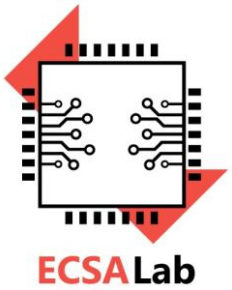
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου

Εργαστήριο Ηλεκτρονικών Κυκλωμάτων, Συστημάτων και Εφαρμογών (ECSA Lab.)



Ασφάλεια Υπολογιστικών Συστημάτων

Διδάσκων: Δρ. Παρασκευάς Κίτσος

Άσκηση στη θεματική ενότητα του Σχεδιασμού Ασφαλούς Υλικού

1) Έστω ο αλγόριθμο RSA που εκτελεί εκθετοποίηση με τον αλγόριθμο square-and-multiply. Με βάση το παρακάτω ίχνος κατανάλωσης που λαμβάνεται κατά την αποκρυπτογράφηση: S M S S M S
Όπου S = square step (σταθερό pattern κατανάλωσης)
M = multiply step (χαρακτηριστική αιχμή)

(α) Ποιο είναι το bit-pattern του εκθέτη d;
(β) Υποθέστε ότι ο αλγόριθμος εκτελείται MSB→LSB. Ποιο είναι το μυστικό κλειδί πραγματικό d;

2) Έστω ο αλγόριθμο RSA που εκτελεί εκθετοποίηση με τον αλγόριθμο square-and-multiply. Για το κλειδί d = 0xF0 = $(11110000)_2$ να βρείτε τα παρακάτω.
α) Ποιες πράξεις (S=Square, M=Multiply) θα εκτελεστούν;

β) Πόσες πράξεις Square και πόσες Multiply θα παρατηρηθούν;

Και επίσης να σχεδιάστε το αναμενόμενο μοτίβο κατανάλωσης

3) Να σχεδιάσετε ένα συνδυαστικό (Combinational) mini-trojan (hardware) με τρεις εισόδους που να:

- Ενεργοποιείται όταν A=1 και B=0 και C=1
- Αντικαθιστά το bit Y με το notY

Ζητείται:
(α) Σχεδιάγραμμα λογικών πυλών

(β) Trigger & payload
(γ) Είναι εύκολα εντοπίσιμο;