Υλοποίηση εργαλείων ηλεκτρονικού αυτοματισμού (Electronic Design Automation) για FPGA με χρήση των βιβλιοθηκών RAPIDWRIGHT της XILINX 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].

Στην παρούσα πτυχιακή εργασία θα γίνει χρήση των εργαλείων Rapidwright (https://www.rapidwright.io) για την υλοποίηση εργαλείων ηλεκτρονικού αυτοματισμού με στόχο την αύξηση της απόδοσης και τη μελέτη ιδιοτήτων ασφάλειας, κρυπτογραφικών FPGA υλοποιήσεων.

Θα αποκτηθεί εμπειρία στο το σύνολο των εργαλείων σύνθεσης για Xilinx FPGAs, σε επιθέσεις υλικού και στη σχεδίαση εργαλείων ηλεκτρονικού αυτοματισμού για εφαρμογές ασφάλειας σε αρχιτεκτονικές FPGA.

Παραδοτέα

- Ο Java κώδικας των EDA αλγορίθμων με χρήση της βιβλιοθήκης RAPIDWRIGHT
- Οι αναλύσεις των επιπέδων ασφάλειας μέσω των υλοποιημένων EDA αλγορίθμων και η σύγκρισή τους με τα αποτελέσματα πειραματικών επιθέσεων υλικού
- Αναφορά πτυχιακής εργασίας

Απαραίτητες και επιθυμητές γνώσεις

Η γνώση της Java ή ισχυρή επιθυμία της εκμάθησής της 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.

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.