ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Ασφάλεια και κρυπτογραφικές εφαρμογές σε ενσωματωμένα συστήματα

ΑΡΓΥΡΙΟΣ Σ. ΣΙΔΕΡΗΣ

ΕΠΙΒΛΕΠΩΝ: Μηνάς Δασυγένης, Αναπληρωτής Καθηγητής Π.Δ.Μ.

ΜΕΛΗ ΤΡΙΜΕΛΟΥΣ

Αθανάσιος Κακαρούντας, Καθηγητής Π.Θ.
Παναγιώτης Σαρηγιαννίδης, Καθηγητής Π.Δ.Μ.

ΜΕΛΗ ΕΠΤΑΜΕΛΟΥΣ

Γεώργιος Φραγκούλης, Καθηγητής Π.Δ.Μ.
Νικόλαος Πλόσκας, Αναπληρωτής Καθηγητής Π.Δ.Μ.
Μιχαήλ Δόσης, Καθηγητής Π.Δ.Μ.
Δημήτριος Καραμπατζάκης, Αναπληρωτής Καθηγητής Δ.Π.Θ.

Επισκόπηση

- Εισαγωγή
- Βιβλιογραφική ανασκόπηση και προτεινόμενη προσέγγιση
- Τεχνική επιτάχυνσης με pipelining του SHA-3 σε FPGA
- Τεχνική επιτάχυνσης με loop unrolling του SHA-3 σε FPGA
- Τεχνική επιτάχυνσης με pipelining και loop unrolling του SHA-3 σε FPGA
- Συμπεράσματα
- Μελλοντικοί στόχοι
- Δημοσιεύσεις

Ερευνητικό πρόβλημα

Επιτάχυνση του αλγόριθμου κατακερματισμού SHA-3 (Secure Hash Algorithm 3)[1] σε FPGA (Field-Programmable Gate Array)

- **Προκλήσεις στην υλοποίηση του αλγόριθμου SHA-3 σε FPGA**
  - Μεγιστοποίηση ταχύτητας λειτουργίας (συχνότητας - MHz)
  - Παράλληλη επεξεργασία δεδομένων
  - Κατανάλωση πόρων (FPGA slices - area)
- **Έλλειψη ολοκληρωμένων μεθοδολογιών βελτιστοποίησης**
  - Μεμονωμένες τεχνικές
  - Υλοποιήσεις brute-force
- **Βασικές τεχνικές επιτάχυνσης**
  - με pipelining
  - με loop unrolling
  - Συνδυασμός (pipelining και loop unrolling)

[1] Επιλέξαμε τον αλγόριθμο SHA-3 που είναι το τελευταίο μέλος της οικογένειας προτύπων Secure Hash Algorithm , που πιστοποιήθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) των ΗΠΑ, στις 5 Αυγούστου 2015.

Ερευνητικά ερωτήματα

- Αρχιτεκτονικές του SHA-3 σε FPGA
  - Ποιες είναι μέχρι σήμερα οι υπάρχουσες υλοποιήσεις;
- Τεχνικές επιτάχυνσης
  - Ποιες τεχνικές επιτάχυνσης βελτιώνουν το κρίσιμο μονοπάτι του αλγορίθμου;
  - Πώς επιτυγχάνεται υψηλή Ρυθμαπόδοση (throughput) και αποδοτικότητα (efficiency) σε FPGA;
- Συγκριτική αξιολόγηση αρχιτεκτονικών
  - Πώς συγκρίνονται με τις πλέον σύγχρονες υλοποιήσεις;
  - Ποια τα πλεονεκτήματα και οι περιορισμοί έναντι των υφιστάμενων λύσεων;
  - Πώς αξιολογούνται ως προς ρυθμαπόδοση και αποδοτικότητα;

Ερευνητικοί στόχοι

- **Χαρτογράφηση υλοποιήσεων του SHA-3 σε FPGA**
  - Ανασκόπηση στρατηγικών και τεχνικών
  - Ανάλυση αρχιτεκτονικών προκλήσεων
- **Έρευνα προηγμένων μεθόδων επιτάχυνσης**
  - Βελτιστοποίηση κρίσιμου μονοπατιού με τεχνικές επιτάχυνσης
- **Ανάπτυξη στρατηγικών επιτάχυνσης & βελτιστοποίησης**
  - Εύρεση τεχνικών για ταχύτητα και αποδοτικότητα
  - Δημιουργία αρχιτεκτονικών με στόχο την υψηλή ρυθμαπόδοση
- **Ανάπτυξη υλοποιήσεων σε FPGA & συγκριτική αξιολόγηση**
  - Υλοποίηση SHA-3 με στόχο την μεγιστοποίηση της επιτάχυνσης και της αποδοτικότητας
  - Λεπτομερής αξιολόγηση και σύγκριση με σύγχρονες υλοποιήσεις
  - Συγκριτικό πλαίσιο επιλογής βέλτιστης προσέγγισης

Βιβλιογραφική ανασκόπηση και προτεινόμενη προσέγγιση

- **Αρχική φάση έρευνας:**
  Συστηματική βιβλιογραφική ανασκόπηση σε υλοποιήσεις του SHA-3 σε FPGA και τεχνικές επιτάχυνσης του κρίσιμου μονοπατιού
- **Ευρήματα:**
  - Έρευνα με πειραματικές εφαρμογές του αλγόριθμου SHA-3 σε FPGA
  - Τεχνικές επιτάχυνσης σε υλικό pipelining και loop unrolling

- **Ανάπτυξη προτεινόμενης προσέγγισης:**
  Σχεδίαση τριών τεχνικών επιτάχυνσης: pipelining, loop unrolling και συνδυασμός αυτών
- **Επικύρωση μέσω πειραμάτων**:
  - Υλοποίηση των προτεινόμενων αρχιτεκτονικών σε πλακέτες FPGA της εταιρίας Xillix (Virtex-5, Virtex-6 και Virtex-7)
  - Χρήση ποσοτικών και ποιοτικών μετρήσεων για σύγκριση: ρυθμαπόδοση (throughput), συχνότητα λειτουργίας (frequency), αποδοτικότητα (efficiency) και χρήση πόρων υλικού (area σε slices)

$$Throughput_{Fpga} = \frac{Bitrate\ size\ "r"}{Total\ clock\ cycles} \times Frequency\ maximum\ clock$$

$$Efficiency_{Fpga} = \frac{Throughput_{Fpga}}{Area_{Fpga}}$$

Βασική υλοποίηση του αλγορίθμου SHA-3 σε FPGA

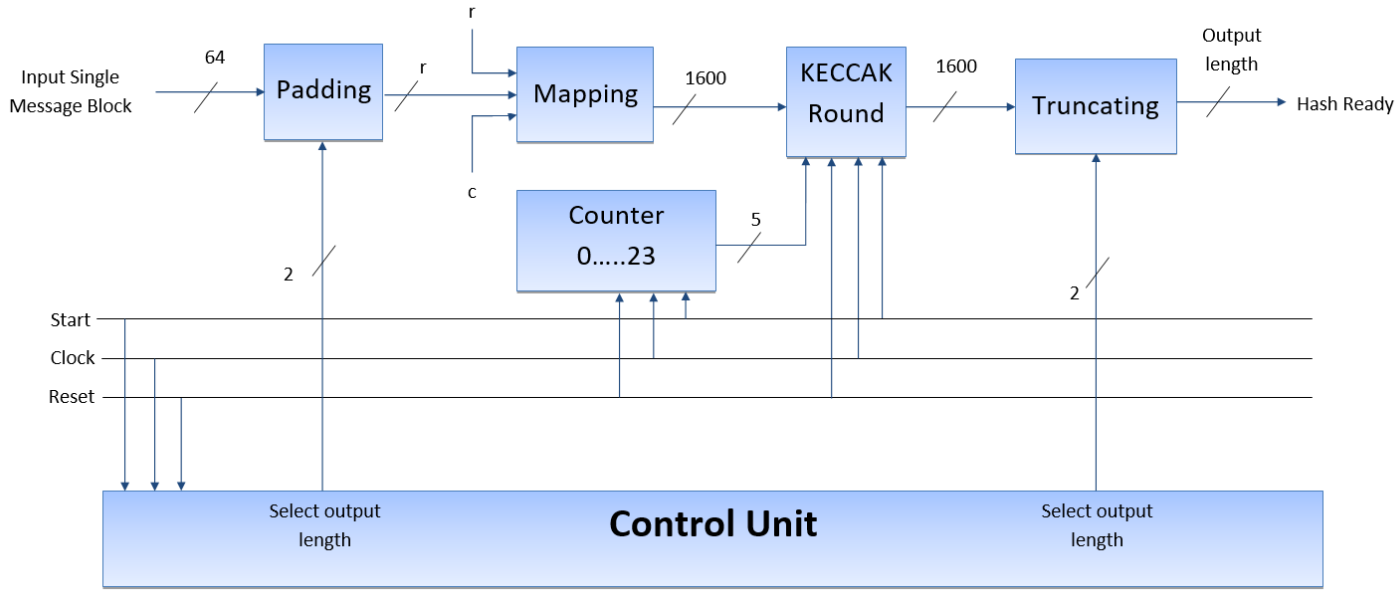
Padding
- Κατάτμηση του μηνύματος σε block size μήκους r *(προσθήκη bits αν χρειάζεται, ώστε να ταιριάζει στο block size r={1152, 1088, 832, 576}).*

Mapping
- Προσθήκη στο bloke size r το capacity c (c={448, 512, 768, 1024}) .

KECCAK Round
- Εκτέλεση 24 γύρων μετασχηματισμών με τα 5 βήματα ***θ, ρ, π, χ*** *και* ***ι***.
- Χρήση μετρητή γύρων για έλεγχο της ακολουθίας.

Truncating
- Απόσπαση από τα r bits από την εσωτερική κατάσταση των 1600 bit.
- Προσαρμογή στο επιθυμητό μήκος εξόδου (π.χ. 224, 256, 384, 512 bits).

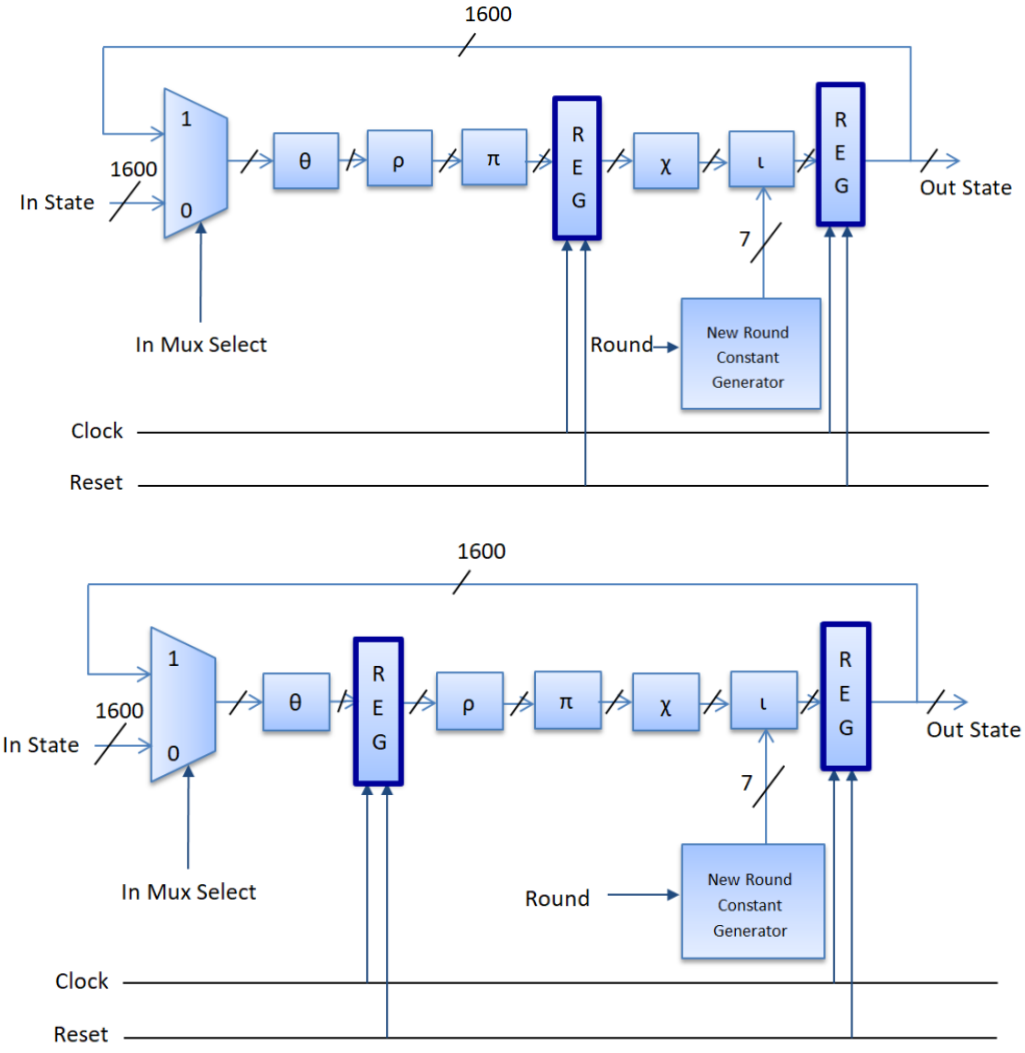
Control Unit
- Διαχείριση λειτουργίας: Start/Reset/Clock.
- Επιλογή μήκους εξόδου και σηματοδότηση "Hash Ready".



Τεχνική επιτάχυνσης με pipelining του SHA-3 σε FPGA (1/2)

Τεχνικές με τοποθέτηση pipeline για την μείωση του κρίσιμου μονοπατιού:

- Τεχνική 1: Pipeline στο βήμα ***π***
- Τεχνική 2: Pipeline στο βήμα ***θ***



Τεχνική επιτάχυνσης με pipelining του SHA-3 σε FPGA (2/2)

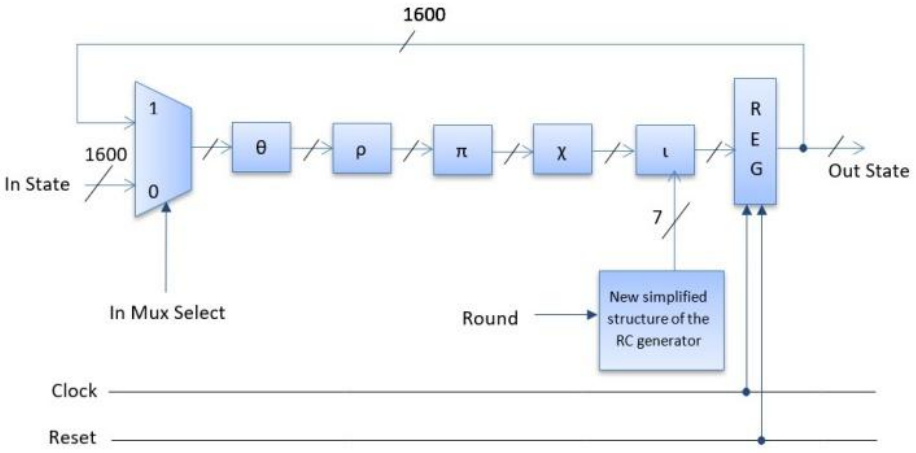
- Συχνότητα & Ρυθμαπόδοση
  - Η δεύτερη τεχνική επιτυγχάνει υψηλότερες συχνότητες λειτουργίας και βελτιωμένη ρυθμαπόδοση
- Αποδοτικότητα (Mbps/slices)
  - Η δεύτερη τεχνική έχει καλύτερη αξιοποίηση πόρων
- Συνολική Αξιολόγηση
  - Το pipelining στο βήμα θ προσφέρει καλύτερο συμβιβασμό μεταξύ κατανάλωσης πόρων, ρυθμαπόδοσης και αποδοτικότητας
  - Το pipelining στο βήμα π εξακολουθεί να είναι ανταγωνιστικό, αλλά απαιτεί μεγαλύτερη επιφάνεια

Σχεδίαση	FPGA	Επιφάνεια σε slices	Συχνότητα (MHz)	Ρυθμαπόδοση (Gbps) r= 1152	Ρυθμαπόδοση (Gbps) r = 1088	Ρυθμαπόδοση (Gbps) r = 832	Ρυθμαπόδοση (Gbps) r = 576
[146]	Virtex-5	2326	306	-	-	-	5,56
[147]	Virtex-5	4793	317,11	-	12,68	-	-
[148]	Virtex-5	1163	273	-	-	-	7,80
[149]	Virtex-5	2652	352	-	-	-	8,44
	Virtex-6	2296	391	-	-	-	9,38
[150]	Virtex-5	1702	389	-	18,07	-	-
	Virtex-6	1649	397	-	19,01	-	-
	Virtex-7	1618	434	-	20,80	-	-
[151]	Virtex-5	2123	-	-	12,523	-	7,380
	Virtex-6	1456	-	-	14,942	-	8,114
[152]	Stratix IV	5363	110	-	-	-	-
[153]	Virtex-5	1680	387	-	-	-	8,06
Προτεινόμενη τεχνική βελτιστοποίησης με διασωλήνωση στο βήμα θ	Virtex-5	998	402	19,29	18,22	13,93	9,64
Προτεινόμενη τεχνική βελτιστοποίησης με διασωλήνωση στο βήμα θ	Virtex-6	1042	422	20,25	19,13	14,62	10,12
Προτεινόμενη τεχνική βελτιστοποίησης με διασωλήνωση στο βήμα θ	Virtex-7	1150	478	22,94	21,66	16,57	11,47

Σχεδίαση	FPGA	Επιφάνεια σε slices	Συχνότητα (MHz)	Αποδοτικότητα (Mbps/slices) r = 1152	Αποδοτικότητα (Mbps/slices) r = 1088	Αποδοτικότητα (Mbps/slices) r = 832	Αποδοτικότητα (Mbps/slices) r = 576
[146]	Virtex-5	2326	306	-	-	-	2,40
[147]	Virtex-5	4793	317,11	-	2,71	-	-
[148]	Virtex-5	1163	273	-	-	-	6,06
[149]	Virtex-5	2652	352	-	-	-	6,37
	Virtex-6	2296	391	-	-	-	8,17
[150]	Virtex-5	1702	389	-	10,98	-	-
	Virtex-6	1649	397	-	11,60	-	-
	Virtex-7	1618	434	-	12,90	-	-
[151]	Virtex-5	2123	-	-	5,90	-	4,16
	Virtex-6	1456	-	-	10,26	-	6,42
[152]	Stratix IV	5363	110	-	-	-	-
[153]	Virtex-5	1680	387	-	-	-	4,91
Προτεινόμενη τεχνική βελτιστοποίησης με διασωλήνωση στο βήμα θ	Virtex-5	998	402	19,33	18,26	13,96	9,67
Προτεινόμενη τεχνική βελτιστοποίησης με διασωλήνωση στο βήμα θ	Virtex-6	1042	422	19,44	18,36	14,04	9,72
Προτεινόμενη τεχνική βελτιστοποίησης με διασωλήνωση στο βήμα θ	Virtex-7	1150	478	19,95	18,84	14,41	9,98

Argyrios Sideris and Minas Dasygenis. Enhancing the Hardware Pipelining Optimization Technique of the SHA-3 via FPGA. Computation, MDPI, 11(8):152, 2023.

Τεχνική επιτάχυνσης με loop unrolling του SHA-3 σε FPGA (1/2)



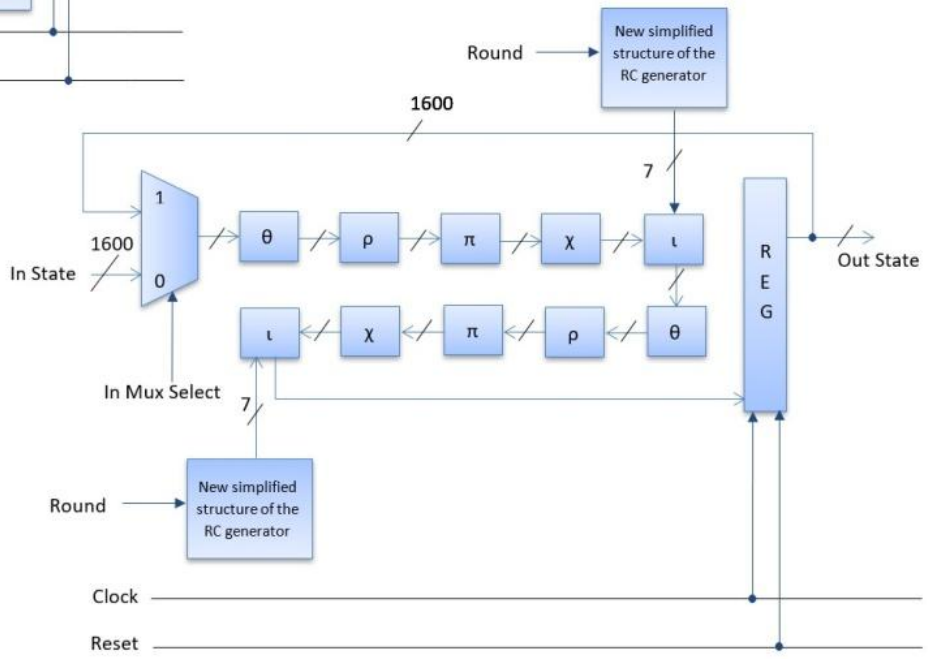
Υλοποίηση του SHA-3 χωρίς καμία τεχνική επιτάχυνσης

Τεχνική loop unrolling με σκοπό την μείωση του κρίσιμου μονοπατιού:
Μείωση χρόνου εκτέλεσης

- Από 24 κύκλους → 12 κύκλους
- Εκτέλεση 2 γύρων σε 1 κύκλο ρολογιού

Αυξημένη ρυθμαπόδοση

- Λιγότεροι κύκλοι → υψηλότερη συχνότητα εξόδου hash.



Τεχνική επιτάχυνσης με loop unrolling του SHA-3 σε FPGA (2/2)

Βελτίωση ρυθμαπόδοσης:
- Στα Virtex-6 και Virtex-7 παρατηρείται σημαντική αύξηση ρυθμαποδοσης

Μείωση χρόνου εκτέλεσης:
- Η εκτέλεση ολοκληρώνεται σε 12 κύκλους αντί για 24, χάρη στην παράλληλη υλοποίηση δύο γύρων ανά κύκλο.

Μείωση μέγιστης συχνότητας:
- Η συχνότητα μειώνεται λόγω της μεγαλύτερης πολυπλοκότητας ανά κύκλο, αλλά αντισταθμίζεται από τη μείωση κύκλων.

Αύξηση επιφάνεια σε slices:
- Η επιφάνεια σε slices αυξάνει, λόγω πιο σύνθετης λογικής.

Καλύτερη αποδοτικότητα:
- Παρά την αύξηση των slices, η αποδοτικότητα (Mbps/slices) είναι ανώτερη

Η αρχιτεκτονική με 12 κύκλους πετυχαίνει υψηλότερη ρυθμαπόδοση και καλύτερη αποδοτικότητα, με συμβιβασμό σε συχνότητα λειτουργίας και επιφάνεια.

Σχεδιασμός	Συσκευή FPGA	Κύκλοι ρολογιού	Μέγιστη Συχνότητα (Mhz)	Ρυθμαπόδοση (r = 1152)	Ρυθμαπόδοση (r = 1088)	Ρυθμαπόδοση (r = 832)	Ρυθμαπόδοση (r = 576)
[183]	Virtex-5	24	277	-	12,56	-	6,48
	Virtex-7	24	300	-	13,60	-	7,17
[184]	Artix-7	24	390,53	-	-	-	16,492
		12	234,97	-	-	-	19,99
[144]	Virtex-6	24	153	-	-	-	3,68
		12	344	-	-	-	16,51
[185]	Virtex-5	24	111,732	-	4,67	-	-
		16	84,21	-	5,38	-	-
[143]	Virtex-5	24	326,38	15,66	14,79	11,31	7,83
		12	192,25	18,45	17,43	13,32	9,228
	Virtex-6	24	413,77	19,86	18,75	14,34	9,93
		12	232,45	22,31	21,07	16,11	11,15
[186]	Virtex-7	24	374,035	-	-	-	7,979
[187]	Virtex-5	24	338,409	15,86	15,34	11,73	8,12
	Virtex-6	24	376,081	17,63	17,05	13,04	9,02
[153]	Virtex-5	24	387	-	-	-	8,06
Παρούσα εργασία	Virtex-5	24	347,49	16,680	15,753	12,046	8,340
		12	203,28	19,515	18,431	14,094	9,757
	Virtex-6	24	438,49	21,048	19,878	15,201	10,524
		12	347,84	33,393	31,537	24,117	16,696
	Virtex-7	24	498,27	23,917	22,588	17,273	11,958
		12	378,73	36,358	34,338	26,259	18,179
	Artix-7	24	397,41	19,075	18,015	13,776	9,537
		12	254,46	24,428	23,071	17,642	12,214

Σχεδιασμός	Συσκευή FPGA	Κύκλοι ρολογιού	Επιφάνεια (συνολικός αριθμός από slices)	Αποδοτικότητα (r = 1152)	Αποδοτικότητα (r = 1088)	Αποδοτικότητα (r = 832)	Αποδοτικότητα (r = 576)
[183]	Virtex-5	24	1217	-	10,31	-	5,4
	Virtex-7	24	998	-	13,63	-	7,27
[184]	Artix-7	24	4188	-	-	-	3,93
		12	7139	-	-	-	2,80
[144]	Virtex-6	24	871	-	-	-	4,22
		12	1406	-	-	-	11,47
[185]	Virtex-5	24	1434	-	3,32	-	-
		16	1562	-	3,44	-	-
[143]	Virtex-5	24	1365	11,47	10,83	8,28	5,73
		12	2144	8,60	8,13	6,21	4,30
	Virtex-6	24	1432	13,87	13,10	10,02	6,93
		12	3557	6,27	5,93	4,53	3,14
[186]	Virtex-7	24	1454	-	-	-	5,49
[187]	Virtex-5	24	935	16,96	16,40	12,54	8,68
	Virtex-6	24	1019	17,30	16,73	12,80	8,85
[153]	Virtex-5	24	1680	-	-	-	4,91
Παρούσα εργασία	Virtex-5	24	868	19,22	18,15	13,88	9,61
		12	1112	17,55	16,57	12,67	8,77
	Virtex-6	24	946	22,25	21,01	16,07	11,12
		12	1287	25,95	24,50	18,74	12,97
	Virtex-7	24	1094	21,86	20,65	15,79	10,93
		12	1375	26,44	24,97	19,10	13,22
	Artix-7	24	902	21,14	19,97	15,27	10,57
		12	1184	20,63	19,48	14,90	10,31

Argyrios Sideris, Theodora Sanida, and Minas Dasygenis. Hardware acceleration design of the SHA-3 for high throughput and low area on FPGA. Journal of Cryptographic Engineering, Springer Nature, pages 1–13, 2024.

Τεχνική επιτάχυνσης με pipelining και loop unrolling του SHA-3 σε FPGA (1/2)

Pipelining:

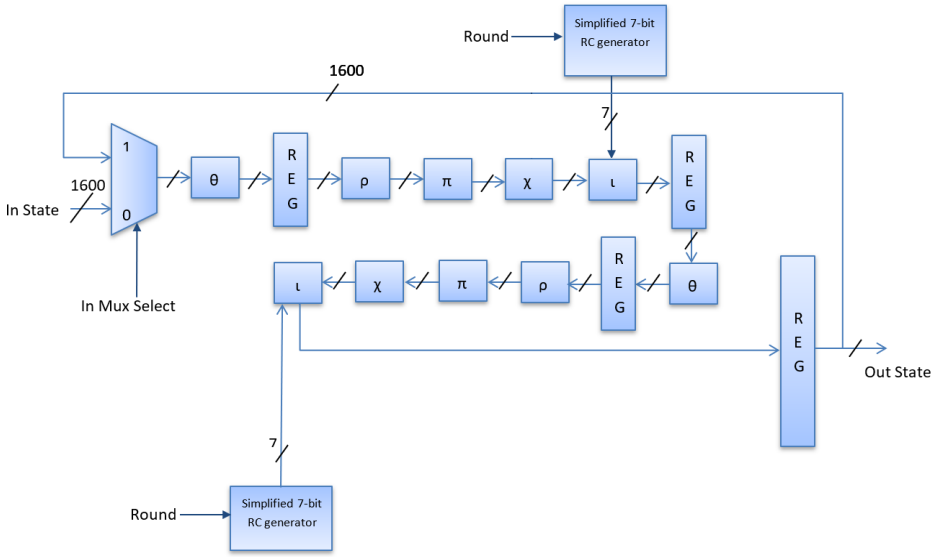
- στο βήμα θ → καλύτερη ισορροπία απόδοσης & πόρων
- Μείωση κρίσιμης διαδρομής → υψηλότερη συχνότητα λειτουργίας.

Loop Unrolling:

- Επιτυγχάνεται μεγαλύτερος βαθμός παραλληλίας.
- Μείωση κύκλων για την ολοκλήρωση του αλγορίθμου.
- Αυξημένη κατανάλωση πόρων (LUTs, FFs, slices).

Συνδυασμός τεχνικών:

- Βελτίωση ρυθμαπόδοσης και συχνότητας λειτουργίας.
- Αποτελεσματική αξιοποίηση υλικού.



Τεχνική επιτάχυνσης με pipelining και loop unrolling του SHA-3 σε FPGA (2/2)

Αύξηση συχνότητας λειτουργίας:
- Οι υλοποιήσεις σε σύγχρονης τεχνολογίας FPGA επιτυγχάνουν υψηλότερες συχνότητες.

Αύξηση ρυθμαπόδοσης (throughput):
- Σημαντική βελτίωση με αύξηση του μεγέθους μπλοκ (r).

Βελτίωση αποδοτικότητας (efficiency):
- Δείχνει θετική αντιστάθμιση μεταξύ ρυθμαπόδοσης και επιφάνειας (slices).

Συμβιβασμός επιφάνειας – επιδόσεων:
- Αύξηση της επιφάνειας (slices) απαιτείται για μεγαλύτερο r, αλλά οδηγεί σε υψηλότερη απόδοση.

Σχεδίαση	FPGA	Επιφάνεια σε slices	Συχνότητα (MHz)	Ρυθμαπόδοση (Gbps) r – 576	Αποδοτικότητα (Mbps/Slices) r – 576
[153]	Virtex-5	1680	387	8,06	4,91
[186]	Virtex-7	1454	374,035	7,979	5,49
[209]	Virtex-5	1409	377,86	8,22	5,83
	Virtex-6	1227	424,44	10,19	8,30
[210]	Virtex-5	1388	287,39	11,50	8,48
	Virtex-6	1167	394,01	15,76	13,83
	Virtex-7	1418	414,54	16,58	11,97
[149]	Virtex-5	2652	352	8,44	6,37
	Virtex-6	2296	391	9,38	8,17
[146]	Virtex-5	2326	306	5,56	2,40
[148]	Virtex-5	1163	273	7,80	6,06
Προτεινόμενος	Virtex-5	1186	272,41	13,076	11,03
	Virtex-6	1348	344,62	16,542	12,27
	Virtex-7	1452	396,28	19,021	13,10

Η τεχνική με pipelining και loop unrolling βελτιστοποιεί σημαντικά τη ρυθμαπόδοση και την αποδοτικότητα, προσφέροντας μια ισχυρή λύση για απαιτητικές κρυπτογραφικές εφαρμογές.

Argyrios Sideris, Theodora Sanida, and Minas Dasygenis. A Novel Hardware Architecture for Enhancing the Keccak Hash Function in FPGA Devices. Information, MDPI, 14(9):475, 2023.

Συμπεράσματα

- **Βελτίωση συχνότητας λειτουργίας**
  - Όλες οι τεχνικές αυξάνουν τη συχνότητα
  - Καλύτερη απόδοση: pipelining στο βήμα θ
- **Κατανάλωση πόρων**
  - Pipelining στο βήμα θ → λιγότεροι πόροι (πιο αποδοτική χρήση slices)
  - Loop unrolling → μεγαλύτερη απαίτηση σε πόρους
- **Αύξηση ρυθμαπόδοσης**
  - Σημαντική βελτίωση και στις τρεις τεχνικές
  - Καλύτερη: pipelling & loop unrolling
- **Βελτίωση αποδοτικότητας (Mbps/slices)**
  - Υψηλότερη με pipelling & loop unrolling
- **Συνολική επίδραση**
  - Όλες οι τεχνικές αυξάνουν ρυθμαπόδοση & αποδοτικότητα
  - Ο σωστός συνδυασμός οδηγεί σε μέγιστη βελτιστοποίηση

Μελλοντικοί στόχοι

- **Επεκτάσεις**
  Εφαρμογή των προτεινόμενων βελτιστοποιήσεων και σε άλλους αλγορίθμους

- **Βελτιστοποίηση με νέες τεχνικές**
  - Η τεχνητή νοημοσύνη μπορεί να χρησιμοποιηθεί για αυτόματη επιλογή βέλτιστων αρχιτεκτονικών ή για πρόβλεψη της απόδοσης σε FPGA.
  - Χρήση machine learning για να βελτιστοποιηθεί το pipelining και το loop unrolling χωρίς χειροκίνητο tuning.

- **Μείωση κατανάλωσης ενέργειας**
  Σχεδίαση αρχιτεκτονικών με χαμηλή ενεργειακή κατανάλωση χωρίς μείωση των επιδόσεων.

Δημοσιεύσεις - Περιοδικά

- **[Π1] Sideris, A.**, Sanida, T., & Dasygenis, M. (2024). *Hardware acceleration design of the SHA-3 for high throughput and low area on FPGA*. Journal of Cryptographic Engineering, Springer Nature, 1-13.**(Q2)**
- **[Π2]** Sanida, T., Sanida, M. V., **Sideris, A.**, & Dasygenis, M. (2024). *Enhancing Pulmonary Diagnosis in Chest X-rays through Generative AI Techniques*. J, MDPI, 7(3), 302-318.
- **[Π3]** Sanida, M. V., Sanida, T., **Sideris, A.**, & Dasygenis, M. (2024). *An advanced deep learning framework for multi-class diagnosis from chest X-ray images*. J, MDPI, 7(1), 48-71.
- **[Π4]** Sanida, T., Sanida, M. V., **Sideris, A.**, & Dasygenis, M. (2024). *Optimizing Lung Condition Categorization through a Deep Learning Approach to Chest X-ray Image Analysis*. BioMedInformatics, MOPI, 4(3), 2002-2021.**(Q2)**
- **[Π5]** Sanida, T., **Sideris, A.**, Sanida, M. V., & Dasygenis, M. (2023). *Tomato leaf disease identification via two–stage transfer learning approach*. Smart Agricultural Technology, Elsevier, 5, 100275. **(Q1)**
- **[Π6] Sideris, A.**, Sanida, T., & Dasygenis, M. (2023). *A Novel Hardware Architecture for Enhancing the Keccak Hash Function in FPGA Devices*. Information, MDPI, 14(9), 475.**(Q2)**
- **[Π7] Sideris, A.** & Dasygenis, M. (2023). *Enhancing the Hardware Pipelining Optimization Technique of the SHA-3 via FPGA*. Computation, MDPI, 11(8), 152.**(Q2)**
- **[Π8]** Sanida, T., Tabakis, I. M., Sanida, M. V., **Sideris, A.**, & Dasygenis, M. (2023). *A Robust Hybrid Deep Convolutional Neural Network for COVID-19 Disease Identification from Chest X-ray Images*. Information, MDPI, 14(6), 310.**(Q2)**
- **[Π9]** Sanida, M. V., Sanida, T., **Sideris, A.**, & Dasygenis, M. (2023). *An Efficient hybrid CNN classification model for tomato crop disease*. Technologies, MDPI, 11(1), 10.**(Q1)**
- **[Π10] Sideris, A.**, Sanida, T., Tsiktsiris, D., & Dasygenis, M. (2022). *Acceleration of Image Processing with SHA-3 (Keccak) Algorithm using FPGA*. Journal of Engineering Research and Sciences, JENRS, 1, 20-28.
- **[Π11]** Sanida, T., Tsiktsiris, D., **Sideris, A.**, & Dasygenis, M. (2022). *A heterogeneous implementation for plant disease identification using deep learning*. Multimedia Tools and Applications, Springer Nature, 81(11), 15041-15059.**(Q1)**
- **[Π12]** Sanida, T., **Sideris, A.**, Tsiktsiris, D., & Dasygenis, M. (2022). *Lightweight neural network for COVID-19 detection from chest X-ray images implemented on an embedded system*. Technologies, MDPI, 10(2), 37.**(Q1)**
- **[Π13] Sideris, A.**, Sanida, T., & Dasygenis, M. (2020). *High throughput implementation of the Keccak hash function using the Nios-II processor*. Technologies, MDPI, 8(1), 15.**(Q1)**

Δημοσιεύσεις - Συνέδρια

- **[Σ1]** Sanida, T., **Sideris, A.**, Sanida, M. V., Dossis, M., & Dasygenis, M. (2024, September). *Accelerating CNNs for Pneumonia Disease Diagnosis via Heterogeneous FPGA Systems*. In 2024 9th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM) (pp. 159-162). IEEE.
- **[Σ2]** Sanida, M. V., Sanida, T., **Sideris, A.**, Dossis, M., & Dasygenis, M. (2024, September). *Fake News Detection Approach Using Hybrid Deep Learning Framework*. In 2024 9th SEEDA-CECNSM (pp. 81-84). IEEE.
- **[Σ3]** Sanida, T., **Sideris, A.**, Sanida, M. V., Dossis, M., & Dasygenis, M. (2023, November). *An Efficiency CNN Solution for Olive Disease Management Through FPGA*. In 2023 8th SEEDA-CECNSM (pp. 1-4). IEEE.
- **[Σ4]** Sanida, T., Sanida, M. V., **Sideris, A.**, Dossis, M., & Dasygenis, M. (2023, November). *Efficient Categorization of Pneumonia Diagnosis Using Low-Power Embedded Devices*. In 2023 8th SEEDA-CECNSM (pp. 1-4). IEEE.
- **[Σ5] Sideris, A.**, Sanida, T., Sanida, M. V., Dossis, M., & Dasygenis, M. (2023, November). *Accelerate Processing of Image with the Keccak-512 Algorithm on Cryptoprocessor*. In 2023 8th SEEDA-CECNSM (pp. 1-4). IEEE.
- **[Σ6]** Sanida, T., **Sideris, A.**, Sanida, M. V., Dossis, M., & Dasygenis, M. (2023, November). *Acceleration of GANs for Potato Crop Disease Identification via FPGA*. In 2023 8th SEEDA-CECNSM (pp. 1-4). IEEE.
- **[Σ7]** Sanida, T., Sanida, M. V., **Sideris, A.**, & Dasygenis, M. (2023, June). *A Lightweight CNN Model for Tomato Crop Diseases on Heterogeneous Embedded System*. In 2023 12th MOCAST (pp. 1-4). IEEE.
- **[Σ8]** Sanida, T., **Sideris, A.**, Chatzisavvas, A., Dossis, M., & Dasygenis, M. (2022, September). *Radiography Images with Transfer Learning on Embedded System*. In 2022 7th SEEDA-CECNSM (pp. 1-4). IEEE.
- **[Σ9] Sideris, A.**, Sanida, T., Chatzisavvas, A., Dossis, M., & Dasygenis, M. (2022, September). High Throughput of Image Processing with Keccak Algorithm using Microprocessor on FPGA. In 2022 7th SEEDA-CECNSM (pp. 1-4). IEEE.
- **[Σ10] Sideris, A.**, Sanida, T., Tsiktsiris, D., & Dasygenis, M. (2022). Image hashing based on SHA-3 implemented on FPGA. In Recent Advances in Manufacturing Modelling and Optimization: Select Proceedings of RAM 2021 (pp. 521-530). Springer, Singapore.
- **[Σ11]** Tsiktsiris, D., Sanida, T., **Sideris, A.**, & Dasygenis, M. (2022). *Accelerated Defective Product Inspection on the Edge Using Deep Learning*. In *Recent Advances in Manufacturing Modelling and Optimization: Select Proceedings of RAM 2021* (pp. 185-191). Springer, Singapore.
- **[Σ12]** Sanida, T., Tsiktsiris, D., **Sideris, A.**, & Dasygenis, M. (2021, July). *A Heterogeneous Lightweight Network for Plant Disease Classification*. In 2021 10th MOCAST (pp. 1-4). IEEE.
- **[Σ13] Sideris, A.**, Sanida, T., & Dasygenis, M. (2020, December). *High throughput pipelined implementation of the SHA-3 cryptoprocessor*. In 2020 32nd ICM (pp. 1-4). IEEE.
- **[Σ14]** Sanida, T., **Sideris, A.**, & Dasygenis, M. (2020, September). *Accelerating the AES algorithm using OpenCL*. In 2020 9th MOCAST (pp. 1-4). IEEE.
- **[Σ15]** Sanida, T., **Sideris, A.**, & Dasygenis, M. (2020, September). *A heterogeneous implementation of the Sobel edge detection filter using OpenCL*. In 2020 9th MOCAST (pp. 1-4). IEEE.
- **[Σ16] Sideris, A.**, Sanida, T., & Dasygenis, M. (2019, November). *Hardware acceleration of the AES algorithm using Nios-II processor*. In 2019 PACET (pp. 1-5). IEEE.
- **[Σ17] Sideris, A.**, Sanida, T., & Dasygenis, M. (2019, May). *Hardware acceleration of SHA-256 algorithm using Nios-II processor*. In 2019 8th MOCAST (pp. 1-4). IEEE.

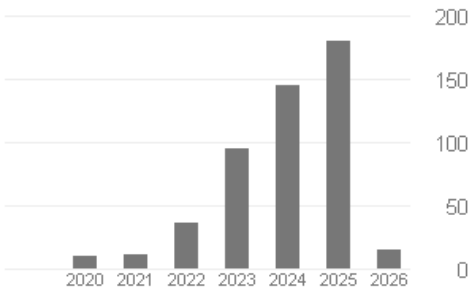
Δημοσιεύσεις - Κεφάλαια Βιβλίων

- **[KB1] Sideris, A.,** Tsiktsiris, D., Ziouzios, D. and Dasygenis, M. (2019). Smart grid hardware security. IoT for Smart Grids: Design Challenges and Paradigms, 85-113.
- **[KB2]** Ziouzios, D., **Sideris, A.,** Tsiktsiris, D. and Dasygenis, M. (2019). Smart-Grid Modelling and Simulation. IoT for Smart Grids: Design Challenges and Paradigms, 43-54.

Google Μελετητής

Παρατίθεται από

	Όλα	Από το 2021
Παραθέσεις	501	488
h-index	13	13
i10-index	15	15



Ευχαριστώ για την προσοχή σας