# 3 θέματα εργασιών στην περιοχή της Ασφάλειας Υλικού (Hardware Security)

- Η πλειοψηφία των σύγχρονων ψηφιακών εφαρμογών (IoT, τραπεζικές εφαρμογές κλπ.) βασίζονται σε κρυπτογραφικές υλοποιήσεις για την παροχή ικανοποιητικών επιπέδων ασφάλειας

# 3 θέματα εργασιών στην περιοχή της Ασφάλειας Υλικού (Hardware Security)

- Η επιτάχυνση υλικού είναι απαραίτητη για εφαρμογές
  - Με περιορισμούς στην κατανάλωση ενέργειας
  - Με υψηλές προδιαγραφές ταχύτητας κρυπτογράφησης
- Αναγκαία για πληθώρα εφαρμογών η συνεργασία επεξεργαστών με κρυπτογραφικών επιταχυντών υλικού για την επίτευξη των απαιτούμενων προδιαγραφών

# 3 θέματα εργασιών στην περιοχή της Ασφάλειας Υλικού (Hardware Security)

- Η επιτάχυνση υλικού είναι απαραίτητη για εφαρμογές
  - Με περιορισμούς στην κατανάλωση ενέργειας
  - Με υψηλές προδιαγραφές ταχύτητας κρυπτογράφησης
- Αναγκαία για πληθώρα εφαρμογών η συνεργασία επεξεργαστών με κρυπτογραφικών επιταχυντών υλικού για την επίτευξη των απαιτούμενων προδιαγραφών

# 3 θέματα εργασιών στην περιοχή της Ασφάλειας Υλικού (Hardware Security)

- Αυξανόμενη τάση χρήσης FPGAs
  - Η χρήση επεξεργαστών ανοικτού instruction set όπως ο RISC-V
  - Η βελτίωση των τεχνολογιών FPGAs
  - Πλεονεκτήματα FPGAs όπως επαναδιαμόρφωση
- Η ανάγκη αύξησης της παραγωγικότητας σχεδίασης οδηγεί στην χρήση υψηλότερου επιπέδου γλωσσών για την περιγραφή υλικού
  - High Level Synthesis (C/C++)

# 3 θέματα εργασιών στην περιοχή της Ασφάλειας Υλικού (Hardware Security)

- Επιθέσεις Υλικού μπορούν να μειώσουν τα επίπεδα ασφάλειας κρυπτογραφικών επιταχυντών
  - Επιθέσεις Πλευρικού Καναλιού (Side Channel Attacks)
  - Επιθέσεις Εισαγωγής Σφαλμάτων (Fault Injection Attacks)
- Καθιστούν αναγκαία τη μελέτη της Ασφάλειας Υλικού!

# 3 θέματα εργασιών στην περιοχή της Ασφάλειας Υλικού (Hardware Security)

- Σχεδίαση και υλοποίηση κρυπτογραφικών επιταχυντών υλικού σε FPGA με σύνθεση υψηλού επιπέδου (High Level Synthesis)
- Σχεδίαση και υλοποίηση αντιμέτρων ενάντια σε επιθέσεις υλικού σε FPGA με σύνθεση υψηλού επιπέδου (High Level Synthesis) για εφαρμογές ασφάλειας
- Υλοποίηση εργαλείων ηλεκτρονικού αυτοματισμού (Electronic Design Automation) για FPGA με χρήση των βιβλιοθηκών RAPIDWRIGHT της XILINX για εφαρμογές ασφάλειας

# 3 θέματα εργασιών στην περιοχή της Ασφάλειας Υλικού (Hardware Security)

- Επιβλέπων:

  Θάνος Παπαδημητρίου,

  Επίκ. Καθηγητής, Τμήμα Ψηφιακών Συστημάτων,

  Πανεπ. Πελοποννήσου

- Email: a.papadimitriou@uop.gr