος φοιτητών

1 ή 2 άτομα. Η ακριβής έκταση της εργασίας θα είναι ανάλογη του αριθμού των φοιτητών που θα την αναλάβουν.

Επιβλέπων

Θάνος Παπαδημητρίου (a.papadimitriou@uop.gr). Προτείνεται η επαφή με τον επιβλέποντα πριν δηλώσετε το παρόν θέμα, ώστε να σας είναι ξεκάθαρη η ακριβής έκταση της εργασίας και οι απαιτήσεις της.