ATHENA Research & Innovation Information Technologies

I3T – Καινοτόμος Εφαρμογή του Βιομηχανικού Διαδικτύου των Πραγμάτων (IIoT) σε Ευφυή Περιβάλλοντα

Αρχιτεκτονική Υλικού μιας Μονάδας Έμπιστης Πλατφόρμας

Πάρης Κίτσος

Συνεργαζόμενο Ακαδημαϊκό Προσωπικό - Αναπληρωτής Καθηγητής

ΕΚ ΑΘΗΝΑ / ΙΝΒΙΣ - Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Παν. Πελοποννήσου

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΑΝΑΠΤΥΞΗΣ ΚΑΙ ΕΠΕΝΔΥΣΕΩΝ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΔΙΑΡΘΡΩΤΙΚΩΝ ΠΡΟΓΡΑΜΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ

ΕΠΑνΕΚ 2014–2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ
ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ
ΚΑΙΝΟΤΟΜΙΑ

ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Περιεχόμενα Παρουσίασης

- Στοιχεία έργου-πακέτων εργασιών
- Πρότυπο σχεδίασης Μονάδας Έμπιστης Πλατφόρμας
- Σχεδιασμός σε περιβάλλοντα IIoT
- Σχεδιασμός αρχιτεκτονικής Μονάδας Έμπιστης Πλατφόρμας στο I3T
- Αποτελέσματα διάχυσης

Στοιχεία Έργου…

- Η ερευνητική ομάδα απαρτίζονταν
- Λάμπρο Πύργα, Συνεργαζόμενος Ερευνητής - Υποψήφιος Διδάκτορας
  - ΕΚ ΑΘΗΝΑ / ΙΝΒΙΣ – Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του π. Πελοποννήσου
- Απόστολο Φούρναρη, Κύριος Ερευνητής
  - ΕΚ ΑΘΗΝΑ / ΙΝΒΙΣ
- Πάρης Κίτσος, Συνεργαζόμενο Ακαδημαϊκό Προσωπικό – Αναπληρωτής Καθηγητής
  - ΕΚ ΑΘΗΝΑ / ΙΝΒΙΣ – Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του π. Πελοποννήσου

…Στοιχεία Έργου

- Αφορά βασικό τμήμα του ΠΕ5 – Ασφαλή Βιομηχανικά Συστήματα
  - Συμμετοχή στην
    - Ε5.1: Ανάπτυξη μοντέλων επιθέσεων για βιομηχανικά συστήματα από το επίπεδο της συσκευής του PLC έως την εφαρμογή
    - Ε5.2: Ανάπτυξη αρχιτεκτονικής για μια Μονάδα Έμπιστης Πλατφόρμας (Trusted Platform Module) Third level
    - Ε5.3: Υλοποίηση συστήματος μιας Μονάδας Έμπιστης Πλατφόρμας (Trusted Platform Module)
- ΕΕ2: Διάχυση και Αξιοποίηση Αποτελεσμάτων

Πρότυπο σχεδίασης Μονάδας Έμπιστης Πλατφόρμας…

- Μια Μονάδα Έμπιστης Πλατφόρμας (Trusted Platform Module - TPM) αποτελεί τμήμα του συστήματος βιομηχανικού ελέγχου και έχει σκοπό την ασφαλή αποθήκευση, επεξεργασία και μεταφορά δεδομένων
- Είναι μια συσκευή ασφαλείας η οποία αποσκοπεί στο να κρατά το υπολογιστικό περιβάλλον ασφαλές απομονώνοντας τους αλγορίθμους κρυπτογράφησης και τα δεδομένα από την κεντρική μονάδα επεξεργασίας

…Πρότυπο σχεδίασης Μονάδας Έμπιστης Πλατφόρμας…

ICS › 35 › 35.030

ISO/IEC 11889-1:2015

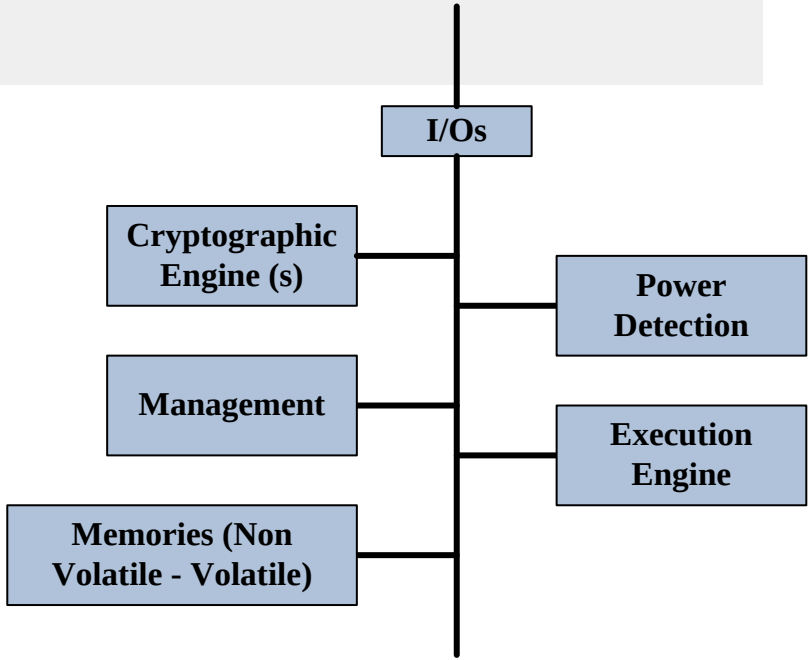
Information technology — Trusted platform module library — Part 1: Architecture

THIS STANDARD WAS LAST REVIEWED AND CONFIRMED IN 2021. THEREFORE THIS VERSION REMAINS CURRENT.

https://www.iso.org/standard/66510.html

…Πρότυπο σχεδίασης Μονάδας Έμπιστης Πλατφόρμας

- Πρότυπο ISO/IEC 11889-1: 2015
- Η αρχιτεκτονική της σύμφωνα με το πρότυπο αποτελείται
  - I/Os
  - Το υποσύστημα Κρυπτογραφίας
  - Το υποσύστημα Εξουσιοδότησης
  - Το υποσύστημα Μνημών (Πτητική κ μη-πτητική)
  - Μονάδα Ανίχνευσης Κατάστασης



Σχεδιασμός σε περιβάλλοντα IIoT…

- Βιομηχανικά περιβάλλοντα: Η μακροζωία και η πιστότητα οποιασδήποτε συσκευής είναι επιτακτική για τη σωστή λειτουργία
- Συσκευές τροφοδοσίας: Η μακροζωία και η πιστότητα οποιασδήποτε συσκευής είναι επιτακτική για τη σωστή λειτουργία

…Σχεδιασμός σε περιβάλλοντα IIoT

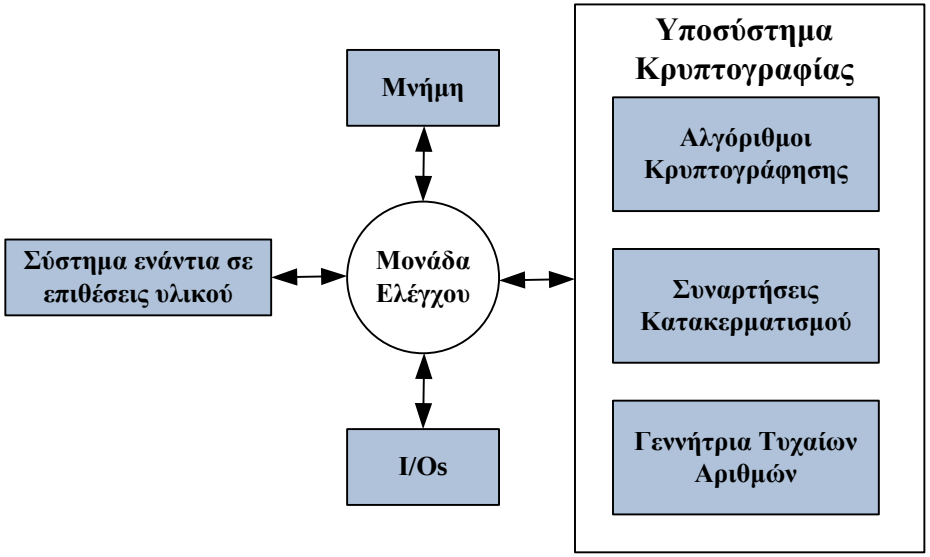
- Έξυπνα εξαρτήματα (αισθητήρες, ενεργοποιητές, MCUs, κλπ) χαμηλής κατανάλωσης
- Απαιτείται σχεδιασμός χαμηλής κατανάλωσης ισχύος
- Χρήση των λιγότερων δυνατών πόρων υλικού για τον σχεδιασμό των συστημάτων που επεξεργάζονται τα δεδομένα

Σχεδιασμός αρχιτεκτονικής Μονάδας Έμπιστης Πλατφόρμας στο IoT

- Στα πλαίσια του παρόντος έργου υλοποιήθηκε μια Μονάδα Έμπιστης Πλατφόρμας ειδικά σχεδιασμένη για χρήση σε βιομηχανικά συστήματα και εφαρμογές IoT
- Υλοποιήθηκαν αρκετοί αλγόριθμοι κρυπτογραφίας
- Υπάρχει πρόβλεψη για τον ασφαλή σχεδιασμό του ολοκληρωμένου (σχεδιασμός ενάντια σε επιθέσεις στο υλικό)

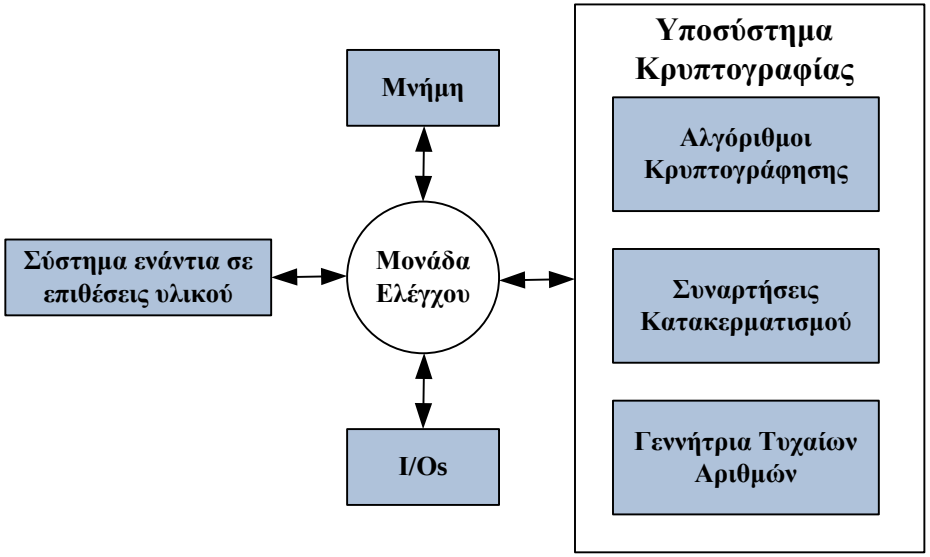
…Σχεδιασμός αρχιτεκτονικής Μονάδας Έμπιστης Πλατφόρμας στο ΙΣΤ…

- Στοιχεία του «κυκλώματος»
  - Χαμηλής Κατανάλωσης Ενέργειας
  - Ελάχιστοι πόροι υλικού



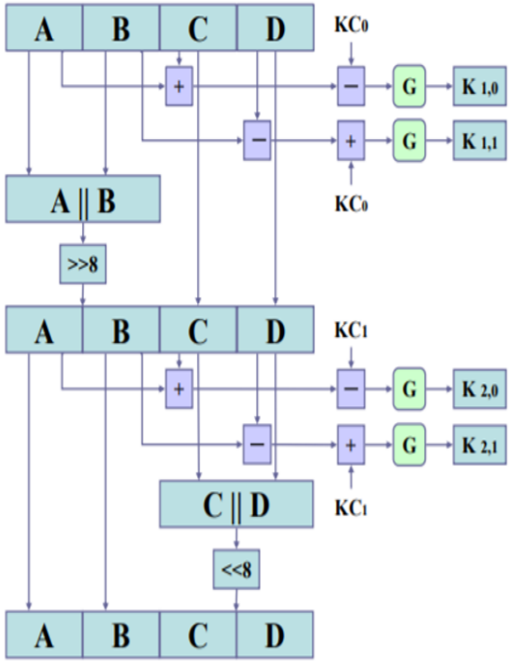
Σχεδιασμός αρχιτεκτονικής Μονάδας Έμπιστης Πλατφόρμας στο I3T…

- Αλγόριθμοι κρυπτογράφησης τμήματος
  - Seed (ISO/IEC 18033-3:2010)
  - Clefia (ISO/IEC 29192-2:2019)
- Αλγόριθμοι κρυπτογράφησης ροής
  - Enocoro-128v2 (ISO/IEC 29192-3:2012)
  - Snow-V (Χρήση στο 5G)
- Συνάρτηση Κατακερματισμού
  - Lesamnta-LW (ISO/IEC 29192-5:2016)
- Σύστημα ενάντια σε επιθέσεις υλικού
  - Ανίχνευση Ιόμορφου Υλικού (Hardware Trojans) με τη μέθοδο του πλέγματος



Αλγόριθμος SEED…

- Αλγόριθμος τμήματος (block cipher)
- Αναπτύχθηκε από τον Κορεατικό Οργανισμό Ασφάλειας Πληροφοριών
- Κείμενο (plaintext/ciphertext) και κλειδί των 128 bit

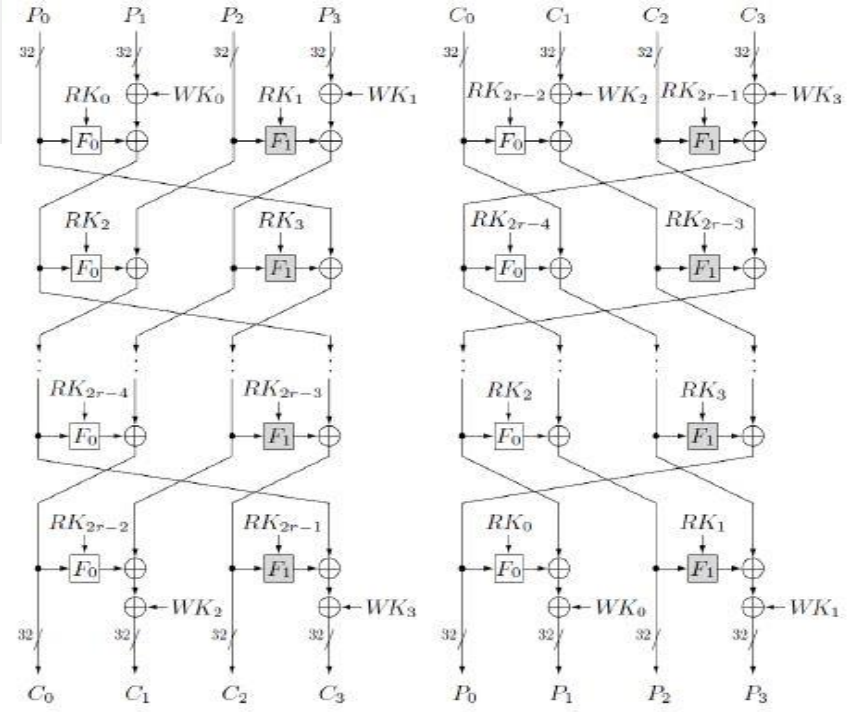


…Αλγόριθμος SEED

- Σχεδιάστηκε μια συμπαγής (compact) αρχιτεκτονική κατάλληλη για εφαρμογές ασφαλείας σε περιβάλλον Internet of Things (IoT)
- Το datapath της σειριακής αυτής αρχιτεκτονικής είναι 4-bit
- Η τελική υλοποίηση επιτυγχάνει απόδοση (throughput) έως 45 Mbps σε συχνότητα ρολογιού 204 MHz
- Κάθε γύρος χρειάζεται 35 κύκλους ρολογιού
- Η υλοποίηση και χρησιμοποιεί μόνο 425 FPGA LUTs, 382 FFs και 1024 x 8 bits Block RAM
- Η κατανάλωση ισχύος ήταν 135 mW @ 205 MHz και 107 mW @ 100 KHz.

Αλγόριθμος Clefia…

- Αναπτύχθηκε από την SONY
- 128 bit Κείμενο (plaintext)
- 128/192/256 bit Κλειδί (key)

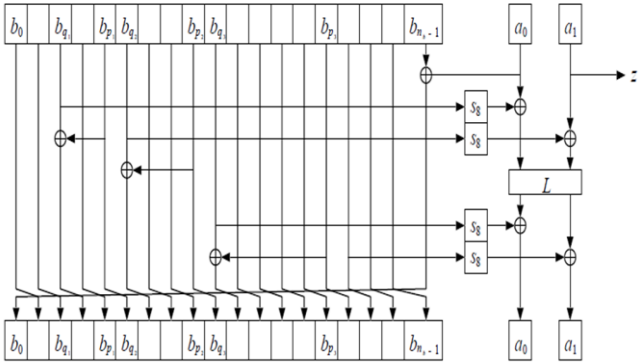


…Αλγόριθμος Clefia

- Εκμετάλλευση της συμμετρίας τμημάτων του αλγορίθμου
- Η υλοποίηση της παρούσας 4-bit αρχιτεκτονικής απαιτεί 477 FFs και 606 LUTs
- Η μέγιστη υποστηριζόμενη συχνότητα είναι 115 MHz ενώ η μέγιστη απόδοση (throughput) αγγίζει τα 28 Mbps
- Επιπλέον, η δυναμική κατανάλωση ισχύος είναι 13 mW (83 mW συνολικά για στατική και δυναμική κατανάλωση ισχύος) κατά την μέγιστη συχνότητα λειτουργίας και λιγότερο από 1 mW (70 mW συνολικά για στατική και δυναμική κατανάλωση ισχύος) στην συχνότητα των 100 KHz

Αλγόριθμος Enocoro-128v2…

- Αλγόριθμος κρυπτογράφησης ροής (stream cipher)
- Αναπτύχθηκε από την Hitachi, Ltd
- 128/192/256 bit Κλειδί (key)
- 64 bit διάνυσμα αρχικοποίησης (IV)
- Μπορεί να χρησιμοποιηθεί και ως γεννήτρια τυχαίων αριθμών



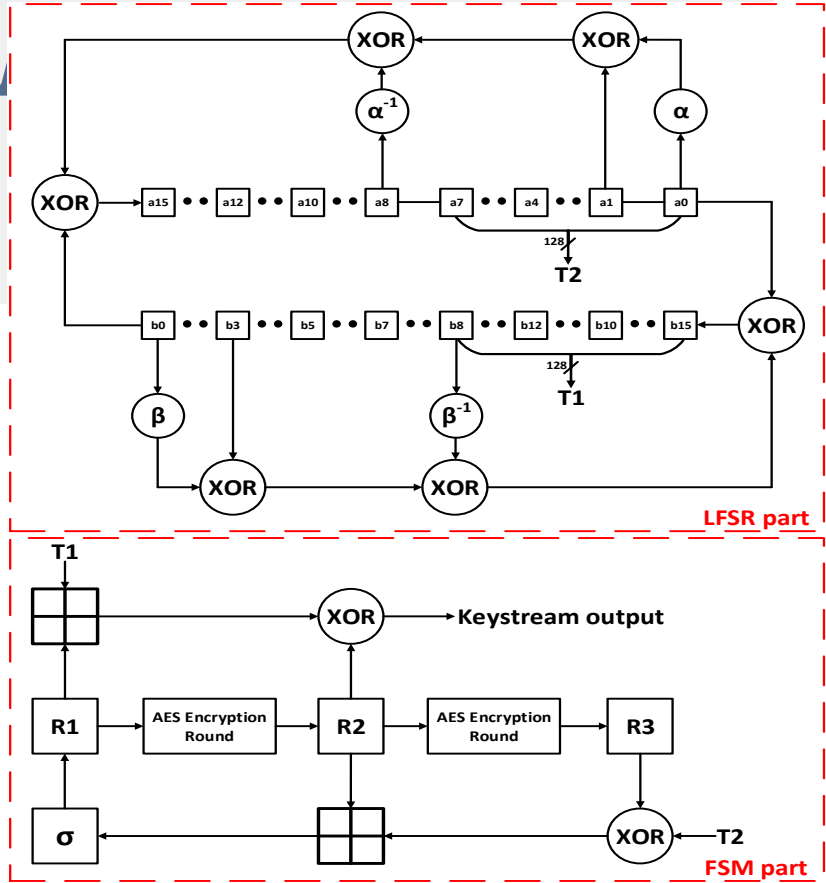
…Αλγόριθμος Enocoro-128v2

- Η 8-bit αρχιτεκτονική χρησιμοποιεί 254 LUTs και 330 FFs. Κάθε γύρος του αλγορίθμου χρειάζεται 5 κύκλους ρολογιού. Η μέγιστη συχνότητα που επιτυγχάνεται είναι 189 MHz και η μέγιστη απόδοση (throughput) 302 Mbps. Η δυναμική κατανάλωση ισχύος της υλοποίησης είναι 41 mW.

- Η 4-bit αρχιτεκτονική χρησιμοποιεί 249 LUTs και 343 FFs. Κάθε γύρος χρειάζεται 9 κύκλους ρολογιού, η μέγιστη συχνότητα της υλοποίησης είναι 204 MHz και η μέγιστη απόδοση (throughput) 181 Mbps. Τέλος, η δυναμική κατανάλωση ισχύος της υλοποίησης είναι 40 mW.

Αλγόριθμος Snow-V

- Αλγόριθμος κρυπτογράφησης ροής (stream cipher)
- 256-bit Κλειδί (key)
- 128-bit διάνυσμα αρχικοποίησης (IV)
- 128-bit έξοδος

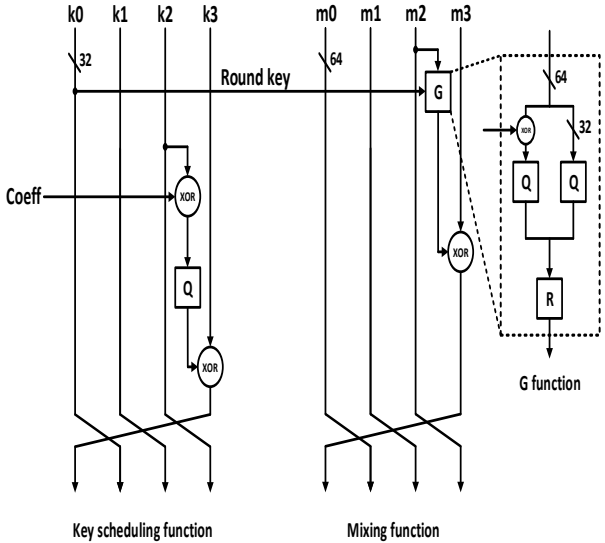


…Αλγόριθμος Snow-V

- Η υλοποίηση της αρχιτεκτονικής απαιτεί 2109 LUTs και 1352 FFs. Δεν χρησιμοποιείται καμία μνήμη
- Η μέγιστη συχνότητα που επιτυγχάνεται είναι 224 MHz και η μέγιστη απόδοση (throughput) 2606 Mbps
- Η προτεινόμενη υλοποίηση συγκρίθηκε με πλήθος άλλων υλοποιήσεων αλγορίθμων κρυπτογράφησης ροής και τα αποτελέσματα κατέδειξαν ότι και η προτεινόμενη υλοποίηση αποτελεί μια αξιόπιστη επιλογή για τον τομέα της ασφαλείας βιομηχανικών εφαρμογών

Συνάρτηση κατακερματισμού Lesamnta-LW…

- Αναπτύχθηκε από την Hitachi, Ltd
- 256 bit Κείμενο (plaintext)
- 128 bit Κλειδί (key)

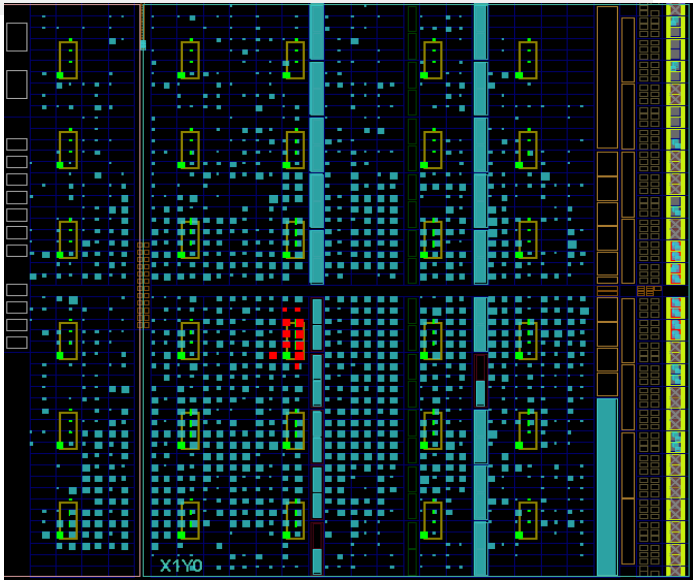


…Συνάρτηση κατακερματισμού Lesamnta-LW

- Χρησιμοποιήθηκαν βέλτιστες τεχνικές κατά τον σχεδιασμό της αρχιτεκτονικής
- Γίνεται επαναχρησιμοποίηση υποσυστημάτων
- Επιπροσθέτως, ο υπολογισμός των υποκλείδιών του επόμενου γύρου γίνεται κατά τους πρώτους κύκλους ρολογιού κάθε γύρου ώστε να αξιοποιούνται αδρανή σε άλλη περίπτωση υποσυστήματα
- Απαιτεί ελάχιστο αριθμό πόρων, συγκεκριμένα 434 LUTs και 474 FFs
- Λειτουργεί με μια μέγιστη συχνότητα 161 MHz, απαιτεί 768 κύκλους ρολογιού για την ολοκλήρωση των 64 γύρων υπολογισμού (κάθε γύρος απαιτεί 12 γύρους ρολογιού) και έχει απόδοση (throughput) ίσο με 50 Mbps
- Επίσης, σε μια τυπική συχνότητα ρολογιού για IoT εφαρμογές (100 KHz) έχει απόδοση 30.3 Kbps

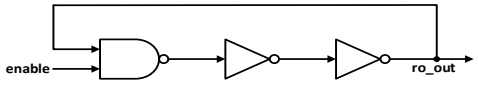
Ανίχνευση Ιόμορφου Υλικού με τη μέθοδο του πλέγματος…

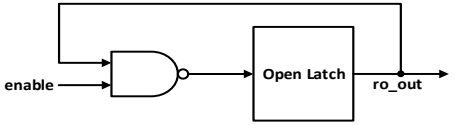
- Κάθε αισθητήρας αποτελείται από δυο μέρη
  - Έναν ταλαντωτής δακτυλίου (Ring Oscillator - RO)
  - Και έναν μετρητή (counter).
- Ο προτεινόμενος μετρητής είναι μετρητής τύπου Αριθμητικού Συστήματος Υπολοίπων (Residue Number System-RNS)
- Για τον υπολογισμό της μέτρησης χρησιμοποιεί το Κινεζικό Θεώρημα Υπολοίπων (Chinese Remainder Theorem – CRT)

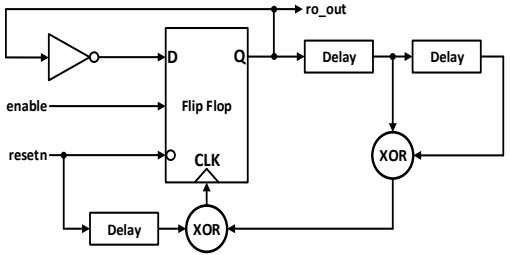


…Ανίχνευση Ιόμορφου Υλικού με τη μέθοδο του πλέγματος…

- Μελετήθηκαν τρεις τύποι ROs
  - Ο κλασσικός 3-Stage RO
  - Ο Latch based RO και
  - Ο Flip-Flop based RO

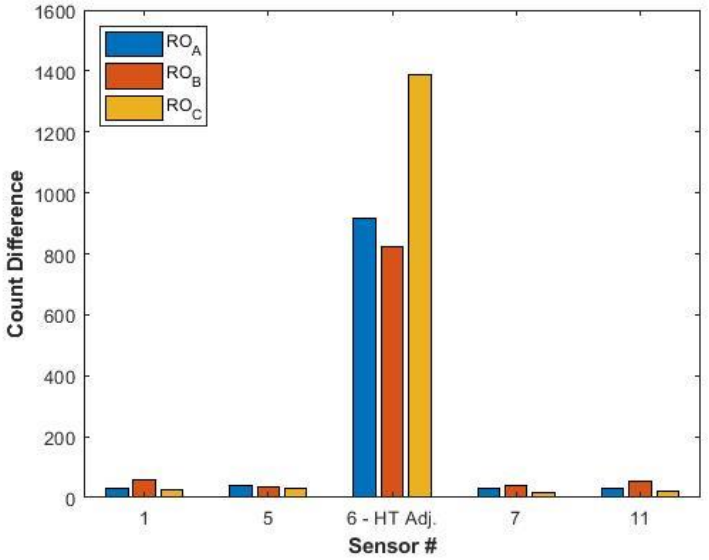






Ανίχνευση Ιόμορφου Υλικού με τη μέθοδο του πλέγματος…

- Παρατηρήθηκε διαφορετική ευαισθησία του κάθε ταλαντωτή ως προς την ανίχνευση κακόβουλου υλικού



Αποτελέσματα διάχυσης – ερευνητικής δραστηριότητας…

- Δημοσιεύτηκαν και παρουσιάστηκαν 10 εργασίες στη διάρκεια του έργου
  - 2 σε διεθνή περιοδικά με κριτές
  - 8 σε διεθνή συνέδρια με κριτές

Αποτελέσματα διάχυσης – ερευνητικής δραστηριότητας…

- L. Pyrgas, P. Kitsos, “FPGA Implementation of SNOW-V Stream Cipher”, DSD 2021. (έχει γίνει αποδεκτή για παρουσίαση)
- L. Pyrgas, P. Kitsos, "Compact Hardware Architectures of Enocoro-128v2 Stream Cipher for Constrained Embedded Devices", Electronics 2020, 9(9), 1505
- L. Pyrgas, A. Panagiotarou and P. Kitsos, "Are ring oscillators without a combinatorial loop good enough for Hardware Trojan detection?", 2020 23rd Euromicro Conference on Digital System Design (DSD), Kranj, Slovenia, 2020, pp. 218-221
- L. Pyrgas, P. Kitsos, "An 8-bit Compact Architecture of Lesamnta-LW Hash Function for Constrained Devices", 2019 26th IEEE International Conference on Electronics, Circuits and Systems (ICECS), pp. 743-746, Genoa, Italy, November 27 - 29, 2019
- L. Pyrgas, P. Kitsos, "A Very Compact Architecture of CLEFIA Block Cipher for Secure IoT Systems", 22nd Euromicro Conference on Digital Systems (DSD'19), pp. 624-627, Kallithea, Chalkidiki, Greece, Czech Republic, August 28 - August 30, 2019

…Αποτελέσματα διάχυσης – ερευνητικής δραστηριότητας

- A. Fournaris, L. Pyrgas, P. Kitsos, ”An efficient multi-parameter approach for FPGA hardware Trojan detection”, Microprocessors and Microsystems, Volume 71, 2019
- F. Pirpilidis, L. Pyrgas, P. Kitsos, "A 4-Bit Architecture of SEED Block Cipher for IoT Applications", 25th IEEE International Conference on Electronics Circuits and Systems (ICECS 2018), pp. 389-392, Bordeaux, France, 9-12 December, 2018
- A. Fournaris, L. Pyrgas, P. Kitsos, “An FPGA Hardware Trojan Detection Approach Based on Multiple Parameter Analysis”, 21st Euromicro Conference on Digital Systems (DSD'18), Prague, Czech Republic, August 29 - August 31, 2018
- L. Pyrgas, P. Kitsos, “A Hybrid FPGA Trojan Detection Technique Based-on Combinatorial Testing and On-chip Sensing”,14th International Symposium on Applied Reconfigurable Computing (ARC 2018), Santorini, Greece, May 2-4, 2018
- L. Pyrgas, F. Pirpilidis, A. Panayiotarou, P. Kitsos, "Thermal Sensor Based Hardware Trojan Detection in FPGAs", 20th Euromicro Conference on Digital System Design (DSD 2017), 8049795, pp. 268-273, Vienna, Austria, 30 August - 1 September, 2017

Ευχαριστώ!