ΟΝΟΜΑ ΕΠΙΘΕΤΟ : ΑΘΑΝΑΣΙΟΣ ΚΑΚΑΡΟΥΝΤΑΣ

Ι. ΠΡΟΣΩΠΙΚΑ ΣΤΟΙΧΕΙΑ

Ημερομηνία γέννησης:	26 Ιουνίου 1973
Τόπος γέννησης:	Λαμία
Διεύθυνση εργασίας:	Φιλοσόφων & Τζεβελέκη, τ.κ. 31100, Λευκάδα
Διεύθυνση κατοικίας:	Οίκημα Παρούση, τ.κ. 31100, Άγιος Ιωάννης, Λευκάδα
Οικογενειακή κατάσταση:	Έγγαμος με 3 παιδιά
Στρατιωτική θητεία:	Εκπληρωμένη

ΙΙ. ΣΠΟΥΔΕΣ

26/06/2009 - σήμερα:	Μεταπτυχιακός φοιτητής στο Μεταπτυχιακό πρόγραμμα σπουδών «Διοίκηση Επιχειρήσεων-MBA» του Ανοικτού Πανεπιστημίου Κύπρου.
2/2004 - 5/2007:	Υπότροφος Μετα - Διδάκτωρ (Ερευνητής) του Τμήματος Ηλεκτρολόγων Μηχ. και Τεχν. Υπολ. του Πανεπιστημίου Πατρών, Εργ. Σχεδιασμού Ολοκληρωμένων Κυκλωμάτων.
17/02/2004:	Διδάκτωρ του Τμήματος Ηλεκτρολόγων Μηχ. και Τεχν. Υπολ. του Πανεπιστημίου Πατρών, Εργ. Σχεδιασμού Ολοκληρωμένων Κυκλωμάτων. Τίτλος Διατριβής: "Σχεδιασμός κυκλωμάτων ασφαλούς λειτουργίας και χαμηλής κατανάλωση ισχύος "
23/07/1998:	Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Τεχνολογίας Υπολογιστών. από το Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών του Πανεπιστημίου Πατρών.

ΙΙΙ. ΑΚΑΔΗΜΑΪΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ

1. ΑΚΑΔΗΜΑΪΚΕΣ ΘΕΣΕΙΣ

2012-σήμερα	Επίκουρος Καθηγητής στο ΤΕΙ Ιονίων Νήσων, Τμήμα Διοίκησης Επιχειρήσεων (πρώην Τμήμα Εφαρμογών Πληροφορικής στη Διοίκηση και στην Οικονομία - Λευκάδα), ΦΕΚ 1123/τ. Γ'/22-12-2011. Γνωστικό αντικείμενο «***Αρχιτεκτονική Ενσωματωμένων Υπολογιστικών Συστημάτων***»

2. ΔΙΔΑΚΤΙΚΗ ΕΜΠΕΙΡΙΑ

Διδασκαλία μαθημάτων πριν από τη λήψη του Διδακτορικού Διπλώματος:

α. Εργαστηριακές ασκήσεις του μαθήματος «Σχεδιασμός Ολοκληρωμένων Κυκλωμάτων Ι» (7ο εξάμηνο) (Ακαδημαϊκό έτος 1999-01)

β. Εργαστηριακές ασκήσεις του μαθήματος «Σχεδιασμός Ολοκληρωμένων Κυκλωμάτων ΙΙ» (8ο εξάμηνο) (Ακαδημαϊκό έτος 1999-01)

γ. Εργαστηριακές ασκήσεις του μαθήματος «Σχεδιασμός Ολοκληρωμένων Συστημάτων με Τεχνικές VLSI» (9ο εξάμηνο) (Ακαδημαϊκό έτος 1999-01)

δ. Φροντιστηριακές ασκήσεις του μαθήματος «Σχεδιασμός Ολοκληρωμένων Κυκλωμάτων Ι» (7ο εξάμηνο) (Ακαδημαϊκό έτος 2003-2004)

ε. Διαλέξεις στα πλαίσια του μαθήματος «Σχεδιασμός Ολοκληρωμένων Κυκλωμάτων ΙΙ» (8ο εξάμηνο) (Ακαδημαϊκό έτος 2003-2004)

στ. Διαλέξεις στα πλαίσια του μαθήματος «Σχεδιασμός Ολοκληρωμένων Συστημάτων με Τεχνικές VLSI» (9ο εξάμηνο) (Ακαδημαϊκό έτος 2003-2004)

Διδασκαλία μαθημάτων μετά τη λήψη του Διδακτορικού Διπλώματος:

ΠΡΩΤΟΥ ΚΥΚΛΟΥ ΣΠΟΥΔΩΝ

Τμήμα Πληροφορικής με εφαρμογές στη Βιοϊατρική, Πανεπιστήμιο Θεσσαλίας

Αρχιτεκτονική Η/Υ (3ο εξάμηνο): Αριθμητικά συστήματα, Τύποι δεδομένων, Εντολές, Υπολογισμός απόδοσης, Υπολογιστικές μηχανές, Κεντρική Μονάδα Επεξεργασίας, Αρχείο Καταχωρητών, Αριθμητική και Λογική Μονάδα, Αρτηρίες, Διακοπές, Pipeline, Μνήμη, Ιεραρχία μνήμης, Κρυφή Μνήμη, Ιδεατή μνήμη, Περιφερειακά, Οδηγοί περιφερειακών, Παραλληλισμός, Σύγχρονα θέματα Αρχιτεκτονικής (Χειμερινό εξάμηνο 2013-2014)

Τμήμα Πληροφορικής με εφαρμογές στη Βιοϊατρική, Πανεπιστήμιο Κευτρικής Ελλάδας

Αρχιτεκτονική Η/Υ (3ο εξάμηνο): Αριθμητικά συστήματα, Τύποι δεδομένων, Εντολές, Υπολογισμός απόδοσης, Υπολογιστικές μηχανές, Κεντρική Μονάδα Επεξεργασίας, Αρχείο Καταχωρητών, Αριθμητική και Λογική Μονάδα, Αρτηρίες, Διακοπές, Pipeline, Μνήμη, Ιεραρχία μνήμης, Κρυφή Μνήμη, Ιδεατή μνήμη, Περιφερειακά, Οδηγοί περιφερειακών, Σύγχρονα θέματα Αρχιτεκτονικής (Χειμερινό εξάμηνο 2006, 2007, 2008, 2009, 2010, 2011, 2012)

Τμήμα Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών, Τ.Ε.Ι. Ιονίων Νήσων

Αρχιτεκτονική Η/Υ (2ο εξάμηνο): Αριθμητικά συστήματα, Τύποι δεδομένων, Εντολές, Υπολογισμός απόδοσης, Υπολογιστικές μηχανές, Κεντρική Μονάδα Επεξεργασίας, Αρχείο Καταχωρητών, Αριθμητική και Λογική Μονάδα, Αρτηρίες, Διακοπές, Pipeline, Μνήμη, Ιεραρχία μνήμης, Κρυφή Μνήμη, Ιδεατή μνήμη, Περιφερειακά, Οδηγοί περιφερειακών, Σύγχρονα θέματα Αρχιτεκτονικής (Εαρινό εξάμηνο 2009, 2010, 2011, 2012)

Ψηφιακή Σχεδίαση (1ο εξάμηνο) : Συστήματα αρίθμησης, Δυαδική λογική, Άλγεβρα Boole, Απλοποίηση συναρτήσεων, Συνδυαστικά κυκλώματα, σύνθετα κυκλώματα, Ακολουθιακά κυκλώματα, Σύγχρονα κυκλώματα, Ασύγχρονα κυκλώματα, μανδαλωτές, καταχωρητές, μηχανές πεπερασμενων καταστάσεων, ολισθητές, απαριθμητές, παράλληλη / σειριακή φόρτωση, Αριθμητικά (Χειμερινό εξάμηνο 2009, 2010, 2011, 2012)

Ενσωματωμένα Συστήματα (5ο εξάμηνο): Σχεδίαση και ανάπτυξη ενσωματωμένων συστημάτων, Formal methods, Επεξεργαστές, Επιταχυντές υλικού (hardware accelerators), πλατφόρμες ανάπτυξης, πρωτόκολλα επικοινωνίας, λειτουργικά συστήματα, περιφερειακά, χρονοπρογραμματισμός, Περιφερειακά, Οδηγοί περιφερειακών, Μνήμη, προσομοίωση, πρωτοτυποποίηση, Σχεδίαση για υψηλή απόδοση, Σχεδίαση για χαμηλή κατανάλωση ενέργειας (Χειμερινό εξάμηνο 2012)

Ηλεκτρονική ΙΙ (Ψηφιακά Ηλεκτρονικά) (2ο εξάμηνο) : Ψηφιακά ολοκληρωμένα κυκλώματα (μονολιθικά, υβριδικά, πλεονεκτήματα ICs, ορισμός λογικής οικογένειας, λογικές οικογένειες,), γενικά χαρακτηριστικά. Λογική άμεσα συζευγμένων τρανζίστορ, λογική αντίστασης τρανζίστορ, λογική διόδου τρανζίστορ. Λογική τρανζίστορ-τρανζίστορ/ βασική σειρά, χαρακτηριστικά Schmitt trigger. Λογική συζευγμένου εκπομπού, Λογικές οικογένειες CMOS κυκλωμάτων. Διασύνδεση μεταξύ λογικών οικογενειών. Κυκλώματα χρονισμού (CMOS μονοσταθής πολυδονητής, ασταθής πολυδονητής, χρήση του 555, ταλαντωτές κρυστάλλου). (Εαρινό εξάμηνο 2012)

Τμήμα Μηχανικών Η/Υ και Πληροφορικής, Πανεπιστήμιο Πατρών
Μικροεπεξεργαστές – εργαστήριο (5ο εξάμηνο) : Προγραμματισμός περιφερειακών συσκευών, λειτουργία των διακοπών προγραμματισμό των χρονιστών (timers) ενός συστήματος, έξυπνοι αλγόριθμοι λειτουργιών και ελέγχου, διασύνδεση μικροϋπολογιστικών συστημάτων (Ακαδημαϊκά έτη 2006, 2007)

Τμήμα Πληροφορικής, Ελληνικό Ανοικτό Πανεπιστήμιο (Πρόγραμμα εξ αποστάσεως εκπαίδευσης)
ΠΛΗ21-Εργαστήριο Ψηφιακών Συστημάτων (ετήσια Θεματική Ενότητα) : Λογική Σχεδίαση, Αρχιτεκτονική Υπολογιστών, Μικροεπεξεργαστές (Ακαδημαϊκό έτος 2005-06)
ΠΛΗ21-Ψηφιακών Συστημάτων (ετήσια Θεματική Ενότητα) : Λογική Σχεδίαση, Αρχιτεκτονική Υπολογιστών, Μικροεπεξεργαστές (Ακαδημαϊκό έτος 2012-2013, 2013-2014)
ΠΛΗ40-Πτυχιακές (Ακαδημαϊκό έτος 2007-2008, 2008-2009)

Τμήμα Ηλεκτρονικής, ΤΕΙ Λαμίας (ως Επιστημονικός Συνεργάτης στη βαθμίδα Επίκουρου Καθηγητή)
Αρχιτεκτονική Η/Υ (4ο εξάμηνο): Αριθμητικά συστήματα, Τύποι δεδομένων, Εντολές, Υπολογισμός απόδοσης, Υπολογιστικές μηχανές, Κεντρική Μονάδα Επεξεργασίας, Αρχείο Καταχωρητών, Αριθμητική και Λογική Μονάδα, Αρτηρίες, Διακοπές, Pipeline, Μνήμη, Ιεραρχία μνήμης, Κρυφή Μνήμη, Ιδεατή μνήμη, Περιφερειακά, Οδηγοί περιφερειακών, Σύγχρονα θέματα Αρχιτεκτονικής (Εαρινό εξάμηνο 2007)

Μικροεπεξεργαστές-Μικροελεγκτές (6ο εξάμηνο) : Εξοικείωση με την δομή ενός Μικροεπεξεργαστή (Αριθμητική και Λογική Μονάδα, Μονάδες Προσκόμισης Εντολών, Αποκωδικοποίησης, Ελέγχου, Καταχωρητές). Μελέτη εναλλακτικών Διαύλων Συστήματος και τρόπους διασύνδεσης με Δυναμικές και Στατικές Μνήμες RAM, ROM, EEPROM, Flash κλπ. Εξετάζονται βασικές περιφερειακές μονάδες όπως Χρονιστές / Μετρητές, Παράλληλες και Σειριακές θύρες, Ελεγκτές Διακοπών, Απευθείας Προσπέλαση Μνήμης. Σύγκριση Συνόλων Εντολών διαφόρων Μικροεπεξεργαστών. Τρόποι διευθυνσιοδότησης. Μελέτη χρήσης ειδικών εντολών. Διασύνδεση και προγραμματισμός των περιφερειακών μονάδων. (Εαρινό εξάμηνο 2007)

Ιατρικά Ηλεκτρονικά (7ο εξάμηνο) : Τελεστικοί ενισχυτές, Κυκλώματα ειδικού σκοπού, Ενεργά φίλτρα, κυκλώματα επεξεργασίας σήματος, Μετατροπή αναλογικού σε ψηφιακό / ψηφιακό σε αναλογικό (Χειμερινό εξάμηνο 2005)

Τμήμα Πληροφορικής, ΤΕΙ Λαμίας (Πρόγραμμα εξ αποστάσεως εκπαίδευσης)
Σχεδίαση VLSI (Ακαδημαϊκό έτος 2006-07)
Ασφάλεια-Κρυπτογραφία (Ακαδημαϊκό έτος 2006-07)

Τμήμα Εφαρμογών Πληροφορικής στην Οικονομία και στη Διοίκηση, Τ.Ε.Ι. Ιονίων Νήσων
Ασφάλεια Πληροφοριακών Συστημάτων (5ο εξάμηνο) : Εισαγωγή στην Κρυπτογραφία: Ασύμμετρα και συμμετρικά κρυπτοσυστήματα. Επαλήθευση ταυτότητας. Μηχανισμοί Αυθεντικοποίησης. Ψηφιακές Υπογραφές. Έλεγχος Πρόσβασης: Λίστες Ελέγχου Πρόσβασης, Ετικέτες Ασφαλείας (MAC / DAC) και Έλεγχος Πρόσβασης με βάση το ρόλο του χρήστη. Ασφάλεια Υπολογιστών: Ασφάλεια από παράνομη αντιγραφή, Ιοί, Ασφάλεια προσωπικού υπολογιστή. Έννοιες Ασφάλειας Δικτύων: Υπηρεσίες και Μηχανισμοί Ασφάλειας (κατά ISO 7498-2) (Χειμερινό εξάμηνο 2008, 2009, 2010, 2011, 2012)

Δίκτυα Η/Υ ΙΙ (4ο εξάμηνο) : Θέματα σχεδίασης επιπέδου σύνδεσης δεδομένων: πλαισίωση, έλεγχος σφαλμάτων, έλεγχος ροής, διαχείριση σύνδεσης. Ανίχνευση και διόρθωση σφαλμάτων. Αλγόριθμοι ελέγχου συμφόρησης. Διασύνδεση δικτύων. Θέματα σχεδίασης επιπέδου μεταφοράς. Τα πρωτόκολλα μεταφοράς TCP/IP και UDP. Σύγκριση TCP/IP και OSI. Ανάλυση της απόδοσης ενός δικτύου με τη χρήση της Θεωρίας Ουρών. Ανάλυση καθυστέρησης. Μοντέλα για δίκτυα μεταγωγής κυκλώματος. Μοντέλα για δίκτυα μεταγωγής πακέτου. Εισαγωγή σε θέματα ποιότητας υπηρεσιών σε δίκτυα: το πρόβλημα της ευστάθειας δικτύων (Εαρινό εξάμηνο 2009)

Τμήμα Διοίκησης Επιχειρήσεων, Τ.Ε.Ι. Ιονίων Νήσων
Ασφάλεια Πληροφοριακών Συστημάτων (5ο εξάμηνο) : Εισαγωγή στην Κρυπτογραφία: Ασύμμετρα και συμμετρικά κρυπτοσυστήματα. Επαλήθευση ταυτότητας. Μηχανισμοί Αυθεντικοποίησης. Ψηφιακές Υπογραφές. Έλεγχος Πρόσβασης: Λίστες Ελέγχου Πρόσβασης, Ετικέτες Ασφαλείας (MAC / DAC) και Έλεγχος Πρόσβασης με βάση το ρόλο του χρήστη. Ασφάλεια Υπολογιστών: Ασφάλεια από παράνομη αντιγραφή, Ιοί, Ασφάλεια προσωπικού υπολογιστή. Έννοιες Ασφάλειας Δικτύων: Υπηρεσίες και Μηχανισμοί Ασφάλειας (κατά ISO 7498-2) (Χειμερινό εξάμηνο 2013)

Τεχνολογίες Διαδικτύου (6ο εξάμηνο) : TCP/IP, και η ανάπτυξη προγραμμάτων για το web. Χρήση της γλώσσας HTML (Τοποθέτηση διαλογικών προγραμμάτων -Γραφικά, Γραμματοσειρά και χρώμα -Εικόνα, κίνηση και ήχος -Απλές διασυνδέσεις χρήστη για μικροεφαρμογές -Διάταξη συστατικών σε μια διασύνδεση χρήστη -Απόκριση σε είσοδο χρήστη σε μια μικροεφαρμογή). Τι είναι τα URL, HTTP, HTML, dynamic HTML, XML, scriptlets, διεπαφή και τεχνολογία CGI. Perl, Tcl/SafeTcl. DNS model, DNS server hierarchy. X.500. DAP, LDAP protocols. Επίσης θα μελετηθεί η ανάκτηση πληροφοριών: Electronic mail, MIME, S/MIME, SMTP, POP, PPP, FTP. Mobile Code: Java, ActiveX, Javascript. (Εαρινό εξάμηνο 2009, 2010, 2011, 2013, 2014)

Εισαγωγή στην Πληροφορική (1ο εξάμηνο) : Εισαγωγικές έννοιες: το μοντέλο υλικό-λογισμικό ως επίπεδα προγραμματισμού. Ψηφιακή Λογική, Αρχιτεκτονική Υπολογιστών, Μικροεπεξεργαστές, Γλώσσες προγραμματισμού, Συμβολομετάφραση. Λειτουργικό Σύστημα. Δίκτυα, Διαδίκτυο και Τεχνολογίες Διαδικτύου. Βάσεις Δεδομένων και Πληροφοριακά Συστήματα. Άλλες Τεχνολογίες (Πολυμέσα, Τηλεματική κ.α.) (Χειμερινό εξάμηνο 2013)

Τεχνικές Σχεδίασης και Ανάλυσης Αλγορίθμων (5ο εξάμηνο) : NP-completeness, Πολύπλοκοι αλγόριθμοι (Χειμερινό εξάμηνο 2013)

Τεχνολογία Λογισμικού (5ο εξάμηνο) : το λογισμικό ως προϊόν και ως εργαλείο, αξία και ποιότητα του λογισμικού, οικονομικές διαστάσεις του λογισμικού, προβλήματα της ανάπτυξης

λογισμικού, περιεχόμενο της τεχνολογίας λογισμικού. Κύκλος ζωής του λογισμικού, μοντέλα κύκλου ζωής (μοντέλο καταρράκτη, μοντέλα πρωτοτυποποίησης και εξελικτικής ανάπτυξης, σπειροειδές μοντέλο), διαδικασίες λογισμικού. Ανάλυση απαιτήσεων λογισμικού: λειτουργικές και μη λειτουργικές απαιτήσεις, περιορισμοί, τεχνικές εκμαίευσης, προδιαγραφής, επικύρωσης και επαλήθευσης απαιτήσεων. Αρχιτεκτονική και λεπτομερής σχεδίαση λογισμικού, έννοιες συνοχής και σύζευξης, χαρακτηριστικά σχεδιαστικής ποιότητας, μετρικές μεγέθους και πολυπλοκότητας σχεδιασμού, φορμαλισμοί σχεδιασμού, αντικειμενοστρεφής σχεδιασμός. Παραγωγή κώδικα, μεθοδολογικές κατευθύνσεις, εργαλεία αυτόματης παραγωγής. Τεκμηρίωση κώδικα, μεθοδολογικές κατευθύνσεις, εργαλεία υποβοήθησης της τεκμηρίωσης. Υλοποίηση και έλεγχος (Χειμερινό εξάμηνο 2013)

Διδακτική Πληροφορικής (5ο εξάμηνο) : Η Πληροφορική στο σχολείο. Θεωρίες για τη γνώση και τη μάθηση. Η Πληροφορική ως αυτόνομο γνωστικό αντικείμενο. Παραδοσιακές και σύγχρονες μέθοδοι διδασκαλίας. Διδακτικές προσεγγίσεις στη διδασκαλία της Πληροφορικής. Εναλλακτικές θεωρήσεις για την εκπαιδευτική διαδικασία και το επάγγελμα του εκπαιδευτικού. Ο υπολογιστής ως εργαλείο μάθησης. Σχεδιασμός εκπαιδευτικού λογισμικού. (Χειμερινό εξάμηνο 2013)

Δομημένος Προγραμματισμός (1ο εξάμηνο) : Γλώσσες προγραμματισμού, Συμβολομεταφραστής, Γλώσσα προγραμματισμού C, Εντολές της C, Η έννοια της βιβλιοθήκης, Η ρουτίνα main(),Εισαγωγή και βασικές έννοιες στον προγραμματισμό και στην αλγοριθμική επίλυση, Δημιουργία, εκτέλεση και εύρεση και διόρθωση σφαλμάτων των προγραμμάτων, Είσοδος/έξοδος, μεταβλητές, αναθέσεις, μαθηματικοί και λογικοί τελεστές και εκφράσεις, διαχείριση αρχείων, Εντολές ελέγχου και επανάληψης, Συναρτήσεις, αναδρομή, Βασικές δομές δεδομένων, Λίστες, Πίνακες, Λεξικά, Σύνολα, Αναζήτηση/ταξινόμηση, μαθηματικές εφαρμογές.
(Χειμερινό εξάμηνο 2014)

Εισαγωγή στην Πληροφορική (1ο εξάμηνο) : Ψηφιακή Λογική, Αρχιτεκτονική Υπολογιστών, Αλγόριθμοι, Γλώσσες προγραμματισμού, Τεχνολογία Λογισμικού, Λειτουργικά Συστήματα, Βάσεις Δεδομένων, Δίκτυα Υπολογιστών, Τεχνολογίες Διαδικτύου, Τεχνολογίες Πολυμέσων, Πληροφοριακά Συστήματα, Τηλεματική, Νέες τεχνολογίες.
(Χειμερινό εξάμηνο 2014)

ΔΕΥΤΕΡΟΥ ΚΥΚΛΟΥ ΣΠΟΥΔΩΝ
ΜΔΕ Τεχνολογίες και Συστήματα Ευρυζωνικών Εφαρμογών και Υπηρεσιών, ΤΕΙ Δυτικής Ελλάδας
Θεματική Ενότητα «14 - Περιβάλλοντα και Μεθοδολογίες Σχεδιασμού Συστημάτων Υλικού/ Λογισμικού» (Ακαδημαϊκό έτος 2013-2014) συνδιδασκαλία

3. ΕΠΙΒΛΕΨΗ ΔΙΔΑΚΤΟΡΙΚΩΝ ΔΙΑΤΡΙΒΩΝ

Δεν προσφέρονται Μεταπτυχιακά Προγράμματα Ειδίκευσης που οδηγούν σε λήψη Διδακτορικού Διπλώματος από ΤΕΙ. Το διάστημα 2006-2008, κατά την διάρκεια Μεταδιδακτορικού Έργου στο Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών, επικούρησα στην επίβλεψη των κάτωθι διδακτορικών διατριβών:

1) Χαράλαμπος Μιχαήλ, επιβλ. Καθηγητής Κων/νος Γκούτης. Διδακτορική Διατριβή

«Βελτιστοποίηση επαναπροσδιοριζομένων αρχιτεκτονικών για απόδοση και κατανάλωση ενέργειας σε κρυπτογραφικές εφαρμογές κυριαρχούμενες από δεδομένα» (http://hdl.handle.net/10889/2829#sthash.aGBaCUGy.dpuf), 2010

2) Σχοινιανάκης Δημήτριος, επιβλ. Καθηγητής Θάνος Στουραΐτης. Διδακτορική Διατριβή «Versatile architectures for cryptographic systems» (http://hdl.handle.net/10889/7623#sthash.Ijn6wabz.dpuf), 2014

4. ΕΠΙΒΛΕΨΗ ΔΙΠΛΩΜΑΤΙΚΩΝ ΕΡΓΑΣΙΩΝ Β' ΚΥΚΛΟΥ ΣΠΟΥΔΩΝ

Δεν προσφέρεται Μεταπτυχιακό Πρόγραμμα Σπουδών 2ου κύκλου από το ΤΕΙ Ιονίων Νήσων, που να οδηγεί σε λήψη Μεταπτυχιακού Διπλώματος Ειδίκευσης. Ως επιβλέπων, σε άλλο Ίδρυμα (Πανεπιστήμιο Πατρών – ΠΜΣ ΟΣΥΛ), ολοκληρώθηκε η επίβλεψη του:

1) Χατζηδημητρίου Επαμεινώνδας, Μεταπτυχιακή Διατριβή «Διερεύνηση του προτύπου P1619 για διαμοιραζόμενα αποθηκευτικά μέσα και πρότυπες προτάσεις υλοποίησης» (επιτροπή αξιολόγησης Αθ. Κακαρούντας, Ο. Κουφοπαύλου, Γ. Θεοδωρίδης), 2013

5. ΕΠΙΒΛΕΨΗ ΔΙΠΛΩΜΑΤΙΚΩΝ/ΠΤΥΧΙΑΚΩΝ ΕΡΓΑΣΙΩΝ Α' ΚΥΚΛΟΥ ΣΠΟΥΔΩΝ

Αυτοδύναμη επίβλεψη περισσότερων από **40 πτυχιακών εργασιών** στα ακόλουθα ιδρύματα: ΤΕΙ Ιονίων Νήσων, Πανεπιστήμιο Θεσσαλίας, Πανεπιστήμιο Κεντρικής Ελλάδας, ΤΕΙ Λαμίας, Ελληνικό Ανοικτό Πανεπιστήμιο.

6. ΑΚΑΔΗΜΑΪΚΕΣ-ΔΙΟΙΚΗΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

1. Υπό συγγραφή ηλεκτρονικό σύγγραμμα «**Λογική Σχεδίαση Ι**», για την πρόσκληση «Ηλεκτρονικά Ακαδημαϊκά Συγγράμματα και Βοηθήματα για Επιστήμες Μηχανικών και Πληροφορική». Συγγραφείς Αθ. Κακαρούντας και Ν. Λελίγκου. (έναρξη 7/10/2014 – δεν έχει ολοκληρωθεί)

2. Υπό συγγραφή πρότασης οργάνωσης της Θεματικής Ενότητας ΣΔΥ62 – **Ενσωματωμένα Συστήματα**, Ελληνικό Ανοικτό Πανεπιστήμιο (2014 – δεν έχει ολοκληρωθεί)

3. Υπό συγγραφή πρότασης οργάνωσης της Θεματικής Ενότητας ΠΛΣ51 – **Βασικές εξειδικεύσεις σε Αρχιτεκτονική και Δίκτυα των Υπολογιστών**, Ελληνικό Ανοικτό Πανεπιστήμιο (2014 – δεν έχει ολοκληρωθεί)

4. Συμμετοχή στο IEEE IST-Academic MOOC, με την διδασκαλία της Θεματικής Ενότητας «**Ψηφιακή Λογική**» (2014-2015)

5. Ανάπτυξη μαθήματος «**Αρχιτεκτονική Υπολογιστών**» για το Τμήμα Πληροφορικής με Εφαρμογές στη Βιοϊατρική, Παν/μιο Στερεάς Ελλάδας (νυν Παν/μιο Θεσσαλίας), (Ακαδ.

Έτη 2006-2010)

6. Ανάπτυξη μαθημάτων «Ψηφιακή Λογική» και «**Αρχιτεκτονική Υπολογιστών**» για το Τμήμα Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών, ΤΕΙ Ιονίων Νήσων (Παράρτημα Λευκάδας), (Ακαδ. Έτη 2009-2011)

7. Υλοποίηση και Διδασκαλία **2ου εργαστηριακού κύκλου Ψηφιακών Συστημάτων** (IEEE Circuits & Systems Society και Ελληνικό Ανοικτό Πανεπιστήμιο) (2009)

8. Σχεδιασμός και υλοποίηση διδακτικού υλικού θεματικής ενότητας ΠΛΣ51 - **Βασικές εξειδικεύσεις σε Αρχιτεκτονική και Δίκτυα των Υπολογιστών**, Ελληνικό Ανοικτό Πανεπιστήμιο (2010)

9. Υλοποίηση και Διδασκαλία **1ου εργαστηριακού κύκλου Ψηφιακών Συστημάτων** (IEEE Circuits & Systems Society και Ελληνικό Ανοικτό Πανεπιστήμιο) (2009)

10. Σχεδιασμός και υλοποίηση e-learning video tutorials για **εργαλεία σχεδιασμού και τεχνικές VLSI**, ΤΕΙ Λαμίας (2006-2007)

11. Σχεδιασμός και υλοποίηση e-learning video tutorials θεματικής ενότητας «**Σχεδίαση VLSI**», ΤΕΙ Λαμίας, (2006-2007)

12. Σχεδιασμός και υλοποίηση e-learning video tutorials θεματικής ενότητας «**Ασφάλεια και Κρυπτογραφία**», ΤΕΙ Λαμίας (2006-2007)

13. Σχεδιασμός, Υλοποίηση και Διδασκαλία της Εργαστηριακής Θεματικής Ενότητας ΠΛΗ21-ΕΨΣ (**Εργαστήριο Ψηφιακών Συστημάτων**), ΕΑΠ, (2005-2006)

14. **Προϊστάμενος Τμήματος** Εφαρμογών Πληροφορικής στη Διοίκηση και στην Οικονομία (ΕΠΔΟ) στο Τ.Ε.Ι. Ιονίων Νήσων, Παράρτημα Λευκάδας (17/1/2012-31/8/2013)

15. **Αναπληρωτής Προϊστάμενος Τμήματος** Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών (ΤΠΤ) στο Τ.Ε.Ι. Ιονίων Νήσων, Παράρτημα Λευκάδας (17/1/2012-31/8/2013)

16. **Προεδρεύων Ομάδας Εσωτερικής Αξιολόγησης** (ΟΜΕΑ) Τμήματος ΕΠΔΟ (2012-2013)

17. **Εξωτερικός Αξιολογητής**: Β. Ταμπακάς, Α. Κακαρούντας, «Αξιολόγηση – Εξωτερική

Αξιολόγηση ΔΑΣΤΑ Λαμίας – 1η περίοδος», ΤΕΙ Λαμίας, Λαμία, 2013.

18. **Εξωτερικός Αξιολογητής**: Β. Ταμπακάς, Α. Κακαρούντας, «Αξιολόγηση – Εξωτερική Αξιολόγηση ΔΑΣΤΑ Λαμίας – 2η περίοδος», ΤΕΙ Λαμίας, Λαμία, 2013

19. **Μέλος επιτροπής για ποιοτική και ποσοτική παραλαβή** έργου που αφορά κατασκευή και τοποθέτηση πινακίδων στο Παράρτημα Λευκάδας, ύψους 4.797,00 Ευρώ (2ο θέμα, 2η Τακτική Συνεδρίαση Διοικούσας Επιτροπής, 15/01/2013)

20. **Μέλος επιτροπής ενστάσεων** για Διεθνή Ανοικτό Διαγωνισμό για τη σίτιση των Φοιτητών Παραρτήματος Λευκάδας ύψους 135.000,00 Ευρώ (26 απόφαση, 2ο θέμα, 17η Τακτική Συνεδρίαση Διοικούσας Επιτροπής, 15/05/2013)

21. **Μέλος επιτροπής ενστάσεων** για Διεθνή Ανοικτό Διαγωνισμό για τη σίτιση των Φοιτητών Παραρτήματος Λευκάδας ύψους 270.000,00 Ευρώ (2ο θέμα, 3η Τακτική Συνεδρίαση Διοικούσας Επιτροπής, 23/01/2013)

22. **Μέλος Επιτροπής** Χορήγησης Φοιτητικού Στεγαστικού Επιδόματος (2012-2013 & 2013-2014) για το ΤΕΙ Ιονίων Νήσων, Παράρτημα Λευκάδας

23. **Μέλος Επιτροπής** Ελέγχου Καλής Εκτέλεσης Λέσχης φοιτητών (2012-2013 & 2013-2014) για το ΤΕΙ Ιονίων Νήσων, Παράρτημα Λευκάδας

24. **Τμηματικός υπεύθυνος** για Πρακτική Άσκηση στο Τμήμα ΕΠΔΟ, (01/10/2012 – 20/09/2013) σύμφωνα με απόφαση 47, θέματα Επιτροπής Εκπαίδευσης και Ερευνών, 29η Τακτική Συνεδρίαση Διοικούσας Επιτροπής, 12/09/2012

25. **Επόπτης Τμήματος** για Πρακτική Άσκηση στο Τμήμα ΕΠΔΟ, (01/10/2012 – 20/09/2013) σύμφωνα με απόφαση 47, θέματα Επιτροπής Εκπαίδευσης και Ερευνών, 29η Τακτική Συνεδρίαση Διοικούσας Επιτροπής, 12/09/2012

26. **Μέλος Επιτροπής Ποιοτικής και Ποσοτικής Παραλαβής Έργου** για το Υποέργο με τίτλο «Ανάδειξη του Τεχνολογικού Ιδρύματος Ιονίων Νήσων ως Διεθνούς Πόλου Εκπαίδευσης και Καινοτομίας – Β' Φάση» και α/α «03» της Πράξης «Ανάδειξη του Τεχνολογικού Ιδρύματος Ιονίων Νήσων ως Διεθνούς Πόλου Εκπαίδευσης και Καινοτομίας» με κωδικό MIS 352400 για το ΤΕΙ Ιονίων Νήσων, Παράρτημα Λευκάδας σύμφωνα με την απόφαση 5, θέματα Επιτροπής Εκπαίδευσης και Ερευνών, 1η Τακτική Συνεδρίαση Διοικούσας Επιτροπής, 09/01/2013 (ισχύς 01/01/2013 – 30/04/2014)

27. **Μέλος Επιτροπής Ποιοτικής και Ποσοτικής Παραλαβής** - Ελέγχου Καλής

Εκτέλεσης έργου καθαρισμού προαύλιου χώρου για το ΤΕΙ Ιονίων Νήσων, Παράρτημα Λευκάδας σύμφωνα με την απόφαση 8, θέμα 1, 34η Τακτική Συνεδρίαση Διοικούσας Επιτροπής, 18/09/2013 (Ακαδημαϊκό Έτος 2013-2014)

28. **Μέλος Επιτροπής Ποιοτικής και Ποσοτικής Παραλαβής** – Δημιουργία αρδευτικού συστήματος κήπου στον προαύλιο χώρο του Νέου Κτιρίου του ΤΕΙ Ιονίων Νήσων, στη Λευκάδα (δαπάνη που βαραίνει τον Τακτικό Προϋπολογισμό 2014 με ΚΑΕ 0889.01). σύμφωνα με την απόφαση 10, θέμα 2, 29η Τακτική Συνεδρίαση Διοικούσας Επιτροπής, 31/07/2014 (Ακαδημαϊκό Έτος 2014-2015)

29. **Μέλος Επιτροπής Αξιολόγησης** για Πρόχειρο Ανοικτό Διαγωνισμό για την «Διαμόρφωση του Περιβάλλοντα Εξωτερικού Χώρου των Εγκαταστάσεων του Τ.Ε.Ι. Ιονίων Νήσων στο Παράρτημα Λευκάδας» ύψους 73.800,00 Ευρώ, σύμφωνα με την απόφαση της 33η Τακτική Συνεδρίαση Διοικούσας Επιτροπής, 13/09/2013 (Ακαδημαϊκό Έτος 2013-2014)

30. **Μέλος Επιτροπής Αξιολόγησης** για Ανοικτό Διεθνή Διαγωνισμό για την «Παροχή Υπηρεσιών Διαμόρφωσης – Οργάνωση Υποδομών και Λειτουργίας Εικονικού Περιβάλλοντος Εξ Αποστάσεως Εκπαίδευσης και Λοιπών Λειτουργιών» ύψους 350.000,00 Ευρώ, σύμφωνα με το αριθ. Πρωτ. 2925/26-11-2012 και την απόφαση της 34η Τακτική Συνεδρίαση Διοικούσας Επιτροπής, 17/10/2012

31. **Υπεύθυνος Εργαστηρίων και Τμήματος Δικτύων** ΤΕΙ Ιονίων Νήσων (Παράρτημα Λευκάδας) σύμφωνα με την απόφαση με αρ.πρωτ 3904/26-11-2009, του Προϊσταμένου του Τμήματος ΕΠΔΟ. (Ακαδημαϊκό Έτος 2009-2010)

32. **Μέλος Επιτροπής Πτυχιακών Εργασιών** σύμφωνα με την απόφαση με αρ.πρωτ 1360/03-03-2009, του Προϊσταμένου του Τμήματος ΕΠΔΟ.

33. **Μέλος Επιτροπής Οργάνωσης Μεταπτυχιακού Προγράμματος** σύμφωνα με την απόφαση με αρ.πρωτ 2106/10-06-2009, του Προϊσταμένου του Τμήματος ΕΠΔΟ.

34. **Συγγραφέας-Μελετητής** «Μελέτη σκοπιμότητας για τη Σχολή Ηλεκτρονικής Διοίκησης και Τηλεπικοινωνιών», ΤΕΙ Ιονίων Νήσων, Λευκάδα (2009)

35. **Συγγραφέας-Μελετητής** «Μελέτη βιωσιμότητας για τη Σχολή Ηλεκτρονικής Διοίκησης και Τηλεπικοινωνιών», ΤΕΙ Ιονίων Νήσων, Λευκάδα (2009)

36. **Υπεύθυνος Βιβλιοθήκης** ΤΕΙ Ιονίων Νήσων (Παράρτημα Λευκάδας) (Ακαδημαϊκό

Έτος 2008-2009)

IV. ΕΠΑΓΓΕΛΜΑΤΙΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ

1. Επίκουρος Καθηγητής στο ΤΕΙ Ιονίων Νήσων, Τμήμα Διοίκησης Επιχειρήσεων (πρώην Τμήμα Εφαρμογών Πληροφορικής στη Διοίκηση και στην Οικονομία - Λευκάδα), ΦΕΚ 1123/τ. Γ'/22-12-2011.

2. Ερευνητής στο Εργαστήριο Μικροηλεκτρονικής – Σχεδιασμού Κυκλωμάτων Υψηλής Κλίμακας (VLSI Design Laboratory), Πανεπιστήμιο Πατρών (διευθυντής: κ. Κ. Γκούτης): 1/10/1998 – 30/12/2011.

3. Ελεγκτής της Γενικής Γραμματείας Έρευνας και Τεχνολογίας (2009)

4. Διευθυντής Στρατηγικού Σχεδιασμού & Ανάπτυξης (και εκτελών χρέη Γενικού Διευθυντή του Επιστημονικού Πάρκου Πατρών) (1/6/07 – 31/5/08)

5. Συγγραφή και ανάπτυξη εκπαιδευτικού-υποστηρικτικού υλικού για το Ελληνικό Ανοικτό Πανεπιστήμιο

6. Μετάφραση βιβλίου για τις εκδόσεις ΚΛΕΙΔΑΡΙΘΜΟΣ

7. Εκπαίδευση ενηλίκων (ΙΔΕΚΕ) στην Πληροφορική.

8. Ελεγκτής της Περιφέρειας Δυτικής Ελλάδας (αντικείμενο Υψηλή Τεχνολογία και Πληροφορική)

V. ΕΡΕΥΝΗΤΙΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ

Προπτυχιακή Έρευνα:

1) Ανάπτυξη πόσιμης κάψουλας για την καταγραφή των υγρών και των χημικών προσμίξεων στο στομάχι και το έντερο, Εργαστήριο Μικροηλεκτρονικής, 1998 (επιβλέπων: Καθ. Κων/νος Γκούτης, ομάδα: Αθ. Κακαρούντας, Ν. Ζέρβας, Β. Κόκκινος).

Μεταπτυχιακή Έρευνα:

1) Ανάπτυξη αυτοελεγχόμενων κυκλωμάτων και συστημάτων χαμηλής κατανάλωσης για ενσωμάτωση σε φορετά συστήματα, Εργαστήριο Μικροηλεκτρονικής, 2000 (επιβλέπων: Καθ. Κων/νος Γκούτης, ομάδα: Αθ. Κακαρούντας, Κ. Παπαδομανωλάκης).

2) Συσκευή έγχυσης ινσουλίνης σε διαβητικούς, υψηλής αξιοπιστίας, Εργαστήριο Μικροηλεκτρονικής & Micrel Medical Devices, 2001 (επιβλέπων: Καθ. Κων/νος Γκούτης & Αλ. Τσούκαλης, ομάδα: Αθ. Κακαρούντας, Κ. Παπαδομανωλάκης).

Μεταδιδακτορική Έρευνα:

1) Ανάπτυξη συστήματος αναγνώρισης της νοηματικής γλώσσας από τον υπολογιστή, ΤΕΙ Ηπείρου και ΤΕΙ Ιονίων Νήσων, 20013-2015 (επιβλέπων: Αθ. Κακαρούντας,, ομάδα: Αθ. Κακαρούντας, Σ. Δραγουμάνος, Δ. Κωτσίδου).

1) Ενσωματωμένα συστήματα για επαύξηση πραγματικότητας, ΤΕΙ Ιονίων Νήσων, 2014 (επιβλέπων: Αθ. Κακαρούντας,, ομάδα: Αθ. Κακαρούντας, Σ. Δραγουμάνος, Κ. Κακαρούντας).

2) Σχεδίαση Κυκλωμάτων και Αρχιτεκτονικές συστήματος κρυπτογράφησης διαμοιραζόμενων αποθηκευτικών μέσων σύμφωνα με το P1619, Πανεπιστήμιο Πατρών, 2013 (επιβλέπων: Αθ. Κακαρούντας,, ομάδα: Αθ. Κακαρούντας, Ε. Χατζηδημητρίου).

3) Ανάπτυξη επιταχυντών υλικού για επεξεργασία εικόνας, Πανεπιστήμιο Πατρών, 2007-2013 (επιβλέπων: Κων/νος Γκούτης και Αθ. Κακαρούντας,, ομάδα: Αθ. Κακαρούντας, Μ. Παπαδονικολάκης, Β. Πανταζής, Α. Πολύζος).

4) Ανάπτυξη συσκευής υποστήριξης σε άτομα με Διαταραχές Λόγου Νευρολογικής Φύσεως, Τμήμα Πληροφορικής με Εφαρμογές στη Βιοϊατρική, Παν/μιο Στερεάς Ελλάδας, 2012 (επιβλέπων: Αθ. Κακαρούντας,, ομάδα: Αθ. Κακαρούντας, Ε. Αρβανίτη).

5) Δυαδικές ακολουθίες παραγόμενες από κυψελιδικά αυτόματα, Τμήμα Πληροφορικής με Εφαρμογές στη Βιοϊατρική, Παν/μιο Στερεάς Ελλάδας, 2010 (επιβλέπων: Αθ. Κακαρούντας, ομάδα: Αθ. Κακαρούντας, Η. Μαυρίδης, Ε. Αρβανίτη).

6) Ανάπτυξη μεθοδολογιών μετασχηματισμού κρυπτογραφικών αλγόριθμων για ανάπτυξη κυκλωμάτων και συστημάτων υψηλής απόδοσης, Εργαστήριο Μικροηλεκτρονικής, Πανεπιστήμιο Πατρών, 2005-2010 (επιβλέπων: Κων/νος Γκούτης, Θ. Στουραΐτης & Αθ. Κακαρούντας, ομάδα: Αθ. Κακαρούντας, Χ. Μιχαήλ, Δ. Σχοινιανάκης, Α. Μπροκαλάκης, Ι. Γιακουμής, Μ. Παπαδονικολάκης, Κ. Αίσωπος).

Συμμετοχή σε Χρηματοδοτούμενα Προγράμματα:

1. "*EASY: Energy-Aware SYstem-on-Chip design of the HIPERLAN/2 standard*" έργο εφαρμοσμένης έρευνας, IST-2000-30093 με χρηματοδότηση από την Ευρωπαϊκή Ένωση (1/9/2001-31/12/2003)

2. "*COSAFE : Low Power Hardware-Software Co-Design for Safety-Critical Applications*" έργο εφαρμοσμένης έρευνας, IST-1998-28593 με χρηματοδότηση από την Ευρωπαϊκή Ένωση ΚΕ 846, (1/8/1998 – 31/7/2001)
3. "*A memory management methodology for real-time and low-power embedded multimedia systems*" έργο εφαρμοσμένης έρευνας, στα πλαίσια του ΠΕΝΕΔ'99 – 99ED501 με χρηματοδότηση από ΓΓΕΤ
4. "*LPGD: A low-power design methodology/flow and its application to the implementation of a DCS1800-GSM/DECT Modulator-Demodulator*" έργο εφαρμοσμένης έρευνας, ESPRIT IV με χρηματοδότηση από την Ευρωπαϊκή Ένωση μέσω της εταιρείας INTRACOM, (Διάρκεια: 1/11/98 – 31/10/99).
5. "*AMDREL: Architectures and Methodologies for Dynamic Reconfigurable Logic*", έργο εφαρμοσμένης έρευνας, IST-2001-34379, με χρηματοδότηση από την Ευρωπαϊκή Ένωση (1/10/2003-29/2/2004)
6. "*TARDIS: Technical Coordination and Dissemination*", Esprit project 25213-ESD-LPD, έργο εφαρμοσμένης έρευνας, με χρηματοδότηση από την Ευρωπαϊκή Ένωση (1/6/1999-31/8/1999))
7. "*MARLOW: A central market place for dissemination of low power microelectronics*", έργο εφαρμοσμένης έρευνας,IST-2001-37115, με χρηματοδότηση από την Ευρωπαϊκή Ένωση (1/4/2003-31/7/2003)
8. "*INTRALED: Industry-driven training for low-power European designers*", έργο εφαρμοσμένης έρευνας, IST-2001-34631, με χρηματοδότηση από την Ευρωπαϊκή Ένωση (1/9/2003-30/9/2003)
9. "*AMIED: Asynchronous low-power methodology and implementation of an encryption-decryption system*", Esprit project 25249-ESD-LPD, έργο εφαρμοσμένης έρευνας, με χρηματοδότηση από την Ευρωπαϊκή Ένωση (1/2/1999-30/11/1999)
10. "*ΠΥΘΑΓΟΡΑΣ: Μεθοδολογίες εύρεσης αρχιτεκτονικών επαναδιατασώμενων ενσωματωμένων συστημάτων*", βασικής και τεχνολογικής έρευνας, ως Κύριος Ερευνητής (Μεταδιδάκτορας), χρηματοδότηση από Γενική Γραμματεία Έρευνας και Τεχνολογίας μέσω Ε.Π.Ε.Α.Ε.Κ. (Διάρκεια: 1/3/04 – 31/8/06)
11. "*ΑΡΧΙΜΗΔΗΣ ΙΙ: Σχεδίαση συστημάτων κρυπτογραφίας βασισμένων σε αριθμητικά συστήματα υπολοίπων*", έργο τεχνολογικής έρευνας, χρηματοδότηση από Γενική Γραμματεία Έρευνας και Τεχνολογίας μέσω Ε.Π.Ε.Α.Ε.Κ. ΙΙ
12. «*ΠΕΡΙΦΕΡΕΙΑΚΟΣ ΠΟΛΟΣ ΚΑΙΝΟΤΟΜΙΑΣ – ΠΕΡΙΦΕΡΕΙΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ*», αναπτυξιακό πρόγραμμα χρηματοδοτούμενο από το Υπουργείο Ανάπτυξης – ΓΓΕΤ, ως ερευνητής – εκπρόσωπος του Επιστημονικού Πάρκου Πατρών.

13. «*ALMA: Architecture oriented paraLlelization for high performance embedded Multicore systems using scilAb*», ως ερευνητής, έργο τεχνολογικής έρευνας, χρηματοδότηση Ευρωπαϊκή Ένωση και 7ο Κοινοτικό Πρόγραμμα Πλαίσιο (MIS 287733). (Διάρκεια: 01/09/2012 - 31/08/2013).
14. «*Ανάπτυξη κωδικοποιητή JPEG-XR για ενσωμάτωση σε ψηφιακά ηλεκτρονικά συστήματα*» στα πλαίσια της Πράξης «Υποστήριξη Νέων Επιχειρήσεων για Δραστηριότητες Έρευνας & Τεχνολογικής Ανάπτυξης», ως έμπειρος ερευνητής, χρηματοδότηση από ΕΥΔΕ-ΕΤΑΚ για εφαρμοσμένη έρευνα. (Διάρκεια: 1/1/11 – 12/2012) (Συγγραφέας πρότασης η οποία αξιολογήθηκε ως 1η στην αντίστοιχη λίστα κατάταξης)
15. «*MOTHER LANGUAGE*», ως συντονιστής του υποέργου, αναπτυξιακό έργο , χρηματοδότηση INTERREG IIIA (διάρκεια: 1/6/07 – 31/5/08)
16. *ΤΟΠΕΚΟ ΛΕΥΚΑΔΑΣ*, αναπτυξιακό έργο, χρηματοδότηση ΕΣΠΑ (Διάρκεια: 1/2011 – 11/2014) ως Επιστημονικός Υπεύθυνος για το ΤΕΙ Ιονίων Νήσων (24ο θέμα, Επιτροπής Εκπαίδευσης και Έρευνας, 18η Τακτική Συνεδρίαση Διοικούσας Επιτροπής, 16/05/2012) .
17. «*Regions 4 Green Growth*» - Regional policy instruments and approaches for improving access to finance and speeding up investments in sustainable energy, αναπτυξιακό έργο, χρηματοδότηση INTERREG IVC, ως μελετητής για εκπόνηση Περιφερειακού Σχεδίου Ενεργειών και Εφαρμογής (Regional Action and Implementation Plan) (Διάρκεια 01/07/2014 – 30/09/2014)
18. "Runtime Verification beyond Monitoring (ARVI)", ICT COST Action IC1402, ως εκπρόσωπος της Ελλάδας στην Επιτροπή Διοίκησης (Management Committee). (12/2014 - 2017)

Διπλώματα Ευρεσιτεχνίας

-

VI. ΣΥΜΜΕΤΟΧΗ ΣΕ ΕΠΑΓΓΕΛΜΑΤΙΚΟΥΣ ΚΑΙ ΑΛΛΟΥΣ ΣΥΛΛΟΓΟΥΣ

- **Senior Member** του IEEE
- Μέλος των IEEE Societies: Computer Society, Solid-State Society, Communications Society, Consumer Electronics Society, Circuits and Systems Society, Biology and Medical Engineering Society, Education Society
- Μέλος του Test Technology Technical Council, Life Sciences Technical Community, Internet of Things Technical Community.
- **Senior Member** Association Computing Machinery (ACM)

- Μέλος του IET
- Μέλος του EURASIP
- Μέλος του Τεχνικού Επιμελητηρίου Ελλάδος (ΤΕΕ)
- Μέλος της Ένωσης Μηχανικών Πληροφορικής & Επικοινωνιών Ελλάδας

VII. ΑΛΛΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

Συντακτικές Δραστηριότητες

Μέλος του Editorial Board των διεθνών περιοδικών:

i) IEEE Potentials, Associate editor (2015 – 2017)
ii) Journal of VLSI Design Tools and Technology (JoVDT),
iii) Journal of Applied Mathematics and Bioinformatics (JAMB).

Στο παρελθόν

i) International Journal of Computational Intelligence (IJCI),
ii) International Journal of Signal Processing (IJSP).

Σεμινάρια – Ομιλίες

08/07/2013: Διάλεξη με τίτλο «Σύγχρονες τάσεις στα διεθνή πρότυπα εικόνας και ήχου – η κρυμμένη πληροφορία», στο Θερινό Σχολείο «Διοίκηση των Μέσων Ενημέρωσης με έμφαση στα νέα ψηφιακά μέσα επικοινωνίας» (Λευκάδα), που διοργανώθηκε στο πλαίσιο της Πράξης «Ανάδειξη του Τεχνολογικού Ιδρύματος Ιονίων Νήσων ως Διεθνούς Πόλου Εκπαίδευσης και Καινοτομίας» (MIS 352400).

12/06/2013: Διάλεξη στο ΤΕΙ Ιονίων Νήσων, με τίτλο « Open Hardware + Arduino workshop», στο πλαίσιο των εκδηλώσεων του IEEE Consumer Electronics Society – Greece Chapter.

27/02/2013: Διάλεξη στο Τμήμα Πληροφορικής με Εφαρμογές στη Βιοϊατρική, με τίτλο «Brain Computing: Νοητικός έλεγχος και εφαρμογές», στην ημερίδα «Biomedical Engineering: trends, Research and Technologies»

16/12/2012: Διάλεξη στο Innohub (Corallia), με τίτλο «Consumer Electronics - a market worth discovering», στο πλαίσιο του 1ου IEEE Hellenic Student Branches Congress

29/03/2012: Διάλεξη στο Τμήμα Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών, με τίτλο «Σχεδιασμός Ενσωματωμένων Συστημάτων», στο πλαίσιο του 2ου εργαστηριακού

κύκλου στα Ενσωματωμένα Συστήματα (συν-διοργάνωση IEEE Consumer Electronics Society – Greece Chapter και Τ.Ε.Ι. Ιονίων Νήσων)

21/03/2012: Διάλεξη-εργαστήριο (tutorial) στο Τμήμα Πληροφορικής με Εφαρμογές στη Βιοϊατρική, με τίτλο «Ανοικτό Υλικό για την δημιουργία καινοτόμων εφαρμογών: μελέτη περίπτωσης το BeagleBoard», στην ημερίδα «Ελεύθερο ή Ανοικτό; Λογισμικό ή Υλικό; Όταν η δημιουργία περνάει από τα χέρια μας»

30/11/2011: Διάλεξη στο Τμήμα Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών, με τίτλο «Σχεδιασμός Ενσωματωμένων Συστημάτων», στο πλαίσιο του 1ου εργαστηριακού κύκλου στα Ενσωματωμένα Συστήματα (συν-διοργάνωση IEEE Consumer Electronics Society – Greece Chapter και Τ.Ε.Ι. Ιονίων Νήσων)

07/04/2011: Διάλεξη στο Τμήμα Πληροφορικής με Εφαρμογές στη Βιοϊατρική, με τίτλο «Συ-Σχεδιασμός Λογισμικού και Υλικού για Ενσωματωμένα Συστήματα», στην ημερίδα «Ενσωματωμένα Συστήματα υπολογιστών και εφαρμογές στη Βιοϊατρική»

08/10/2010: Ομιλία στο Athens Digital Week (2010) με θέμα «IEEE – Όχημα Αριστείας»

26/11/2009: Διάλεξη στο Πολυτεχνείο Κρήτης (Χανιά), Τμήμα Ηλεκτρονικών Μηχανικών & Μηχανικών Υπολογιστών με θέμα «Επιταχυντές υλικού (Hardware Accelerators) για Ενσωματωμένα Συστήματα»

15/04/2008: Διάλεξη στο ΕΠΠ με θέμα «Το Επιστημονικό Πάρκο Πατρών ως διαχειριστής - εμψυχωτής καινοτομίας στην Δυτική Ελλάδα», στα πλαίσια της ημερίδας «Business Angels Center: Από την Καινοτομία στην Επιχειρηματικότητα».

14/04/2008: Διάλεξη στον Πύργο με θέμα «Διαδραστικά Ψηφιακά Εκθέματα», στα πλαίσια της ημερίδας Ευρυζωνικότητα & Τουρισμός.

11/04/2008: Διάλεξη στο Αγρίνιο (Παπαστράτειο) με θέμα «Διαδραστικά Ψηφιακά Εκθέματα», στα πλαίσια της ημερίδας Ευρυζωνικότητα & Τουρισμός.

09/04/2008: Διάλεξη στην Πατρα (Συνεδριακό Οργ. Λιμένος Πατρών) με θέμα «Διαδραστικά Ψηφιακά Εκθέματα», στα πλαίσια της ημερίδας Ευρυζωνικότητα & Τουρισμός.

23/01/2008: Διάλεξη στο ΑΤΕΙ Πατρών, με θέμα «ΕΡΕΥΝΑ ΚΑΙ ΚΑΙΝΟΤΟΜΙΑ: ΜΟΧΛΟΙ ΑΝΑΠΤΥΞΗΣ ΓΙΑ ΤΗΝ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΜΙΑΣ ΧΩΡΑΣ», στα πλαίσια της ημερίδας Καινοτομία και Επιχειρηματικότητα.

19/12/2007: Διάλεξη στο Πανεπιστήμιο Πελοποννήσου (Τρίπολη), Τμήμα Επιστήμης & Τεχνολογίας Υπολογιστών με θέμα «Σχεδίαση Κρίσιμων Υπολογιστικών Συστημάτων»

24/11/2007: Διάλεξη στο MoneyShow2007, Πάτρα, με θέμα «Επιστημονικό Πάρκο Πατρών: το παρών και το μέλλον»

24/11/2007: Διάλεξη στο MoneyShow2007, Πάτρα, με θέμα «Διεθνής Ζώνη Καινοτομίας στη Δυτική Ελλάδα»

17/11/2007: Διάλεξη στο ΓΕΦΥΡΕΣ 2007, ΟΛΠΑ, με θέμα «Περιφερειακός Πόλος Καινοτομίας Δυτικής Ελλάδας»

19/01/2007: Διάλεξη στο ΤΕΙ Ιονίων Νήσων (Λευκάδα), Τμήμα Πληροφορικής, με θέμα «Σύγχρονες τάσεις στην Αρχιτεκτονική Υπολογιστών»

15/10/2006: Διάλεξη στο ΤΕΙ Άρτας, Τμήμα Πληροφορικής, με θέμα «Οι σύγχρονες τεχνολογικές τάσεις στην Αρχιτεκτονική Υπολογιστών»

29/09/2006: Διάλεξη στο Πανεπιστήμιο Ιωαννίνων, Τμήμα Πληροφορικής, με θέμα «Αποσυζευγμένη Αρχιτεκτονική – Επιταχύνοντας την εκτέλεση ειδικών εφαρμογών»

13/01/2006: Διάλεξη στο Αριστοτέλειο Πανεπιστήμιο, Τμήμα Φυσικής, προσκεκλημένος του Εργαστηρίου Ηλεκτρονικής, με θέμα «Σύγκρουση Τεχνικών Σχεδιασμού Κυκλωμάτων. Παράδειγμα: Όταν η ασφάλεια λειτουργίας δεν είναι ‘φιλική’ προς την ενέργεια»

* κάποιες από τις ομιλίες έχουν πραγματοποιηθεί στο πλαίσιο αξιολόγησης από Εκλεκτορικό Σώμα του ερευνητικού έργου του Δρ. Κακαρούντα

Κριτής Περιοδικών, Συνεδρίων

Περιοδικά:

i) IEEE Transactions on Computers, ii) IEEE Transactions on Parallel and Distributed Systems, iii) IEEE Transactions on Circuits and Systems-I, iv) IEEE Transactions on Circuits and Systems-II, v) IEEE Transactions on VLSI Systems, vi) IEEE Transactions on Dependable and Secure Computing, vii) IEEE Computer, viii) International Journal of Computational Intelligence (IJCI), ix) International Journal of Signal Processing (IJSP), x) Journal of Computers (JCP), xi) International Journal of Computer Aided Engineering and Technology (IJCAET), xii) International Journal of Sensor Networks (IJSNET), xiii) Information Security Journal: A Global Perspective (ISJ), xiv) Elsevier, Microprocessors and Microsystems (MICPRO), xv) Elsevier, Microelectronics Journal (MEJ), xvi) Elsevier, Integration, the VLSI Journal (VLSI), xvii) IEEE Consumer Electronics Magazine, xviii) SPIE, Journal of Applied Remote Sensing (JARS), xix) Springer, Journal of Real-Time Image Processing (JRTIP), xx) Elsevier, Scientia Iranica (SCIENTIA), xxi) IEEE, Access, xxi) IEEE, Systems Journal, xxii) IEEE, Transactions on Information Forensics & Security, xxiii) SPIE, Journal of Electronic Imaging, xxiv) Springer, Studies in Computational Intelligence, xxv) Wiley, Security and Communications Network (SCN), xxvi) ACM Transactions on Reconfigurable Technology and Systems (TRETS).

Συνέδρια:

i) IEEE Int. Symp. on Circuits and Systems, (ISCAS), ii) IEEE International Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS), iii) IEEE Int. Conf. on Electronics, Circuits, and Systems (ICECS), iv) IEEE Mediterranean Electrotechnical Conference (MELECON 2004, 2010, 2012), v) IFIP/IEEE Conference on Very Large Scale Integration (VLSI-SOC 2008,2009,2010), vi) International Workshop on Systems, Architectures, Modeling, and Simulation, (SAMOS 2007, 2009), vii) IEEE International Conference on Computer as a Tool (EUROCON 2005,2010,2011), viii) ACM International Conference on Compilers, architecture and synthesis (CASES 2006,2007), ix) 6th International conference on Design & Technology of Integrated Systems in nanoscale era (DTIS 2011), x) IEEE International Symposium on Wireless Communication Systems (ISWCS 2007), xi) IEEE International Conference on Digital Signal Processing (DSP 2009,2011), xii) IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2008), xiii) IEEE International Conference on Circuits and Systems for Communications (ICCSC 2008), xiv) IEEE 30th Annual Northeast Bioengineering, xv) IEEE International Symposium on Consumer Electronics (ISCE 2009, 2012, 2013), xvi) IEEE

Wireless Communications and Networking Conference (WCNC 2009), xvii) International Conference on Computer Design (CDES 2005), xviii) IEEE Int. Conf. on Innovations in Information Technology (IIT 2007), xviii) International Conference on Network Computing and Information Security (NCIS 2011), xix) International Conference on Multimedia and Signal Processing (CMSP 2011), xx) IEEE Vehicular Technology Conference (VTC 2010, 2012), xxi) 7th International Conference on Embedded and Multimedia Computing (EMC 2012), xxii) IEEE International Symposium on Computers and Communications (ISCC 2011,2013,2014, 2015), xxiii) IEEE Business, Engineering & Industrial Applications Colloquium (BEIAC 2013), xxiv) IEEE Colloquium on Humanities, Science and Engineering Research (CHUSER 2012, 2014), xxv) Design Automation Conference (DAC 2013, 2014), xxvi) International Conference Field Programmable Logic and Applications (FPL 2014), xxvii) IEEE/SAE International Conference on Connected Vehicles (ICCVE 2013), xxviii) IEEE Colloquium on Humanities, Science and Engineering Research (CHUSER 2012, 2014), xxix) IEEE International Symposium on VLSI (ISVLSI 2013), xxx) IEEE Symposium on Industrial Electronics and Applications (ISIEA 2013), xxxi) Pan-Hellenic Conference on Informatics (PCI 2012, 2014), xxxii) International Symposium on Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC 2012,2013,2014), xxxiii) Jordanian International Electrical and Electronics Engineering Conference (JIEEEC 2013), xxxiv) ICST Conference on Wireless Mobile Communication and Healthcare (MobiHealth 2011), xxxv) IEEE Symposium on Humanities, Science and Engineering Research (SHUSER 2013), xxvi) IEEE International Conference on Microelectronics (ICM 2012, 2013, 2014), xxvii) IEEE International Workshop on Quality of Multimedia Experience (QoMEX 2015).

Κρίσεις βιβλίων

1. William Stallings, "**Computer Organization and Architecture**", 10th edition, Pearson, 2014 (έκδοση το 2015).
2. Κωνσταντίνος Χωριανόπουλος, "Σχεδίαση και Ανάλυση Συστημάτων Υλικού-Λογισμικού (ΣΔΥ 60)", Τόμος Α - " **Σχεδιασμός Διάδρασης και Συσκευών**", Α' Έκδοση, Ελληνικό Ανοικτό Πανεπιστήμιο, Πάτρα 2013-σήμερα
3. Παρασκευάς Κίτσος, "**Ενσωματωμένα Συστήματα** (ΣΔΥ 62)" Τόμος Α, Α' Έκδοση, Ελληνικό Ανοικτό Πανεπιστήμιο, Πάτρα 2012-σήμερα
4. Δημήτριος Νικολός, "Ψηφιακά Συστήματα" Τόμος Β - "**Αρχιτεκτονική Υπολογιστών**", Β' Έκδοση, Ελληνικό Ανοικτό Πανεπιστήμιο, Πάτρα 2008, ISBN 978-960-538-753-2 (Κριτική ανάγνωση)

5. Γεώργιος Αλεξίου, "Ψηφιακά Συστήματα" Τόμος Γ - "**Μικροεπεξεργαστές**", Β' Έκδοση, Ελληνικό Ανοικτό Πανεπιστήμιο, Πάτρα 2008, ISBN 978-960-538-745-7 (Κριτική ανάγνωση)
6. Κριτής συγγράμματος στο πρόγραμμα «Κάλλιπος - Ακαδημαϊκά Ηλεκτρονικά Συγγράμματα και Βοηθήματα για Επιστήμες Μηχανικών και Πληροφορική» (διατίθενται πληροφορίες εφόσον ζητηθούν)

Συμμετοχή σε Επιτροπές

- **Εθνικός Αντιπρόσωπος (Delegate)** του Ελληνικού Παραρτήματος στο IEEE R8 Committee Meeting (2008, 2009,2012,2014)
- **Chairman** του Executive Committee του IEEE Consumer Electronics Society - Greece Chapter (2011-σήμερα)
- Μέλος του Συμβουλίου του Ελληνικού **IEEE GOLD Affinity Group** (2008-2010)
- **Μέλος επιτροπής αξιολόγησης** Best Student Paper για το Panhellenic Conference on Artificial Intelligence 2012
- **Μέλος** Ομάδας Εργασίας ΕΕΛ/ΛΑΚ «Ανοικτές Άδειες» (2013-σήμερα)
- **Μέλος** Ομάδας Εργασίας ΕΕΛ/ΛΑΚ «Ανοικτές Τεχνολογίες Υλικού» (2013-σήμερα)
- **Μέλος** Ομάδας Έρευνας «Τεχνολογίες Πληροφορικής και Επικοινωνιών», Περιφερειακός Πόλος Καινοτομίας – Περιφέρεια Δυτικής Ελλάδας, Οριζόντια Δράση 3: «Τεχνολογική Προοπτική Διεύρυνση στην Περιφέρεια Δυτικής Ελλάδας», 2008
- **Μέλος του Organizing Committee** (Publicity Chair) του i) IEEE International Symposium on Circuits and Systems (ISCAS) 2006, ii) IEEE International Conference on Emerging Technologies and Factory Automation (ETFA) 2007, iii) IEEE International Symposium on Wireless Pervasive Computing (SWPC) 2008, iv) IEEE International Conference on Circuits, Electronics, and Systems (ICECS 2010), v) 2nd International ICST Conference on Wireless Mobile Communication and Healthcare (MobiHealth 2012), vi) IEEE MELECON 2012, vii) IEEE 18th International Conference on Digital Signal Processing (DSP 2013), viii) . 2nd International ICST Conference on Wireless Mobile Communication and Healthcare (MobiHealth 2014), ix) 6th International Symposium on Communications, Control, and Signal Processing (ISCCSP 2014)
- **Μέλος του Program Committee** του i) International Conference on Computer Design (CDES-2005), ii) International Conference on Computational Intelligence (ICCI 2005), iii) International Conference on Information Security (ICIS 2005), iv) International Conference on Artificial Intelligence (ICAI 2005), v) International

Conference on Image Analysis (ICIA 2005), vi) International Conference on Data Analysis (ICDA 2005), vii) International Conference on Machine Intelligence (ICMI 2005), viii) International Conference on Automation Technology (ICAT 2005), ix) International Conference on Communication Technology (ICCT 2006), x) International Conference on Pattern Analysis (ICPA 2006), ix) International Conference on Neural Networks (ICNN 2006), xi) IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS2010), xii) 15th IEEE Mediterranean Electrotechnical Conference (MELECON 2010), xiii) IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS2011), xiv) 6th International conference on Design & Technology of Integrated Systems in nanoscale era (DTIS 2011), xv) 2011 International Conference on Network Computing and Information Security (NCIS 2011), xvi) International Conference on Microelectronics (ICM 2011), xvii) IEEE Symposium on Computers and Communications (ISCC 2011), xviii) 1st AI in Education Workshop: Innovations and Applications (AIeIA 2012), xix) 2012 International Symposium on Consumer Electronics (ISCE 2012), xx) 7th International Conference on Embedded and Multimedia Computing (EMC 2012), xxi) 18th Panhellenic Conference on Informatics (PCI 2012), xxii). 7th International Workshop on Reconfigurable and Communication-centric Systems-on-Chip (ReCoSoC 2012), xxiii) International Conference on Microelectronics (ICM 2013), xxiv) 8th International Workshop on Reconfigurable and Communication-centric Systems-on-Chip (ReCoSoC 2013), xxv) 6th International Symposium on Communications, Control, and Signal Processing (ISCCSP 2014), xxvi) 18th Panhellenic Conference on Informatics (PCI 2014), xxvii) 4th special session on Mobile Device & Web Software Development - Small Systems Development (in conjunction with PCI 2014), xxviii) 24th International Conference on Field Programmable Logic and Applications (FPL2014), xxix) IEEE Symposium on Computers and Communication (ISCC 2014), xxx) 2014 International Conference on Connected Vehicles & Expo (ICCVE 2014), xxxi) 9th International Workshop on Reconfigurable and Communication-centric Systems-on-Chip (ReCoSoC 2014), xxxii) International Conference on Microelectronics (ICM 2013), xxxiii) International Conference on Microelectronics (ICM 2014)

Άλλα

- **Session Chair** στα ICECS 2010, DSP 2011
- **Special Session Organizer** στο ICECS 2010 με τίτλο “Tools, Techniques & Circuits for low-power consumer electronics”

- **Track co-chair** "Circuits and Systems for Signal Processing" στο 16th International Conference on Computer as a Tool (EUROCON 2015)
- **Track co-chair** "Architectures and VLSI Systems" στο International Conference on Microelectronics (ICM 2011)
- **Υπεύθυνος δημοσιότητας** του IEEE Greece Section (2011-σήμερα)
- **IEEE Day Ambassador** στην Ελλάδα (2013,2014)
- Υπεύθυνος για την έκδοση του διμηνιαίου ενημερωτικού φυλλαδίου της Ελληνικής κοινότητας Circuit and Systems του IEEE (2003-2006)
- **Ιδρυτής και Counsellor Professor** του IEEE Student Branch του ΤΕΙ Ιονίων Νήσων (2012-σήμερα).
- **Ιδρυτής και Counsellor Professor** του IEEE Student Branch του Πανεπιστημίου Κεντρικής Ελλάδας (2008-2013).
- **Mentor** του IEEE Student Branch του Πανεπιστημίου Θεσσαλίας-Λαμία (2014).
- **Ιδρυτής και Counsellor Professor** του IEEE EMBS Student Club του Πανεπιστημίου Κεντρικής Ελλάδας (2009-2011).
- **Διαιτητής (Proctor)** των IEEEXtreme Programming Contest για το Πανεπιστήμιο Κεντρικής Ελλάδας (2009-2012) και του Πανεπιστημίου Θεσσαλίας (2013)
- **Διοργανωτής** του ετήσιου θεσμού της ημερίδας Τεχνολογίας στο Τμήμα Πληροφορικής με Εφαρμογές στη Βιοϊατρική, Πανεπιστήμιο Θεσσαλίας (πρώην Πανεπιστήμιο Στερεάς Ελλάδας)
- **Εκπρόσωπος** του Τμήματος Πληροφορικής με Εφαρμογές στη Βιοϊατρική, Πανεπιστήμιο Θεσσαλίας (πρώην Πανεπιστήμιο Στερεάς Ελλάδας) για την εγγραφή και συμμετοχή του Τμήματος στο si-Cluster του Corallia (2011).
- **Liaison** του Τμήματος Πληροφορικής με Εφαρμογές στη Βιοϊατρική, Πανεπιστήμιο Θεσσαλίας με τις εταιρίες ARM και Xilinx (University Programs).

VIII. ΔΙΑΚΡΙΣΕΙΣ-ΒΡΑΒΕΙΑ

• Βραβείο «IEEE Outstanding Branch Counselor and Advisor Award Recognition Program» 2012, ως University of Central Greece IEEE Student Branch Counselor

• Ε. Αρβανίτη, Α. Κακαρούντας (ομάδα BrainArk), «Ανάπτυξη συσκευής υποστήριξης σε άτομα με Διαταραχές Λόγου Νευρολογικής Φύσεως», 3ο βραβείο στο Hellenic Startup BioMed 2012

• Βραβείο "Best CAS Chapter of the Year" (2004) στο Ελληνικό Παράρτημα Κυκλωμάτων και Συστημάτων (Greece Circuits and Systems Chapter) του IEEE, όταν εκτελούσε χρέη βοηθού του προέδρου καθ. Α. Σκόδρα. Συν-συγγραφέας της αναφοράς βάσει της οποία βραβεύτηκε το παράρτημα.

• Ως μεταδιδάκτορας οργάνωσε δύο ομάδες φοιτητών, τα έτη 2004 και 2005 αντίστοιχα, προκειμένου να ασχοληθούν, οι φοιτητές, με πιο εξειδικευμένα θέματα στο αντικείμενο «Σχεδιασμός Ολοκληρωμένων Κυκλωμάτων». Η ομάδα του 2004 έχει βραβευθεί από το τοπικό (Πάτρα) παράρτημα φοιτητών του IEEE (IEEE Patras Student Branch) για την καλύτερη επιστημονική εργασία για το 2004, ενώ η ίδια εργασία προκρίθηκε στους τελικούς (5 φιναλίστ) του IEEE Region 8, καταλαμβάνοντας την τρίτη θέση. Το 2005, η δεύτερη ομάδα έλαβε τη δεύτερη θέση στον ίδιο διαγωνισμό.

• Διεθνές βραβείο από EUROPRACTICE για τα αποτελέσματα του Ερευνητικού Ευρωπαϊκού Προγράμματος COSAFE #28593 "Low Power Hardware-Software Co-Design for Safety-Critical Applications", ύστερα από διεθνή διαγωνισμό στην Ευρώπη (Design Contest) που απονεμήθηκε στα πλαίσια του Συνεδρίου Design Automation and Testing in Europe (DATE), που πραγματοποιήθηκε το διάστημα 4-8 Μαρτίου 2003, Παρίσι, Γαλλία.

• Διεθνές βραβείο από Mentor Graphics και SUN Microsystems για τα αποτελέσματα του Ερευνητικού Ευρωπαϊκού Προγράμματος COSAFE #28593 "Low Power Hardware-Software Co-Design for Safety-Critical Applications", ύστερα από διεθνή φοιτητικό διαγωνισμό (Student Design Contest) 2002.

ΙΧ. ΔΗΜΟΣΙΕΥΣΕΙΣ

Α. ΔΙΑΤΡΙΒΕΣ

Α.1 ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ.

«Σχεδιασμός Κυκλωμάτων Ασφαλούς Λειτουργίας με Χαμηλή Κατανάλωση Ισχύος», Διδακτορική διατριβή, Πανεπιστήμιο Πατρών, Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών, 2004.

Α.2 ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ (Master)

-

Α.3 ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Σχεδιασμός Ολοκληρωμένου Συστήματος για την Μέτρηση των Οξέων του Πεπτικού Συστήματος», Πανεπιστήμιο Πατρών, Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών, 1998

Β. ΣΥΓΓΡΑΜΜΑΤΑ-ΣΗΜΕΙΩΣΕΙΣ

Β.1 Οδηγός χρήσης και υποδειγματικές ασκήσεις της πλατφόρμας ανάπτυξης Mentor Graphics για το μάθημα «Σχεδιασμός Ολοκληρωμένων Συστημάτων με Τεχνικές VLSI», Κων/νος Γκούτης, **Αθ. Κακαρούντας**, Ε. Φωτοπούλου, για το Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών, Πανεπιστήμιο Πατρών, (ΕΠΕΑΚ ΙΙ – ΠΕ3, 2004)

Β.2 Οδηγός χρήσης και υποδειγματικές ασκήσεις της πλατφόρμας ανάπτυξης Mentor Graphics για το μάθημα «Σχεδιασμός Ολοκληρωμένων Κυκλωμάτων Ι», Κων/νος Γκούτης, **Αθ. Κακαρούντας**, για το Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών, Πανεπιστήμιο Πατρών, (ΕΠΕΑΚ ΙΙ – ΠΕ3, 2004)

Β.3 Οδηγός χρήσης και υποδειγματικές ασκήσεις της πλατφόρμας ανάπτυξης Mentor Graphics για το μάθημα «Σχεδιασμός Ολοκληρωμένων Κυκλωμάτων ΙΙ», Κων/νος Γκούτης, **Αθ. Κακαρούντας**, για το Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών, Πανεπιστήμιο Πατρών, (ΕΠΕΑΚ ΙΙ – ΠΕ3, 2004)

Β.4 Επίσημη μετάφραση (ως συμμετέχων στην ομάδα ανάπτυξης) - οδηγός χρήσης του Logisim (**Αθ. Κακαρούντας**) για το μάθημα «Ψηφιακή Λογική» του ΤΕΙ Ιονίων Νήσων (2009)

Β.5 V.A. Pedroni, "Σχεδίαση Κυκλωμάτων με χρήση της VHDL". Έκδοση από τις εκδόσεις Κλειδάριθμος. ISBN: 978-960-461-118-8 (Επιμέλεια – Μετάφραση στην Ελληνική γλώσσα Γ. Θεοδωρίδης, Σ. Νικολαΐδης, Δ. Σούντρης, **Αθ. Κακαρούντας**)

Β.6 Ν. Ασημάκης, Γ. Βουρβουλάκης, **Αθ. Κακαρούντας**, Ν. Λελίγκου: «Λογική Σχεδίαση», e-book, ISBN: 978-960-87539-2-1, 2011.

Γ. ΚΕΦΑΛΑΙΑ ΣΕ ΒΙΒΛΙΑ

Γ.1 ***A.P. Kakarountas**, K.S. Papadomanolakis, C.E. Goutis, "Low-Power Design for Safety-Critical Applications" in "Designing CMOS Circuits for Low Power," editors D. Soudris, C. Piguet, and C.E. Goutis, September 2002, Dordrecht/London/Boston, Kluwer Academic Publishers, pp. 205–234, September 2002.*

Γ.2 ***Α. Κακαρούντας**, Ρ.Ε. Κινγκ, «Κεφάλαιο 11: Προσομοίωση και Εικονική Πραγματικότητα», στο βιβλίο «Βιομηχανική Πληροφορική», εκδόσεις Τζιόλα, 2004.*

Γ.3 ***A.P. Kakarountas**, H.E. Michail, "Performance for Cryptography: hardware and software approach", in "Supercomputing Research Advances", Ed. Yongge Huang, Nova Science Publishers, Inc., ISBN: 978-1-60456-186-9, 2008, pp. 403-418.*

Γ.4 ***A.P. Kakarountas**, H.E. Michail, "Performance for Cryptography: a hardware approach", in "Cryptography Research Perspectives", Ed. Roland E. Chen, Nova Science Publishers, Inc., ISBN: 978-1-60456-492-1, 2009, pp. –*

Δ. ΔΙΕΘΝΗ ΠΕΡΙΟΔΙΚΑ ΜΕ ΚΡΙΤΕΣ

Δ.1 ***S. Nikolaidis, E. Karaolis, A. Kakarountas, K. Papadomanolakis and C.E. Goutis**, "A Methodology for Calculating the Undetactable Double-Faults in Self-Checking Circuits", Journal of Circuits, Systems and Computers, World Scientific, Vol. 12, No. 1, pp. 75-91, February 2003.*

Δ.2 ***A. Milidonis, G. Dimitroulakos, M. D. Galanis, A. P. Kakarountas, G. Theodoridis, C.Goutis, and F.Catthoor**, "A Framework for Data Partitioning for C++ Data-Intensive Applications", Journal of Design Automation for Embedded Systems, Springer Science+Business Media B.V., Vol. 9, No. 2, pp. 101-121, June. 2005.*

Δ.3 ***M.D. Galanis, A. Milidonis, A.P. Kakarountas, and C.E. Goutis**, "A Design Flow for Speeding-up DSP Applications in Heterogeneous Reconfigurable Systems", Microelectronics Journal, Elsevier, vol 37, pp. 554-564, 2006.*

Δ.4 ***A.P. Kakarountas, H. Michail, A. Milidonis, G. Theodoridis, C.E Goutis**, "High-Speed FPGA Implementation of Secure Hash Algorithm for IPSec and VPN Applications", Journal of Supercomputing, Springer Science + Business Media, vol. 37, pp. 179–195, 2006.*

Δ.5 ***H.E. Michail, A.P. Kakarountas, A.Milidonis, C.E. Goutis****, "Efficient FPGA Implementation of Novel Cryptographic Hashing Core", Computing Letters, VSP/Brill Publishing, vol. 2, num. 1-2, pp. 21-27(7), 2006.*

Δ.6 ***I. Yiakoumis, M. Papadonikolakis, H.E. Michail, A.P. Kakarountas, C.E. Goutis*** *"Maximizing the hash function of authentication codes", IEEE Potentials, vol. 25, iss. 2, pp. 9–12, 2006.*

Δ.7 ***H.E. Michail, A.P. Kakarountas, C.E. Goutis*** *"Server Side Hashing Core Exceeding 3 Gbps of Throughput", International Journal of Network Security (special issue), Vol. 1, Nos. 1/2/3, pp. 43–53, 2007.*

Δ.8 ***A.P. Kakarountas, N.D. Zervas, H.E. Michail, G. Theodoridis, and D. Soudris****, "Power Management through Dynamic Frequency Scaling for Low and Medium bit-rate Digital Receivers", Journal of Low Power Electronics, ASP, vol.2, no 3, pp. 356–364, 2006.*

Δ.9 ***G. N. Selimis, A.P. Kakarountas, A. P. Fournaris, A. Milidonis and O.Koufopavlou****, "A Low Power Design for SBOX Cryptographic Primitive of Advanced Encryption Standard for Mobile End-Users", in Journal of Low Power Electronics, ASP, vol.3, no.3, pp. 327-336, 2007.*

Δ.10 ***H.E. Michail, A. P. Kakarountas, A. S. Milidonis and C. E. Goutis****, "A Top-Down Design Methodology for Implementing Ultra High-Speed Hashing Cores", IEEE Transactions on Dependable and Secure Computing, vol.6, is.4, pp.255-268, 2009.*

Δ.11 ***M. Papadonikolakis, A.P. Kakarountas, C.E. Goutis****, "Efficient High-Performance Implementation of JPEG-LS Encoder", in Journal of Real-Time Processing, Springer. vol. 3, no. 4, pp 303-310, 2008.*

Δ.12 ***A. Milidonis, V. Porpodas, N. Alachiotis, A. P. Kakarountas, H. Michail, G. Panagiotakopoulos and C. E. Goutis****, "Low Power Architecture with Scratch-Pad Memory for Accelerating Embedded Applications with Run Time Reuse", IET Computers & Digital Techniques, IET, vol. 3, is. 1, pp.109-123, 2009.*

Δ.13 ***D.M. Schinianakis, A.P. Fournaris, A.P. Kakarountas and T. Stouraitis****, "An RNS Architecture of an Fp Elliptic Curve Point Multiplier", IEEE Transactions on Circuits and Systems I, vol.56, no.6, pp. 1202-1213, June 2009.*

Δ.14 ***A.P. Kakarountas, H.E. Michail, C.E. Goutis, A.M. Rjoub****, "High-Throughput Implementation of RipeMD-160", International Journal for Internet Technology and Secured Transactions, Inderscience Ltd, vol. 1, no. 3/4, pp. 309 – 316, 2009.*

Δ.15 ***A. Milidonis, N. Alachiotis, V. Porpodas, H. Michail, G. Panagiotakopoulos, A.P. Kakarountas, C.E. Goutis****, "Decoupled Processors Architecture for Accelerating Data Intensive Applications using Scratch-Pad Memory Hierarchy", Journal of Signal Processing Systems. Springer Science + Business Media, LLC, vol. 59, no.3, pp. 281-296, 2010.*

Δ.16 ***H.E. Michail, A.P. Kakarountas, D. Schinianakis, G. Selimis, C.E. Goutis****, "Cipher Block based Authentication Module: A Hardware Design Perspective", Journal of Circuits, Systems and Computers, World Scientific Publishing, Vol. 20, No. 2, pp. 163-184, 2011.*

Ε. ΔΙΕΘΝΗ ΣΥΝΕΔΡΙΑ ΜΕ ΚΡΙΤΕΣ ΚΑΙ ΠΡΑΚΤΙΚΑ

E.1 **A.P. Kakarountas, K. Papadomanolakis, E. Karaolis, S. Nikolaidis, N. Alachiotis, C.E. Goutis**, "*Hardware and Power Requirements of Self-Checking Circuits*", in Proc. of 6th IEEE International Conference on Electronics, Circuits and Systems (ICECS'99), Pafos, Cyprus, pp 1655-1658, Sept. 1999.

E.2 **A.P. Kakarountas, K. Papadomanolakis, E. Karaolis, S. Nikolaidis, C.E. Goutis,** "*Hardware/Power Requirements vs. Fault Detection Effectiveness in Self-Checking Circuits*", in Proc. of IEEE 1999 International Workshop on Power And Timing Modeling, Optimization and Simulation (PATMOS'99), Kos, Greece, pp. 387-396, Oct. 1999.

E.3 **A.P. Kakarountas, K. Papadomanolakis, V. Kokkinos, C.E. Goutis**, "*Comparative Study on Self-Checking Carry-Propagate Adders in Terms of Area, Power and Performance*", in Proc. of IEEE 2000 International Workshop on Power And Timing Modeling, Optimization and Simulation (PATMOS'00), Göttingen, Germany, pp. 187-194, Sept. 2000.

E.4 **A.P. Kakarountas, V. Kokkinos, C.E. Goutis**, "*Design of Low-Power On-Line Reconfigurable Datapaths Using Self-Checking Circuits*", in Proc. of 8th IEEE International Conference on Electronics, Circuits and Systems (ICECS'01), Malta, vol.III, pp.1565-1568, Sept. 2001.

E.5 **K. Papadomanolakis, A.P. Kakarountas, V. Kokkinos, S. Nikolaidis, C.E. Goutis**, "*Low-Power Design of a Safety Critical Microcontroller*", in Proc. of 1st Conference on Microelectronics, Microsystems and Nanotechnology (MMN'00), Athens, Greece, Nov. 2000.

E.6 **K. Papadomanolakis, A.P. Kakarountas, V. Kokkinos, N. Sklavos, C.E. Goutis**, "*The Effect of Fault Secureness in Low-Power Multiplier Designs*", in Proc. of IEEE 2001 International Workshop on Power And Timing Modeling, Optimization and Simulation (PATMOS'01), Yverdon-Les-Bains, Switzerland, pp. 10.3, Sept. 2001.

E.7 **K. Papadomanolakis, A.P. Kakarountas, V. Kokkinos, N. Sklavos, C.E. Goutis**, "*A Comparative Study on Fault Secure Signed Multiplication Designs*", in Proc. of 11th IFIP International Conference on Very Large Scale Integration (IFIP VLSI-SOC'01), Montpellier, France, pp. 183-188, Dec. 2001.

E.8 **A.P. Kakarountas, K. Papadomanolakis, V. Spiliotopoulos, S. Nikolaidis, C.E. Goutis,** "*Designing a Low-Power Fault-Tolerant Microcontroller for Medicine Infusion Devices*", in Proc. of Design, Automation & Test in Europe (DATE'02), Paris, France, pp. 205-211, March 2002.

E.9 **A.P. Kakarountas, K. Papadomanolakis, S. Nikolaidis, D. Soudris, C.E. Goutis,** "*Confronting Violations of the TSCG(t) in Low-Power Design*", in Proc. of the IEEE 2002 International Symposium on Circuits and Systems (ISCAS'02), Scottsdale, Arizona, USA, pp. 2606-2609, May 2002.

E.10 **N.D. Zervas, S. Theoharis, A.P.Kakarountas, G. Theodoridis, D. Soudris, C.E. Goutis**, "Reducing Power Consumption *through Dynamic Frequency Scaling for a Class of Digital Receivers*", in Proc. of IEEE 2000 International Workshop on Power And Timing Modeling, Optimization and Simulation (PATMOS'00), Göttingen, Germany, pp. 47-55, Sept. 2000.

E.11 **N. Liveris, N.D. Zervas, A.P. Kakarountas, C.E. Goutis**, "*A code Transformation-Based Methodology for Improving I-Cache Performance*", in Proc. of 8th IEEE International Conference on Electronics, Circuits and Systems (ICECS'01), Malta, vol.II, pp.917-920, Sept. 2001.

E.12 **K. Masselos, F. Catthoor, A.P. Kakarountas, C.E. Goutis, H. DeMan**, "*Memory Hierarchy Layer Assignment for Data Re-Use Exploitation in Multimedia Algorithms Realized on Predefined Processor Architectures*", in Proc. of 8th IEEE International Conference on Electronics, Circuits and Systems (ICECS'01), Malta, vol.I, pp.285-288, Sept. 2001.

E.13 **K.S. Papadomanolakis, A.P. Kakarountas, N. Sklavos, C.E. Goutis**, "*A Low-Power Fault-Secure Timer Implementation*", in Proc. of the IEEE 2002 International Conference on Electronics, Circuits and Systems (ICECS'02), Croatia, pp. 537-540, Sept. 2002.

E.14 **A.P. Kakarountas, G. Theodoridis, K.S. Papadomanolakis, C.E. Goutis**, "*A Novel High-Speed Counter with Counting Rate Independent of the Counter's Length*", in Proc. of the IEEE 2003 International Conference on Electronics, Circuits and Systems (ICECS'03), UAE, pp. 1164 - 1167, Dec. 2003.

E.15 **K.S. Papadomanolakis, A.P. Kakarountas, N. Sklavos, C.E. Goutis**, "*A Fast Johnson-Mobius Encoding Scheme for Fault Secure Binary Counters*", in Design, Automation & Test in Europe (DATE'02), Paris, France, Mar. 2002.

E.16 **D. Karatasos, A.P. Kakarountas, G. Theodoridis, C.E. Goutis**, "*A Novel Constant-Time Fault-Secure Binary Counter*", in Proc. of IEEE 2004 Internationsl Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS'04), Santorini island, Greece, Sept. 2004.

E.17 **A.P. Kakarountas, V. Spiliotopoulos, S. Nikolaidis, C.E. Goutis**, "*The Impact of Low-Power Techniques on the Design of Portable Safety-Critical Systems*", in Proc. of the IEEE 2004 International Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS'04), Santorini island, Greece, September 2004.

E.18 **H.E. Michail, A.P. Kakarountas, C.E. Goutis**, "*Efficient Implementation of the Keyed-Hash Message Authentication Code (HMAC) Using the SHA-1 Hash Function*", in Proc. of the IEEE 2004 International Conference on Electronics, Circuits and Systems (ICECS'04), Tel-Aviv, Israel, pp. 567-570, Dec. 2004.

E.19 **A.P. Kakarountas, V. Spiliotopoulos, S. Nikolaidis, C.E. Goutis**, "*COSAFE: Efficient Safety-Critical Portable System*", in Proc. of the IEEE 2004 International Workshop on Biomedical Circuits and Systems (BioCAS'04), Singapore, pp. S1.6(13-16), Dec. 2004.

E.20 **H. Michail, A.P. Kakarountas, O. Koufopavlou, C.E. Goutis**, "*A Low-Power and High-Throughput Implementation of the SHA-1 Hash Function*", in Proc. of IEEE 2005 International Symposium on Circuits and Systems (ISCAS'05), Kobe, Japan, pp. 4086-4089, May 2005.

E.21 **A.P. Kakarountas, H. Michail, C.E. Goutis**, "*Σχεδιασμός Ταχύτατων Κρυπτογραφικών Αλγορίθμων για Διαφύλαξη Απορρήτου και Ακεραιότητας Δεδομένων*", στα πρακτικά του 1ου Πανελλήνιου Συνεδρίου Ηλεκτρολόγων Μηχανικών, Αθήνα, Μάρτιος 2005.

E.22 **H. Michail, A.P. Kakarountas, A. Milidonis, C.E. Goutis**, "*Low Power and High Throughput Implementation of SHA-256 Hash Function*", in Proc. of International E-Conference on Computer Science (IeCCS 2005), pp. 170-173, May 2005.

E.23 **A.P. Kakarountas, G. Theodoridis, T. Laopoulos, C.E. Goutis**, "*A High-Speed FPGA Implementation of the SHA-1 Hash Function*", in Proc. of IEEE Third International Workshop on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS'05), Sofia, Bulgaria, pp. 211-215, Sep. 5-7, 2005.

E.24 **H.E. Michail, A.P. Kakarountas, G.N. Selimis, C.E. Goutis**, "*State-of-the-Art Implementation of SHA-1 Hash Function for Low-Power and High Throughput*", in Proc. of IEEE 2005 International Workshop on Power And Timing Modeling, Optimization and Simulation (PATMOS'05), Leuven, Belgium, pp. 591-600, Sep. 2005.

E.25 **K. Aisopos, A.P. Kakarountas, H. Michail, C.E. Goutis**, "*High throughput implementation of the new Secure Hash Algorithm through partial unrolling*", in Proc. of IEEE 2005 International Workshop on Signal Processing Systems (SiPS'05), Athens, Greece, pp. 99-103, Nov. 2-4, 2005.

E.26 **A. Brokalakis, A.P. Kakarountas, C.E. Goutis**, "*A High-Throughput Area Efficient FPGA Implementation of AES-128 Encryption*", in Proc. of IEEE 2005 International

Workshop on Signal Processing Systems (SiPS'05), Athens, Greece, pp. 116-121, Nov. 2-4, 2005.

E.27 **H. Michail, A. Milidonis, A.P. Kakarountas, C.E. Goutis**, "*Novel High Throughput Implementation of SHA-256 Hash Function Through Pre-Computation Technique*", in Proc. of the IEEE 2005 International Conference on Electronics, Circuits and Systems (ICECS'05), Gammarth, Tunisia, pp. 1-4, Dec. 2005.

E.28 **M. D. Galanis, G. Dimitroulakos, A. P. Kakarountas, and C.E. Goutis**, "*Speedups from Partitioning Software Kernels to FPGA Hardware in Embedded SoCs*", in Proc. of IEEE 2005 International Workshop on Signal Processing Systems (SiPS'05), Athens, Greece, pp. 485-490, Nov. 2-4, 2005.

E.29 **I. Yiakoumis, M. Papadonikolakis, H. Michail, A.P. Kakarountas, C.E. Goutis**, "*Efficient small-sized implementation of the keyed-hash message authentication code*", in Proc. of IEEE 2005 EUROCON as finalist in the IEEE Region 8 Best Student Paper Contest, Belgrade, Yugoslavia, pp. 1875-1878, Nov. 21-24, 2005.

E.30 **D.M. Schinianakis, A.P. Fournaris, A.P. Kakarountas and T. Stouraitis**, "*An RNS Architecture of an Fp Elliptic Curve Point Multiplier*", in Proc. of IEEE International Symposium on Circuits and Systems (ISCAS) 2006, Kos Island, Greece, May 21-24, 2006.

E.31 **F. Aisopos, K. Aisopos, D.M. Schinianakis, H.E. Michail, A.P. Kakarountas**, "*A Novel High-Throughput Implementation of a Partially Unrolled SHA-512*" in Proc. of IEEE Mediterranean Electrotechnical Conference, MELECON 2006, Malaga, Spain, pp. 61-65, May 16-19, 2006.

E.32 **D.M. Schinianakis, A.P. Kakarountas, T. Stouraitis**, "*A New Approach to Elliptic Curve Cryptography: An RNS Architecture*" in Proc. of IEEE Mediterranean Electrotechnical Conference, MELECON 2006, Malaga, Spain, pp. 1241-1245, May 16-19, 2006.

E.33 **H.E. Michail, A.P. Kakarountas, A.S. Milidonis, G.A. Panagiotakopoulos, V.N. Thanasoulis, C. E.Goutis**, "*Temporal and System Level Modifications for High Speed VLSI Implementations of Cryptographic Core*" in Proc. of the IEEE 2006 International Conference on Electronics, Circuits and Systems (ICECS'06), Nice, France, pp. 1180-1183, Dec. 2006.

E.34 **A. Milidonis, N. Alachiotis, V. Porpodas, H. Michail, *A. P. Kakarountas*, and C. E. Goutis**, "*A Decoupled Architecture of Processors with Scratch-Pad Memory Hierarchy*", in Proc. of Design, Automation & Test in Europe (DATE'07), Nice, France, pp. 612-617, April 2007.

E.35 **M. Papadonikolakis, V. Pantazis, and A.P. Kakarountas**, "*Efficient High-Performance ASIC Implementation of JPEG-LS Encoder*", in Proc. of Design, Automation & Test in Europe (DATE'07), Nice, France, pp. 159-164, April 2007.

E.36 **A.P. Kakarountas, H.E. Michail, and C.E. Goutis**, "*RipeMD-160 Implementation Optimized in Terms of Throughput*", in Proc. of 3rd International Conference on Information Technology (ICIT'07), Amman, Jordan, pp. - , May 2007.

E.37 **H.E. Michail, A.P. Kakarountas, G. Selimis and C.E. Goutis**, "*Throughput Optimization of the Cipher Message Authentication Code*", in Proc. of the 2007 IEEE Intl. Conf. on Digital Signal Processing (DSP'07), Cardiff, Wales, UK, pp. 495-498, July 2007.

E.38 **A.P. Kakarountas, H. Michail, C.E. Goutis, and C. Efstathiou**, "*Implementation of HSSec: a High-Speed Cryptographic Co-processor*", in Proc. of the 2007 IEEE Conference on Emerging Technologies and Factory Automation, (ETFA 2007), Patras, Greece, pp. 625-631, Sept. 2007.

E.39 **A. Kakarountas, H. Michail, and C.E. Goutis** "*Integration of a Concurrent Signature Monitoring Mechanism in a System-on-a-Chip*", in Proc. of the 2007 IEEE International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS'07), Rabat, Morocco, pp. 47-51, Sept. 2007.

E.40 **A. P. Kakarountas, H.E. Michail, G. Theodoridis and C. E. Goutis** "*A Segmented High-Speed Counter Based on the Use of Redundant Bits*", in Proc. of the 16th IFIP/IEEE Conference on Very Large Scale Integration (VLSI-SOC'08), Rhodes, Greece, pp. 42 – 48, Oct. 2008.

E.41 **A. Milidonis, V. Porpodas, N. Alachiotis, A. Kakaroudas, H. Michail, G. Panagiotakopoulos and C.E. Goutis**, "*A Scratch-Pad Memory Accelerator for Exploiting Run-Time Reuse*", in Proc. of the 16th IFIP/IEEE Conference on Very Large Scale Integration (VLSI-SOC'08), Rhodes, Greece, pp. 271 – 276, Oct. 2008.

E.42 **D. Schinianakis, A. Kakarountas, T. Stouraitis, A. Skavantzos**, "*Elliptic Curve Point Multiplication in GF(2^n) Using Polynomial Residue Arithmetic*", in Proc. of the IEEE 2009 International Conference on Electronics, Circuits and Systems (ICECS'09), Medina, Tunisia, pp. 980-983, Dec. 2009.

E.43 **E. Hatzidimitriou, A.P. Kakarountas**, "*Implementation of a Low Cost Crypto-System for P1619 (XTS) on FPGA*", in Proc. of 11th International Workshop on Computer Science and Information Technologies (CSIT), Rethymnon, Crete, Greece, pp. 1–4, Oct. 2009.

E.44 **C. Chrysoulas, N. Sklavos, A.P. Kakarountas**, "*Enhancing Service Portability in Upcoming 3G UMTS Networks & Security Aspects*", in Proc. of IEEE Mediterranean Electrotechnical Conference, MELECON 2010, Valetta, Malta, pp. 420-424, April 2010.

E.45 **E. Hatzidimitriou, A.P. Kakarountas**, "*Implementation of a P1619 Crypto-Core for Shared Storage Media*", in Proc. of IEEE Mediterranean Electrotechnical Conference, MELECON 2010, Valetta, Malta, pp. 597-601, April 2010.

E.46 **E. Arvaniti, I. Mavridis, A. Kakarountas**, "*Exploration of 2D Cellular Automata as Binary Sequence Generators*", in Proc. of IEEE Computer Society Annual Symposium on VLSI, ISVLSI 2010, Lixouri Kefalonia, Greece, pp. 41-45, July 2010.

E.47 **D. Tychalas, A. Kakarountas**, "*Planning and Development of the Backend Software for an Electronic Health Record Client based on the Android Platform*", in Proc. of 14th Panhellenic Conference on Informatics, PCI 2010, Tripoli, Greece, pp. 3-6, September 2010.

E.48 **E. Hatzidimitriou, A.P. Kakarountas, A. Milidonis**, "*Exploration and Enhancement of P1619-Based Crypto-Cores for Efficient Performance*", in Proc. of the IEEE 2011 International Conference on Consumer Electronics (ICCE'11), Las Vegas, Nevada, USA, pp. 369-370, Jan. 2011.

E.49 **A.P. Kakarountas, E. Hatzidimitriou, A. Milidonis**, "*A Survey on Throughput-Efficient Architectures for IEEE P1619 for Shared Storage Media*", in Proc. of the 16th IEEE symposium on Computers and Communications, ISCC 2011, Corfu, Greece, pp. 758-763, June 2011.

E.50 **A.P. Kakarountas, E. Hatzidimitriou, A. Milidonis**, "*High-Throughput ASIC Implementation of an Encryption Core for Securing Shared Storage Media*", in Proc. of the 17th International Conference on Digital Signal Processing, DSP 2011, Corfu, Greece, pp. – (TC3.1), July 2011.

E.51 **A.P. Kakarountas, I. Mavridis**, "*Efficient Exploitation of Parallel Computing on the Server-Side of Health Organizations' Intranet for Distributing Medical Images to Smart Devices*", in Proc. of the 2nd International ICST Conference on Wireless Mobile Communication and Healthcare, Mobihealth 2011, Kos Island, Greece, pp. , October 2011.

Μετά το διορισμό στην θέση του Επίκουρου Καθηγητή (Τ.Ε.Ι. Ιονίων Νήσων)

E.52 **A.P. Kakarountas, E. Hatzidimitriou, P. Kitsos**, "*Cipher Text Stealing Integrated in Implementations of IEEE P1619 for Shared Storage Media*", in Proc. of the 6th International Symposium on Communications, Control, and Signal Processing, ISCCSP 2014, Athens, Greece, pp. 574 - 577, May 2014.

E.53 **A.P. Kakarountas, S. Dragoumanos, K. Kakarountas**, "*Extending Visitor's Reality at Museums*", in Proc. of the 5th International Conference on Information, Intelligence, Systems and Applications, IISA 2014, Chania, Greece, pp. 196 - 200, July 2014.

E.54 **P. Christodoulou, I. Diamantis, S. Dragoumanos, A.P. Kakarountas**, "*A Marketing Tool Based on Games for Smart Devices*", accepted for inclusion in Proc. of the 18th Panhellenic Conference on Informatics (PCI 2014), Athens, Greece, pp. - , October 2014.

E.55 **A.P. Kakarountas**, "*Disappearing Computing for Elderly Assisted Living*", accepted for inclusion in Proc. of the 4th International Conference on Wireless Mobile Communication and Healthcare, Mobihealth 2014, Athens, Greece, pp. - , November 2014.

E.56 **A.P. Kakarountas**, "*Safety and Security for Shared Storage Media*", accepted for inclusion in Proc. of the 3rd Pan-Hellenic Conference on Electronics and Telecommunications, PACET 2015, Ioannina, Greece, pp. - , May 2015.

ΣΤ. ΆΛΛΕΣ ΔΗΜΟΣΙΕΥΣΕΙΣ (Συνέδρια δίχως κριτές, Μη επιστημονικά περιοδικά, Τεχνικές αναφορές κ.λ.π.)

1. *Athanasios Kakarountas, "Greek Chapter Starts Its Life Cycle with Distinguished Lecturer Talk", IEEE Consumer Electronics Magazine, pp. 15, Jan. 2012.*
2. *Άρθρο στο The Economist (ένθετο περιοδικό της εφημερίδας «Η Καθημερινή») με τίτλο «Η εποχή της αυτοδιάγνωσης», σελ. 92, τεύχος 46, Δεκ. 2007.*

Z. ΕΡΓΑΣΙΕΣ ΠΟΥ ΕΧΟΥΝ ΥΠΟΒΛΗΘΕΙ

Z.1 ***A.P. Kakarountas,*** *"P1619 – Hardware Implementations review from an architectural perspective", IEEE Transactions on Circuits and Systems II*

Z.2 ***A.P. Kakarountas****, I. Mavridis, "Remote Parallel Processing for Displaying Medical Images on Smart Devices", IEEE Transactions on Biomedical Engineering*

Z.3 ***A.P. Kakarountas****, S. Dragoumanos, K. Kakarountas, "Extending Visitor's Reality at Museums", Int. J. of Computational Intelligence Studies, Special Issue on: "Computational Intelligence in Cultural Informatics"*

Z.4 ***A.P. Kakarountas****, "Cellular Automata for Single Step Forward Counters", IEEE Transactions on Computers*

Z.5 ***A.P. Kakarountas****, H.E. Michail, "Hardware Exploration of SHA-1 like Hash Cores Tolerant to Power Attacks", EUROCON 2015*

Z.6 ***A.P. Kakarountas****, H.E. Michail, "SHA-256 Hardware Exploration for FPGA and ASIC Technologies", EUROCON 2015*

Z.7 S. Dragoumanos, ***A.P. Kakarountas****, "Interactivity with gestures (Part I)", IEEE Consumer Electronics Society's Magazine*

Z.8 ***A.P. Kakarountas****, E. Arvaniti, S. Dragoumanos, "Brain-Computing for on an Embedded Portable System for Disabled Patients due to Neurological Cause", IEEE Transactions on Biomedical Engineering*

Z.9 S. Dragoumanos, ***A.P. Kakarountas****, "Interactivity with gestures (Part II)", IEEE Consumer Electronics Society's Magazine (To be submitted on November)*

Z.10 ***A.P. Kakarountas,*** *"A TSC P1619 compatible core", Journal of Engineering Science and Technology Review - JESTR*

ΧΙ. ΑΝΑΛΥΣΗ ΤΩΝ ΕΡΓΑΣΙΩΝ (ΔΗΜΟΣΙΕΥΣΕΩΝ)

Α. ΔΙΑΤΡΙΒΕΣ

Α.1 ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ.

«*Σχεδιασμός Κυκλωμάτων Ασφαλούς Λειτουργίας με Χαμηλή Κατανάλωση Ισχύος*», Παν/μιο Πατρών, Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών, 2004.

Στη διδακτορική διατριβή προσφέρονται σχεδιαστικές λύσεις σε θέματα που άπτονται της Σχεδίασης για Δοκιμή (Design for Testing) για φορητές Εφαρμογές Κρίσιμης Ασφαλείας (Safety Critical Applications). Εφαρμογές κρίσιμης ασφαλείας θεωρούνται, από τα διεθνή πρότυπα, όλες εκείνες οι οποίες συντηρούν, υποβοηθούν ή επηρεάζουν το ανθρώπινο σύνολο, είτε πρόκειται για μεμονωμένο άτομο ή για πλήθος ανθρώπων. Οι πλειοψηφία των φορητών εφαρμογών κρίσιμης ασφαλείας συναντάται στο χώρο των ιατρικών συσκευών. Τέτοιου είδους συσκευές είναι ο βηματοδότης, η αντλία έγχυσης φαρμάκου κ.ο.κ. Τα πρότυπα επιτάσσουν τον σχεδιασμό αυτών των συστημάτων με τέτοιο τρόπο ώστε η λειτουργία τους να κινείται μέσα σε αυστηρά πλαίσια ασφαλείας.

Τα κριτήρια σχεδιασμού συστημάτων που στόχο έχουν την αγορά των ιατρικών συσκευών είναι η αξιοπιστία και η έγκαιρη ανίχνευση σφάλματος κατά τη λειτουργία. Η αξιοπιστία ενός συστήματος επιτυγχάνεται μέσω της ποιότητας του υλικού που χρησιμοποιείται προκειμένου να μην είναι ιδιαίτερα δεκτικό σε σφάλματα όπως π.χ. η ακτινοβολία. Επιπλέον μέτρα που λαμβάνονται, στην πλειονότητα των υπαρχόντων συσκευών, κυρίως λόγω κόστους των αξιόπιστων υλικών και τεχνολογιών, είναι η χρήση πολλαπλών ομοίων μονάδων προκειμένου να επιτευχθεί αξιοπιστία λόγω πλεονασμού. Αυτή η τεχνική παρέχει μία τυπική μορφή ανίχνευσης σφάλματος κατά την εμφάνισή του. Άλλες τεχνικές ανίχνευσης σφάλματος οι οποίες ακολουθούνται είναι ο πλεονασμός λογισμικού καθώς και ο ενσωματωμένος αυτοέλεγχος (Built-In Self-Test, BIST). Οι προαναφερθέντες τεχνικές παρουσιάζουν είτε χαμηλή αξιοπιστία, είτε δεν επιτυγχάνουν να συμμορφωθούν με τα χρονικά κριτήρια της ανίχνευσης του σφάλματος. Αυτά τα χαρακτηριστικά του σχεδιασμού, τα οποία δεν επιτυγχάνονται από τις προαναφερθέντες τεχνικές, αποτέλεσαν το στόχο της παρούσας διατριβής.

Η ερευνητική διαδικασία που ακολουθήθηκε και παρουσιάζεται, ασχολείται με το σχεδιασμό κυκλωμάτων ταυτόχρονου ελέγχου με την κανονική λειτουργία (Concurrent Testing). Προτείνεται μία πλήρης μεθοδολογία ανάπτυξης τέτοιων εφαρμογών, από την φάση των προδιαγραφών μέχρι την ολοκλήρωσή τους σε επίπεδο συστήματος. Όλοι οι σχεδιασμοί κυκλωμάτων βασίστηκαν στη χρήση ειδικών κωδικοποιήσεων προκειμένου να επιτευχθεί η ασφαλής διάδοση των εσωτερικών σημάτων του συστήματος. Οι τεχνικές και οι κωδικοποιήσεις, που χρησιμοποιήθηκαν, παρουσιάζονται και αναλύονται ανά επίπεδο σχεδιασμού.

Στα πλαίσια της παρουσιαζόμενης μεθοδολογίας ορίζεται εξ αρχής ένα μοντέλο σφάλματος που διέπει το σύνολο της ροής σχεδιασμού και ανάπτυξης ενός συστήματος κρίσιμης ασφαλείας. Επιπλέον, ορίζεται ένα στατιστικό μέτρο αξιολόγησης, εμπλουτισμένο με τη πιθανότητα δραστηριότητας των γραμμών, προκειμένου να μετρηθεί η αξιοπιστία των

κυκλωμάτων. Ένα εργαλείο, το FSES (Fault-Secure Evaluation Script), αναπτύχθηκε για την αυτόματη αξιολόγηση το οποίο αναφέρεται ειδικά στην ταυτόχρονη δοκιμή κυκλώματος και λαμβάνει για πρώτη φορά υπ' όψιν ξεχωριστά τα χαρακτηριστικά της λειτουργίας της κάθε εφαρμογής. Έτσι, η επιλογή της κατάλληλης κωδικοποίησης παύει να λειτουργεί διαισθητικά αλλά καθοδηγείται από πειραματικά και ακριβή στοιχεία.

Για την ανάπτυξη ενός συστήματος από την αρχή, δημιουργήθηκε μία βιβλιοθήκη που περιέχει παραμετροποιημένες γεννήτριες κυκλωμάτων σε επίπεδο περιγραφής, ως προς το εύρος των δεδομένων όσο και προς την κωδικοποίηση, αυτοεξεταζόμενων κυκλωμάτων (Self-Checking circuits). Αυτός ο τύπος κυκλωμάτων επιτρέπει την ανίχνευση σφάλματος σχεδόν σε πραγματικό χρόνο. Έτσι παρέχεται στον σχεδιαστή του συστήματος όλο το φάσμα των βασικών μονάδων που ενσωματώνονται σε ένα σύστημα προκειμένου να αναπτύξει την εφαρμογή από το επίπεδο Κυκλώματος.

Στο επίπεδο Καταχωρητή, παρουσιάζονται όλες οι δομές που μπορούν να χρησιμοποιηθούν. Επιπλέον, παρέχονται κανόνες σχεδίασης και διασύνδεσης των μονάδων προκειμένου να διατηρηθεί το επίπεδο αξιοπιστίας. Διάφορες τεχνικές ΣΧΚΕ αξιολογούνται και τροποποιούνται προκειμένου να μην παραβιάζονται οι προδιαγραφές της ταυτόχρονης ανίχνευσης σφάλματος.

Στο επίπεδο Συστήματος αναφέρονται όλες οι μονάδες οι οποίες υποβοηθούν ένα σύστημα στη λειτουργία του και προτείνονται μηχανισμοί για την αύξηση της παρατηρησιμότητας (Observability). Επιπλέον, εισάγονται εξειδικευμένοι μηχανισμοί οι οποίοι αναλαμβάνουν την διαρκή παρατήρηση του συστήματος για την ορθή εκτέλεση των διαδικασιών. Σε περίπτωση σφάλματος, ανάλογα με το βαθμό επίδρασής του στη λειτουργία του συστήματος, είτε παράγεται ακολουθία προειδοποιήσεων είτε γίνεται ασφαλή επανεκκίνηση και αποκατάσταση της λειτουργίας. Σε αυτό το επίπεδο παρουσιάζεται και μία τεχνική διατήρησης της συνοχής εκτέλεσης του κώδικα της εφαρμογής προκειμένου να ελεγχθούν ανεπιθύμητες αλλαγές στην ροή του. Προκειμένου να επιτευχθεί ο κύριος στόχος της διδακτορικής διατριβής, ολοκληρώνεται η δημιουργία της μεθοδολογίας συμπληρώνοντας την με την ανάπτυξη του κατάλληλου αναπτυξιακού συστήματος σε λογισμικό. Δεδομένου ότι η διδακτορική έρευνα συνέπεσε με την πραγματοποίηση του ερευνητικού προγράμματος CoSafe ("COSAFE : Low Power Hardware-Software Co-Design for Safety-Critical Applications" , IST-1998-28593), η ανάπτυξη του λογισμικού που υποστηρίζει το αναπτυσσόμενο υλικό, πραγματοποιήθηκε ταυτόχρονα, σε μια κοινή φάση συσχεδιασμού υλικού-λογισμικού. Το αναπτυξιακό λογισμικό περιελάμβανε, εκτός από εξομοιωτές σφαλμάτων (fault simulators) και εκτιμητές κατανάλωσης (power estimators), ένα πλήρες παραθυρικό περιβάλλον ανάπτυξης κώδικα, αποσφαλμάτωσης και συμβολομετάφρασής του για το υπό ανάπτυξη σύστημα.

Επιπλέον, λόγω της προϋπόθεσης της φορητότητας, η διατριβή ασχολείται, όπου εμπίπτει δυνατότητα, με τον εμπλουτισμό του σχεδιασμού ενός συστήματος κρίσιμης ασφαλείας με τον Σχεδιασμό για Χαμηλή Κατανάλωση Ενέργειας (ΣΧΚΕ, Low-Power Design). Από τα πρώτα κεφάλαια της διατριβής αποδεικνύεται ο αντιφατικός χαρακτήρας των δύο τεχνικών σχεδιασμού και αναδεικνύονται τόσο τα σημεία σύγκλισης όσο και οι συνήθεις κανόνες σχεδιασμού που θα πρέπει να αποφεύγονται. Ειδικά σε μερικές περιπτώσεις κυκλωμάτων, ανάλογα με την κωδικοποίηση που χρησιμοποιείται, επιτυγχάνεται μέχρι και 40% μείωση της καταναλισκόμενης ενέργειας.

Τέλος, η μεθοδολογία εφαρμόστηκε για την ανάπτυξη ενός πρότυπου φορητού

συστήματος για την έγχυση ινσουλίνης σε διαβητικούς. Αναπτύχθηκε ένας προγραμματιζόμενος μικροελεγκτής, ο οποίος συμπεριλαμβάνει προγραμματιζόμενο ολισθητή, πολλαπλασιαστή και πλήρη Αριθμητική και Λογική Μονάδα. Χρησιμοποιεί για λόγους συμβατότητας, προκειμένου να μπορεί να αξιολογηθεί με υπάρχων κώδικα, το σετ εντολών του Texas Instruments MSP. Μπορεί να διαχειρισθεί 128 Kb μνήμης, ενώ διαθέτει διαχείριση διακοπών και 256 περιφερειακών μονάδων. Ενσωματώνει 16 καταχωρητές γενικής χρήσης και 16 ειδικής. Επιπλέον, το σύστημα διαθέτει ειδικό PID ελεγκτή ο οποίος αναπτύχθηκε με την ίδια μεθοδολογία, προκειμένου να αναλάβει την ομαλή έκχυση του φαρμάκου.

Το πρωτότυπο παρουσίασε επιτυχία ολοκλήρωσης (yield) 90%, λόγω της μεθοδολογίας σχεδιασμού που ακολουθήθηκε (correct by construct). Η κατανάλωση ενέργειας, σε σύγκριση με το σύστημα αναφοράς, που βασίζεται σε πλεονασμό υλικού και λογισμικού, μειώθηκε κατά 36%, ενώ η κάλυψη των σφαλμάτων ξεπέρασε το 98%.

Καταλήγοντας, σε αυτή τη διατριβή δίνονται λύσεις σχεδιασμού φορητών συσκευών λαμβάνοντας υπ όψιν εξαρχής τις ανάγκες της εφαρμογής. Η ανάπτυξη βασίζεται στο συσχεδιασμό υλικού-λογισμικού προκειμένου να αντιμετωπιστούν προβλήματα που προκύπτουν από άλλες προσεγγίσεις. Με αυτό τον τρόπο επιτυγχάνεται υψηλό επίπεδο ασφαλούς λειτουργίας σε αντίθεση με τις τεχνικές που έχουν προταθεί μέχρι τώρα, οι οποίες απευθύνονταν σε γενικού σκοπού εφαρμογές. Τα οφέλη σε κόστος και σε κατανάλωση ενέργειας είναι σημαντικά ενώ η ασφαλής λειτουργία διασφαλίζεται σε κάθε επίπεδο σχεδιασμού.

Α.2 ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ (Master)

-

Α.3 ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

"*Σχεδιασμός Ολοκληρωμένου Συστήματος για την Μέτρηση των Οξέων του Πεπτικού Συστήματος*", Πανεπιστήμιο Πατρών, Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών, 1998

Σύντομη Περίληψη

Η διπλωματική εργασία είχε ως κύριο αντικείμενο την μελέτη μιας πρώιμης μορφής μιας ενδοσκοπικής κάψουλας. Ως εκ τούτου έπρεπε να μελετηθεί ο βαθμός σμίκρυνσης ενός αυτόνομου συστήματος το οποίο θα μπορεί να ολοκληρωθεί σε τεχνολογία ASIC και στη συνέχεια να προστατευθεί από περίβλημα σε σχήμα χαπιού, προκειμένου να χορηγηθεί σε ασθενή. Μελετήθηκαν πλήρως όλοι οι αισθητήρες που θα μπορούσαν να ενσωματωθούν (απαιτήσεις, προδιαγραφές κ.ο.κ.). Στη συνέχεια σχεδιάστηκε ανοικτή αρχιτεκτονική, προκειμένου να υποστηρίζει σύνδεση με πλήθος αισθητήρων (ακόμα και μελλοντικής κάμερας μικροσκοπικών διαστάσεων), ένας υποτυπώδης μικροελεγκτής 8-bit με περιορισμένο σύνολο εντολών (μόλις 8) και μια μνήμη RAM χαμηλής κατανάλωσης προκειμένου να καταγράφεται σε raw μορφή οι μετρήσεις από τους αισθητήρες. Πραγματοποιήθηκε λογικός έλεγχος, λειτουργική προσομοίωση, ανάλυση χρόνου και spice

DC analysis. Ο σχεδιασμός έγινε σε όλα τα επίπεδα, από αρχιτεκτονική μέχρι transistor, αξιοποιώντας όλο το ASIC design flow της Mentor Graphics. Στο πλαίσιο της διπλωματικής, περιλαμβάνεται και η δημιουργία του GDSII αρχείου (πριν την αποστολή στο εργοστάσιο)

Β. Συγγράμματα-Σημειώσεις

Β.1 Ν. Ασημάκης, Γ. Βουρβουλάκης, Αθ. Κακαρούντας, Ν. Λελίγκου: «Λογική Σχεδίαση», e-book, ISBN: 978-960-87539-2-1, 2011

Περίληψη:

Η πρώτη απόπειρα ανάπτυξης ενός διαδραστικού ηλεκτρονικού βιβλίου (e-book) στην ελληνική γλώσσα, το οποίο διατίθεται δωρεάν, και στόχο έχει να αξιοποιηθεί ως εκπαιδευτικό βοήθημα για το μάθημα της «Ψηφιακής Λογικής». Οι συγγραφείς προέρχονται από τρία διαφορετικά ΑΕΙ της Ελλάδας και το ψηφιακό υλικό που παρέχεται, εκτείνεται από τη σχεδίαση ψηφιακών συνδυαστικών κυκλωμάτων έως σύνθετων ακολουθιακών μηχανών

Β.2 V.A. Pedroni, "Σχεδίαση Κυκλωμάτων με χρήση της VHDL". Έκδοση από τις εκδόσεις Κλειδάριθμος. ISBN: 978-960-461-118-8 (Επιμέλεια – Μετάφραση στην Ελληνική γλώσσα Γ. Θεοδωρίδης, Σ. Νικολαΐδης, Δ. Σούντρης, **Αθ. Κακαρούντας**)

Περίληψη:

Μεταφορά στην Ελληνική Γλώσσα του συγγράμματος «Circuit Design with VHDL», προκειμένου να χρησιμοποιηθεί ως σύγγραμμα από τους διδάσκοντες των Ελληνικών Ιδρυμάτων Τριτοβάθμιας Εκπαίδευσης σε μαθήματα όπου αντικείμενο είναι ο σχεδιασμός με τη χρήση Hardware Description Languages, όπως η VHDL. Στόχος είναι να συμπληρωθεί ένα κενό που είχε εντοπιστεί από την ομάδα, που επιμελήθηκε την μεταφορά στην Ελληνική Γλώσσα, στον Ελληνικό Ακαδημαϊκό χώρο. Το βιβλίο έχει ήδη υιοθετηθεί σε πλήθος ΑΕΙ της χώρας ως βασικό εκπαιδευτικό σύγγραμμα, σε προπτυχιακά προγράμματα σπουδών.

Β.3 Οδηγός χρήσης και υποδειγματικές ασκήσεις της πλατφόρμας ανάπτυξης Mentor Graphics για το μάθημα «Σχεδιασμός Ολοκληρωμένων Συστημάτων με Τεχνικές VLSI», Κων/νος Γκούτης, **Αθ. Κακαρούντας**, Ε. Φωτοπούλου, για το Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών, Πανεπιστήμιο Πατρών, (ΕΠΕΑΚ ΙΙ – ΠΕ3, 2004)

Περίληψη:

Ανάπτυξη σημειώσεων για το μάθημα «Σχεδιασμός Ολοκληρωμένων Συστημάτων με Τεχνικές VLSI», του Τμήματος Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών. Βασικό αντικείμενο του μαθήματος είναι η παρουσίαση ο σχεδιασμός με τη χρήση Hardware Description Languages, όπως η VHDL. Δίνονται πλήθος παραδειγμάτων και κανόνες σχεδίασης (σύμφωνοι με το design flow της Mentor Graphics), προκειμένου τα κυκλώματα να είναι συνθέσιμα και σωστά από το σχεδιασμό. Οι σημειώσεις χρηματοδοτήθηκαν από το ΕΠΕΑΕΚ ΙΙ)

Β.4 Οδηγός χρήσης και υποδειγματικές ασκήσεις της πλατφόρμας ανάπτυξης Mentor Graphics για το μάθημα «Σχεδιασμός Ολοκληρωμένων Κυκλωμάτων Ι», Κων/νος Γκούτης, **Αθ. Κακαρούντας**, για το Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών, Πανεπιστήμιο Πατρών, (ΕΠΕΑΚ ΙΙ – ΠΕ3, 2004)

Περίληψη:

Ανάπτυξη σημειώσεων για το μάθημα «Σχεδιασμός Ολοκληρωμένων Συστημάτων Ι», του Τμήματος Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών. Βασικό αντικείμενο του μαθήματος είναι ο σχεδιασμός συνδυαστικών κυκλωμάτων με την χρήση CAD εργαλείων. Παρατίθεται πλήθος παραδειγμάτων και κανόνες σχεδίασης (σύμφωνοι με το design flow της Mentor Graphics), προκειμένου ο σχεδιασμός να μπορεί να προσομοιωθεί. Τα περιεχόμενα των σημειώσεων περιλαμβάνουν απλά και σύνθετα συνδυαστικά κυκλώματα, καθώς και θέματα που αφορούν στον σχεδιασμό όπως η μετασταθερότητα, ρεύματα διαρροής κ.ο.κ. Οι σημειώσεις χρηματοδοτήθηκαν από το ΕΠΕΑΕΚ ΙΙ)

Β.5 Οδηγός χρήσης και υποδειγματικές ασκήσεις της πλατφόρμας ανάπτυξης Mentor Graphics για το μάθημα «Σχεδιασμός Ολοκληρωμένων Κυκλωμάτων ΙΙ», Κων/νος Γκούτης, **Αθ. Κακαρούντας**, για το Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών, Πανεπιστήμιο Πατρών, (ΕΠΕΑΚ ΙΙ – ΠΕ3, 2004)

Περίληψη:

Ανάπτυξη σημειώσεων για το μάθημα «Σχεδιασμός Ολοκληρωμένων Συστημάτων ΙΙ», του Τμήματος Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών. Βασικό αντικείμενο του μαθήματος είναι ο σχεδιασμός ακολουθιακών κυκλωμάτων με την χρήση CAD εργαλείων. Παρατίθεται πλήθος παραδειγμάτων και κανόνες σχεδίασης FSM (σύμφωνοι με το design flow της Mentor Graphics), προκειμένου ο σχεδιασμός να μπορεί να προσομοιωθεί. Στις σημειώσεις περιλαμβάνονται και οδηγίες για την ανάπτυξη συστημάτων που περιλαμβάνουν συνδυαστικά και ακολουθιακά κυκλώματα. Οι σημειώσεις χρηματοδοτήθηκαν από το ΕΠΕΑΕΚ ΙΙ)

Β.6 Επίσημη μετάφραση (ως συμμετέχων στην ομάδα ανάπτυξης) - οδηγός χρήσης του Logisim (**Αθ. Κακαρούντας**) για το μάθημα «Ψηφιακή Λογική» του ΤΕΙ Ιονίων Νήσων (2009)

Περίληψη:

Ανάπτυξη οδηγού χρήσης για το ελεύθερα διαθέσιμο εργαλείο Logisim προκειμένου να μπορεί να χρησιμοποιηθεί ως εργαστηριακό σύγγραμμα στο μάθημα «Ψηφιακή Λογική». Οι σημειώσεις είναι ελεύθερα διαθέσιμες και επιδεικνύουν τις λειτουργίες που παρέχει το Logisim. Η μετάφραση έχει εγκριθεί από την ομάδα ανάπτυξης, και ακολουθεί την επίσης Ελληνική μετάφραση του εργαλείου (επίσης από τον Δρ. Κακαρούντα, ως μέλος της ομάδας του Logisim)

Γ. Κεφάλαια σε Βιβλία

Γ.1 ***A.P. Kakarountas****, K.S. Papadomanolakis, C.E. Goutis, "Low-Power Design for Safety-Critical Applications" in "Designing CMOS Circuits for Low Power," editors D. Soudris, C. Piguet, and C.E. Goutis, September 2002, Dordrecht/London/Boston, Kluwer Academic Publishers, pp. 205–234, September 2002.*

Περίληψη:

Ο σχεδιασμός για χαμηλή κατανάλωση ενέργειας έχει γίνει πολύ σημαντικός για τις σύγχρονες εφαρμογές, τόσο για θέματα ευρείας αυτονομίας καθώς και για οικολογικούς λόγους. Λόγω της διαρκούς συρρίκνωσης των μεγεθών ολοκλήρωσης, τα ηλεκτρονικά κυκλώματα είναι ιδιαίτερα επιδεκτικά σε λάθη λειτουργίας που οφείλονται στην επίδραση εξωτερικών παραγόντων, όπως ο βιομηχανικός θόρυβος, η ακτινοβολία και η θερμοκρασία.

Γι' αυτό η ασφάλεια της λειτουργίας των ηλεκτρονικών κυκλωμάτων πρέπει να λαμβάνεται ιδιαιτέρως υπ' όψιν πλέον κατά τη φάση του σχεδιασμού. Στο κεφάλαιο αυτό, παρουσιάζονται κανόνες σχεδιασμού κυκλωμάτων με αυξημένες απαιτήσεις για χαμηλή κατανάλωση ενέργειας και υψηλά επίπεδα ασφαλούς λειτουργίας. Το βιβλίο στο οποίο συμπεριλαμβάνεται το συγκεκριμένο κεφάλαιο έχει τίτλο "Designing CMOS Circuits for Low Power", Kluwer Academic Publishers.

Γ.2 ***Α. Κακαρούντας****, Ρ.Ε. Κινγκ, «Κεφάλαιο 11: Προσομοίωση και Εικονική Πραγματικότητα», στο βιβλίο «Βιομηχανική Πληροφορική», εκδόσεις Τζιόλα, 2004.*

Περίληψη:

Ο σχεδιασμός συστημάτων έχει γίνει ιδιαίτερα πολύπλοκος με αποτέλεσμα ο χρόνος για την ανάπτυξη ενός συστήματος και της διάθεσής του στην αγορά να μεγαλώνει διαρκώς. Αυτό έχει σαν αποτέλεσμα η ανάπτυξη συστημάτων να μην ενδείκνυται (από πλευρά κόστους) αν δεν έχει γίνει ενδελεχής προσομοίωση της λειτουργίας τους και εξομοίωση διάφορων καταστάσεων που προκαλούν λανθασμένη λειτουργία. Το κεφάλαιο αυτό αποτελεί επέκταση εξαμηνιαίας εργασίας στο μάθημα «Βιομηχανική Πληροφορική», που εκπονήθηκε κατά τις σπουδές του Αθ. Κακαρούντα.

Γ.3 ***A.P. Kakarountas****, H.E. Michail, "Performance for Cryptography: hardware and software approach", in "Supercomputing Research Advances", Ed. Yongge Huang, Nova Science Publishers, Inc., ISBN: 978-1-60456-186-9, 2008, pp. 403-418.*

Περίληψη:

Ο σχεδιασμός για εφαρμογές κρυπτογραφίας δεν λάμβανε μέχρι τώρα υπόψη την απόδοση-ταχύτητα επεξεργασίας μιας και δεν υπήρχαν αντίστοιχα απαιτητικές εφαρμογές ή πρωτόκολλα. Η αύξηση των τηλεπικοινωνιακών υποδομών παγκοσμίως, ο μεγάλος πλέον αριθμός των χρηστών πλειάδας υπηρεσιών και η διαρκής ζήτηση για ασφάλεια στην επικοινωνία, επιβάλλει τη δημιουργία κρυπτογραφικών ενσωματωμένων συστημάτων τα οποία θα μπορούν να ικανοποιήσουν τα νέα δεδομένα. Στο κεφάλαιο αυτό, παρουσιάζονται κανόνες σχεδιασμού κρυπτογραφικών συστημάτων – αλγορίθμων με αυξημένες απαιτήσεις για υψηλή απόδοση, σχεδόν πραγματικού χρόνου.

Γ.4 ***A.P. Kakarountas****, H.E. Michail, "Performance for Cryptography: a hardware approach", in "Cryptography Research Perspectives", Ed. Roland E. Chen, Nova Science Publishers, Inc., ISBN: 978-1-60456-492-1, 2009, pp. –*

Περίληψη:

Η αξιοποίηση όσων παρουσιάστηκαν σε προηγούμενο συλλογικό τόμο, επεκτείνεται σε μικτά συστήματα υλικού-λογισμικού, παρουσιάζοντας τη χαρτογράφηση σε υπολογιστικούς πυρήνες με διαφορετικά χαρακτηριστικά. Η επιδόσεις, είναι δυνατόν να βελτιωθούν ακόμα και 10 φορές, μειώνοντας σημαντικά ταυτόχρονα το κόστος (λόγω μείωσης της επιφάνειας) αλλά και της συνολικής κατανάλωσης. Αν και είναι εξαιρετικά δύσκολο να συμβούν όλα αυτά ταυτόχρονα, στο συγκεκριμένο κεφάλαιο επιδεικνύεται πως μέσω μετασχηματισμού κρυπτογραφικών αλγορίθμων είναι δυνατόν να βρουν τα προαναφερθέντα εφαρμογή.

Δ. Διεθνή περιοδικά με κριτές

Δ.1 ***S. Nikolaidis, E. Karaolis, A. Kakarountas, K. Papadomanolakis and C.E.***

***Goutis**, "A Methodology for Calculating the Undetactable Double-Faults in Self-Checking Circuits", Journal of Circuits, Systems and Computers, World Scientific, Vol. 12, No. 1, pp. 75-91, February 2003.*

Περίληψη:

Σε αυτή την εργασία, παρουσιάζεται μία μεθοδολογία για τον υπολογισμό των μη ανιχνεύσιμων διπλών-σφαλμάτων σε αυτο-εξεταζόμενα κυκλώματα. Αυτή η μεθοδολογία βασίζεται σε μία συμμετρική διερεύνηση των συνδυασμών των κόμβων όπου μπορούν να εμφανιστούν μη ανιχνεύσιμα διπλά-σφάλματα. σαν όχημα δοκιμής για την παρουσίαση της μεθοδολογίας χρησιμοποιείται ο αυτο-εξεταζόμενος 2-σε-1 πολυπλέκτης των n-bit κωδικοποιημένος με ισοτιμία και ο αριθμός των μη ανιχνεύσιμων διπλών-σφαλμάτων δίνεται με παραμετρικό τρόπο. Η προτεινόμενη μεθοδολογία μπορεί εύκολα να εφαρμοστεί σε άλλα bit-sliced κυκλώματα. Υλοποιούνται σύνηθη αυτο-εξεταζόμενα κυκλώματα με διαφορετικούς τρόπους κωδικοποίησης και χρησιμοποιούν την πρότυπη τεχνολογία κυττάρου για την επαλήθευση της προτεινόμενης μεθοδολογίας. Διερευνάται η αποδοτικότητα αυτών των υλοποιήσεων στην ανίχνευση σφαλμάτων καθώς και οι απαιτήσεις τους σε υλικό και ισχύ.

Δ.2 ***A. Milidonis, G. Dimitroulakos, M. D. Galanis, A. P. Kakarountas, G. Theodoridis, C.Goutis, and F.Catthoor**, "A Framework for Data Partitioning for C++ Data-Intensive Applications", Journal of Design Automation for Embedded Systems, Springer Science+Business Media B.V., Vol. 9, No. 2, pp. 101-121, June. 2005.*

Περίληψη:

Παρουσιάζεται ένα αυτοματοποιημένο πλαίσιο εργασίας, το οποίο διαμοιράζει τον κώδικα και τους τύπους δεδομένων για τις ανάγκες της διαχείρισης των δεδομένων σε έναν αντικειμενοστραφή πηγαίο κώδικα. Ο στόχος είναι η αναγνώριση των κρίσιμων τύπων δεδομένων από άποψης διαχείρισης δεδομένων και τον διαχωρισμό τους από τον υπόλοιπο κώδικα. Με αυτό τον τρόπο, η πολυπλοκότητα σχεδιασμού μειώνεται επιτρέποντας στον σχεδιαστή να επικεντρωθεί εύκολα στα σημαντικά κομμάτια του κώδικα για να εκτελέσει περαιτέρω βελτιώσεις και βελτιστοποιήσεις. Για να επιτευχθεί αυτό, εκτελείται στατική και δυναμική ανάλυση στον αρχικό κώδικα προδιαγραφής C++. Με βάση την ανάλυση των αποτελεσμάτων, οι τύποι δεδομένων της εφαρμογής χαρακτηρίζονται ως κρίσιμοι ή μη κρίσιμοι. Συνεχίζοντας, ο αρχικός κώδικας ξαναγράφεται αυτόματα με τέτοιο τρόπο ώστε οι κρίσιμοι τύποι δεδομένων και τα κομμάτια του κώδικα που τα χειρίζονται να διαχωρίζονται από τον υπόλοιπο κώδικα. Πειράματα σε πολύ γνωστές εφαρμογές πολυμέσων και τηλεπικοινωνιών δείχνουν την ορθότητα της εκτελούμενης αυτόματης ανάλυσης και επανασύνταξης του κώδικα καθώς και την καταλληλότητα του παρουσιαζόμενου πλαισίου εργασίας σε ότι έχει να κάνει με τον χρόνο εκτέλεσης και τις απαιτήσεις σε μνήμη. Συγκρίσεις με το πακέτο Quantify™ της Rational δείχνουν αποτυχία του Quantify™ να αναλύσει σωστά τον αρχικό κώδικα για τις ανάγκες της διαχείρισης δεδομένων.

Δ.3 ***M.D. Galanis, A. Milidonis, A.P. Kakarountas, and C.E. Goutis**, "A Design Flow for Speeding-up DSP Applications in Heterogeneous Reconfigurable Systems", Microelectronics Journal, Elsevier, vol 37, pp. 554-564, 2006.*

Περίληψη:

Σε αυτή την εργασία προτείνεται μία μεθοδολογία για την επιτάχυνση DSP εφαρμογών. Η μεθοδολογία αυτή εκμεταλλεύεται τις ιδιότητες των αρχιτεκτονικών ετερογενών επαναδιατασώμενων συστημάτων. Η μεθοδολογία βασίζεται στην σωστή ανάθεση των διεργασιών (tasks) στους κατάλληλους πόρους. Τα αναμενόμενα αποτελέσματα της μεθοδολογίας επιβεβαιώθηκαν μετά από την υλοποίηση ενός OFDM μεταδότη, ενός αλγορίθμου επεξεργασίας

ιατρικών εικόνων, ενός συμπιεστή εικόνας βασισμένου σε wavelet, ενός συμπιεστή video και ενός κωδικοποιητή JPEG. Τα πειραματικά αποτελέσματα επέδειξαν επιτάχυνση έως και 4.17 φορές, σε σύγκριση με τυπικές και άλλες προτεινόμενες υλοποιήσεις για αυτές τις εφαρμογές.

Δ.4 ***A.P. Kakarountas, H. Michail, A. Milidonis, G. Theodoridis, C.E Goutis****, "High-Speed FPGA Implementation of Secure Hash Algorithm for IPSec and VPN Applications", Journal of Supercomputing, Springer Science + Business Media, vol. 37, pp. 179–195, 2006.*

Περίληψη:

Σε αυτή την εργασία παρουσιάζεται μία υλοποίηση του Secure Hash Function type 1 για χρήση σε απαιτητικές εφαρμογές επικοινωνιών όπου υπάρχει μεγάλος φόρτος από τους χρήστες. Πρόκειται για την πρώτη φορά που παρουσιάζεται μία υλοποίηση που ξεπερνά τα 2.5Gbps χωρίς ιδιαίτερη αύξηση του κόστους (μικρότερη από 2%), συγκρινόμενη με τις συμβατικές λύσεις από τον ακαδημαϊκό και τον εμπορικό χώρο. Η αύξηση της τάξης του 30% της απόδοσης του SHA-1 επιτυγχάνεται με επαναπροσδιορισμό της χρονικής εκτέλεσης των διαδικασιών με το ίδιο υλικό.

Δ.5 ***H.E. Michail, A.P. Kakarountas, A.Milidonis, C.E. Goutis****, "Efficient FPGA Implementation of Novel Cryptographic Hashing Core", Computing Letters, VSP/Brill Publishing, vol. 2, num. 1-2, pp. 21-27(7), 2006.*

Περίληψη:

Σε αυτή την εργασία παρουσιάζεται μία υλοποίηση του Secure Hash Function type 2 για χρήση σε απαιτητικές εφαρμογές. Η προτεινόμενη υλοποίηση ξεπερνά τις υπάρχουσες στην αγορά και αυτές που έχουν προταθεί στον ακαδημαϊκό τύπο κατά 40% περίπου στην ταχύτητα επεξεργασίας των μηνυμάτων. Παρά την επίτευξη υψηλής ταχύτητας λειτουργίας, το επιπλέον υλικό το οποίο απαιτείται δεν ξεπερνά το 20%.

Δ.6 ***I. Yiakoumis, M. Papadonikolakis, H.E. Michail, A.P. Kakarountas, C.E. Goutis*** *"Maximizing the hash function of authentication codes", IEEE Potentials, vol. 25, iss. 2, pp. 9–12, 2006.*

Περίληψη:

Παρουσιάζονται ταχύτατες υλοποιήσεις βασικών κρυπτογραφικών κυκλωμάτων για την ακεραιότητα και την αυθεντικότητα μηνυμάτων που ανταλλάσσονται σε ένα δίκτυο. Παρά την επίτευξη υψηλής ταχύτητας λειτουργίας, το επιπλέον υλικό το οποίο απαιτείται δεν ξεπερνά το 5%. Παράπλευρο χαρακτηριστικό είναι η χαμηλή κατανάλωση ενέργειας όταν το κύκλωμα χρονίζεται στη συχνότητα λειτουργίας ανταγωνιστικών υλοποιήσεων.

Δ.7 ***H.E. Michail, A.P. Kakarountas, C.E. Goutis*** *"Server Side Hashing Core Exceeding 3 Gbps of Throughput", International Journal of Network Security (special issue), Vol. 1, Nos. 1/2/3, pp. 43–53, 2007.*

Περίληψη:

Παρουσιάζονται ταχύτατες υλοποιήσεις βασικών κρυπτογραφικών κυκλωμάτων τα οποία επιτυγχάνουν απόδοση υψηλότερη των 3 Gbps. Είναι η πρώτη φορά στη διεθνή επιστημονική βιβλιογραφία που αναφέρεται τέτοια απόδοση για τα συγκεκριμένα κυκλώματα. Η αύξηση της απόδοσης βασίζεται στον ανασχεδιασμό του αλγορίθμου και την ορθή χρονοδρομολόγηση των διεργασιών. Αυτό έχει σαν αποτέλεσμα την αύξηση της απόδοσης με σχεδόν το ίδιο απαιτούμενο υλικό. Με voltage scaling είναι δυνατή η μείωση της απόδοσης στα σημερινά επίπεδα με

παράπλευρη μείωση της κατανάλωσης.

Δ.8 ***A.P. Kakarountas, N.D. Zervas, H.E. Michail, G. Theodoridis, and D. Soudris****, "Power Management through Dynamic Frequency Scaling for Low and Medium bit-rate Digital Receivers", Journal of Low Power Electronics, ASP, vol.2, no 3, pp. 356–364, 2006.*

Περίληψη:

Σε αυτή την εργασία παρουσιάζεται η τεχνική δυναμικής κλιμάκωσης της συχνότητας λειτουργίας ψηφιακών δεκτών χαμηλού και μέσου ρυθμού. Με την τεχνική αυτή αμέσως μετά το χρονισμό του καναλιού με τη ροή των δεδομένων από τον πομπό, απενεργοποιείται το κύκλωμα συγχρονισμού προκειμένου να επιτευχθεί μείωση της συνολικά απαιτούμενης ενέργειας. Έτσι με αύξηση του συνολικού κόστους (επιφάνεια ολοκλήρωσης) περίπου στο 13%, το οποίο αντιστοιχεί στα κυκλώματα που υλοποιούν την μονάδα διαχείρισης της προαναφερθείσας διαδικασίας, η συνολική κατανάλωση ισχύος μειώνεται στο 40%.

Δ.9 ***G. N. Selimis, A.P. Kakarountas, A. P. Fournaris, A. Milidonis and O.Koufopavlou****, "A Low Power Design for SBOX Cryptographic Primitive of Advanced Encryption Standard for Mobile End-Users", in Journal of Low Power Electronics, ASP, vol.3, no.3, pp. 327-336, 2007.*

Περίληψη:

Τεχνική σχεδίασης του AES αλγορίθμου για ενσωμάτωσή του σε φορητά συστήματα. Η κατανάλωση ενέργειας μπορεί να μειωθεί μέχρι 40%. Είναι η πρώτη φορά που παρουσιάζεται μια εργασία για ενσωματωμένα συστήματα φορητών συσκευών στην οποία ο κρυπτογραφικός αλγόριθμος προσαρμόζεται στα χαρακτηριστικά της συσκευής και ταυτόχρονα μειώνεται δραματικά η κατανάλωση ενέργειας.

Δ.10 ***H.E. Michail, A. P. Kakarountas, A. S. Milidonis and C. E. Goutis****, "A Top-Down Design Methodology for Implementing Ultra High-Speed Hashing Cores", IEEE Transactions on Dependable and Secure Computing, vol.6, is.4, pp.255-268, 2009.*

Περίληψη:

Οι μονόδρομες συναρτήσεις hashing αποτελούν βασικά κρυπτογραφικά τμήματα σε όλους σχεδόν τους αλγορίθμους τηλεπικοινωνιών. Με την αύξηση της υπολογιστικής ισχύος των σύγχρονων υπολογιστών, απαιτείται η δημιουργία συστημάτων ειδικού σκοπού, με αυξημένη απόδοση, προκειμένου να πραγματοποιούνται οι διεργασίες κρυπτογραφίας σε χρόνο μικρότερο αυτού στον οποίο ένας hacker θα μπορούσε να «σπάσει» τους κώδικες. Στην εργασία αυτή παρουσιάζεται μια συστηματική μεθοδολογία για τη δημιουργία ηλεκτρονικών συστημάτων ειδικού σκοπού που επιταχύνουν την κρυπτογράφηση, όταν πραγματοποιείται κρυπτογράφηση hashing.Τα αποτελέσματα είναι σημαντικά, αφού η προτεινόμενη μεθοδολογία (πρώτη στο είδος της) οδηγεί σε αύξηση απόδοσης ακόμη και 500%.

Δ.11 ***M. Papadonikolakis, A.P. Kakarountas, C.E. Goutis****, "Efficient High-Performance Implementation of JPEG-LS Encoder", in Journal of Real-Time Processing, Springer. vol. 3, no. 4, pp 303-310, 2008.*

Περίληψη:

Στην εργασία παρουσιάζεται μια νέα αρχιτεκτονική υλοποίησης ενός κωδικοποιητή JPEG-LS.

Βασίζεται στην επαναχρησιμοποίηση ήδη επεξεργασμένων δεδομένων, προκειμένου να μειωθεί το υπολογιστικό φορτίο και να επιταχυνθεί ο απαιτούμενος χρόνος κωδικοποίησης. Η συγκεκριμένη εργασία αποτελεί τη βάση για real-time κωδικοποίηση κατά JPEG-LS σε ενδοσκοπικές κάψουλες.

Δ.12 ***A. Milidonis, V. Porpodas, N. Alachiotis, A. P. Kakarountas, H. Michail, G. Panagiotakopoulos and C. E. Goutis****, "Low Power Architecture with Scratch-Pad Memory for Accelerating Embedded Applications with Run Time Reuse", IET Computers & Digital Techniques, IET, vol. 3, is. 1, pp.109-123, 2009.*

Περίληψη:

Στην εργασία παρουσιάζεται μια καινοτομική αρχιτεκτονική η οποία βασίζεται στη χρήση scratch-pad μνημών για την αποθήκευση δεδομένων που επαναχρησιμοποιούνται. Η διαφορά της με την τυπική cache μνήμη είναι η ενσωμάτωση επιπλέον λογικής προκειμένου να αυτοματοποιηθούν οι μεταφορές δεδομένων από τη μνήμη προς τον επεξεργαστικό πυρήνα και πάλι πίσω. Ο στόχος είναι να γίνει χρήση της προτεινόμενης αρχιτεκτονικής σε εφαρμογές ενσωματωμένων συστημάτων, όπου η απόδοση είναι κρίσιμη αλλά συνήθως το διαθέσιμο υλικό είναι χαμηλών δυνατοτήτων. Η επιπλέον απαίτηση που εισάγεται και ικανοποιείται πλήρως από την προτεινόμενη αρχιτεκτονική είναι η μικρή κατανάλωση ενέργειας προκειμένου να υπάρχει μείωση της αυτονομίας του συστήματος. Η προτεινόμενη αρχιτεκτονική επιτυγχάνει σε ορισμένους αλγορίθμους αύξηση της απόδοσης πάνω από 300% με μικρή άνοδο της κατανάλωσης εως 10%

Δ.13 ***D.M. Schinianakis, A.P. Fournaris, A.P. Kakarountas and T. Stouraitis****, "An RNS Architecture of an Fp Elliptic Curve Point Multiplier", IEEE Transactions on Circuits and Systems I, vol.56, no.6, pp. 1202-1213, June 2009.*

Περίληψη:

Οι σύγχρονες εφαρμογές κρυπτογράφησης βασίζονται στην αναδυόμενη τάση για χρήση ελλειπτικών καμπυλών (ECC). Ένα δομικό στοιχείο για αυτή την κρυπτογράφηση είναι ο πολλαπλασιαστής σημείου ελλειπτικής καμπύλης. Πολλές υλοποιήσεις έχουν προταθεί, οι οποίες όμως παρουσιάζουν χαμηλή απόδοση, κυρίως λόγω της πολυπλοκότητάς τους. Σε αυτή την εργασία παρουσιάζεται μια δομή για την υλοποίηση ενός τέτοιου πολλαπλασιαστή ο οποίος βασίζεται στη χρήση αριθμητικού συστήματος υπολοίπου (RNS). Αυτό έχει σαν αποτέλεσμα να μειωθεί σημαντικά η πολυπλοκότητα και να αυξηθεί η απόδοση κατά μια τάξη μεγέθους.

Δ.14 ***A.P. Kakarountas, H.E. Michail, C.E. Goutis, A.M. Rjoub****, "High-Throughput Implementation of RipeMD-160", International Journal for Internet Technology and Secured Transactions, Inderscience Ltd, vol. 1, no. 3/4, pp. 309 – 316, 2009.*

Περίληψη:

Σχεδίαση κυκλώματος το οποίο πραγματοποιεί κωδικοποίηση – αποκωδικοποίηση κατά RIPEMD-160. Το χαρακτηριστικό του στοιχείο είναι ο υψηλός ρυθμός κωδικοποίησης-αποκωδικοποίησης.

Δ.15 ***A. Milidonis, N. Alachiotis, V. Porpodas, H. Michail, G. Panagiotakopoulos, A.P. Kakarountas, C.E. Goutis****, "Decoupled Processors Architecture for Accelerating Data Intensive Applications using Scratch-Pad Memory Hierarchy", Journal of Signal Processing Systems. Springer Science + Business Media, LLC, vol. 59, no.3, pp. 281-296, 2010.*

Περίληψη:

Μια αποσυζευγμένη διάταξη δύο πυρήνων, η οποία περιλαμβάνει στην αρχιτεκτονική της μνήμη scratchpad αντί της τυπικής cache. Εκμεταλλευόμενοι τα χαρακτηριστικά της αρχιτεκτονικής, τροποποιούμε κατάλληλα το λογισμικό προκειμένου να έχουμε μέγιστη αξιοποίηση των πόρων του συστήματος. Τα αποτελέσματα είναι εξαιρετικά αφού προκύπτει speedup της τάξης του 500% σε σύγκριση με την αρχιτεκτονική που χρησιμοποιεί μνήμη cache.

Δ.16 ***H.E. Michail, A.P. Kakarountas, D. Schinianakis, G. Selimis, C.E. Goutis****, "Cipher Block based Authentication Module: A Hardware Design Perspective", Journal of Circuits, Systems and Computers, World Scientific Publishing, Vol. 20, No. 2, pp. 163-184, 2011.*

Περίληψη:

Μια προτεινόμενη αρχιτεκτονική CMAC πλήρως υλοποιημένη σε υλικό. Αξιοποιώντας τα αποτελέσματα μετασχηματισμών κρυπτογραφικών αλγορίθμων, δημιουργήθηκε ένα σύστημα με 4 επίπεδα ομοχειρίας (pipeline) το οποίο δίνει τη δυνατότητα για αύξηση των επιδόσεων 5-100 φορές σε σύγκριση με τον ανταγωνισμό.

Ε. Διεθνή συνέδρια με κριτές και Πρακτικά

Ε.1 **A.P. Kakarountas, K. Papadomanolakis, E. Karaolis, S. Nikolaidis, N. Alachiotis, C.E. Goutis**, "*Hardware and Power Requirements of Self-Checking Circuits*", in Proc. of 6th IEEE International Conference on Electronics, Circuits and Systems (ICECS'99), Pafos, Cyprus, pp 1655-1658, Sept. 1999.

Περίληψη:

Σε αυτή την εργασία εξετάζονται οι απαιτήσεις σε υλικό και ισχύ των αυτό-ελεγχόμενων αρχιτεκτονικών (self-checking architectures) για τα συνήθη data path και κυκλώματα αποθήκευσης δεδομένων. Οι έξοδοι αυτών των κυκλωμάτων κωδικοποιούνται σύμφωνα με τον parity κώδικα και τον CRC. Συγκεκριμένη τεχνολογία κελιού έχει χρησιμοποιηθεί και η ανίχνευση ενός μονού stack-at σφάλματος ,μόνιμου ή παροδικού, εξασφαλίζεται σε όλα τα προτεινόμενα κυκλώματα καθώς επίσης καθορίζεται η αποδοτικότητα του κάθε coding συστήματος κατά την ανίχνευση διπλών ή τριπλών σφαλμάτων. Όπως παρατηρείται από τα αποτελέσματα οι απαιτήσεις σε υλικό και ισχύ καθώς και η αποτελεσματικότητα στην ανίχνευση λαθών εξαρτάται σε πολύ μεγάλο βαθμό από το επιλεγμένο coding σύστημα.

Ε.2 **A.P. Kakarountas, K. Papadomanolakis, E. Karaolis, S. Nikolaidis, C.E. Goutis,** "*Hardware/Power Requirements vs. Fault Detection Effectiveness in Self-Checking Circuits*", in Proc. of IEEE 1999 International Workshop on Power And Timing Modeling, Optimization and Simulation (PATMOS'99), Kos, Greece, pp. 387-396, Oct. 1999.

Περίληψη:

Σε αυτήν την εργασία παρουσιάζονται οι απαιτήσεις σε υλικό και σε καταναλούμενη ισχύ των αυτό-ελεγχόμενων (self-checking) αρχιτεκτονικών για συχνά data paths και κυκλώματα αποθήκευσης δεδομένων. Αυτά τα κυκλώματα υλοποιούνται για διαφορετικά coding συστήματα χρησιμοποιώντας συγκεκριμένες τεχνολογίες κελιών. Η ανίχνευση καθενός μονού σφάλματος, μόνιμου ή παροδικού εξασφαλίζεται σε όλα τα προτεινόμενα κυκλώματα ενώ επίσης καθορίζεται η αποτελεσματικότητα καθενός coding συστήματος όταν συμβεί διπλό λάθος. Σύμφωνα με τα αποτελέσματα οι απαιτήσεις σε υλικό και ισχύ καθώς και η αποτελεσματικότητα στην ανίχνευση λαθών εξαρτάται σε πολύ μεγάλο βαθμό από το επιλεγμένο σύστημα κωδικοποίησης.

E.3 **A.P. Kakarountas, K. Papadomanolakis, V. Kokkinos, C.E. Goutis**, "*Comparative Study on Self-Checking Carry-Propagate Adders in Terms of Area, Power and Performance*", in Proc. of IEEE 2000 International Workshop on Power And Timing Modeling, Optimization and Simulation (PATMOS'00), Göttingen, Germany, pp. 187-194, Sept. 2000.

Περίληψη:

Σε αυτή την εργασία εξετάζονται πολλοί αυτό-ελεγχόμενοι διάδοσης κρατούμενου αθροιστές (self-checking carry propagate adders). Αυτοί συγκρίνονται όσον αφορά την έκταση ολοκλήρωσης ,την κατανάλωση ισχύος και την απόδοση τους. Η σε πραγματικό χρόνο ανίχνευση οποιουδήποτε μονού λάθους, μόνιμου ή παροδικού, επιβεβαιώνεται για όλα τα παρουσιαζόμενα κυκλώματα ενώ ταυτόχρονα παρουσιάζονται και τα χαρακτηριστικά του κάθε αθροιστή. Τα αποτελέσματα δείχνουν ότι τα χαρακτηριστικά των αθροιστών μεταβάλλονται όταν εφαρμόζεται κάποιος μηχανισμός ασφαλείας. Επίσης οι περιορισμοί του απαιτούμενου συστήματος καθορίζουν και το είδος του αθροιστή που θα χρησιμοποιηθεί

E.4 **A.P. Kakarountas, V. Kokkinos, C.E. Goutis**, "*Design of Low-Power On-Line Reconfigurable Datapaths Using Self-Checking Circuits*", in Proc. of 8th IEEE International Conference on Electronics, Circuits and Systems (ICECS'01), Malta, vol.III, pp.1565-1568, Sept. 2001.

Περίληψη:

Σε αυτήν την εργασία παρουσιάζεται μια καινούρια τεχνική για την υλοποίηση ανεκτικών σε σφάλματα (fault-tolerant) κυκλώματα. Έλεγχος οδηγούμενος από τον υπολογιστή χρησιμοποιείται για να ανιχνεύσει τα λάθη και μια επανα-προγραμματιζόμενη αρχιτεκτονική χρησιμοποιείται για να απομονωθεί η μονάδα που εισάγει λάθη. Τα κύρια χαρακτηριστικά αυτής της τεχνικής είναι η μειωμένη κατανάλωση ισχύος συγκρινόμενη με τις συμβατικές υλοποιήσεις, και ο ελάχιστος χρόνος που απαιτείται ώστε να εκτελεστεί η διαδικασία επανα-προγραμματισμού. Παρουσιάζονται εφαρμογές αυτής της τεχνικής σε FIR όπου η έκταση ολοκλήρωσης είναι κατά 40% μικρότερη ενώ ταυτόχρονα επιτυγχάνεται μια μείωση 33% όσον αφορά την κατανάλωση ισχύος.

E.5 **K. Papadomanolakis, A.P. Kakarountas, V. Kokkinos, S. Nikolaidis, C.E. Goutis**, "*Low-Power Design of a Safety Critical Microcontroller*", in Proc. of 1st Conference on Microelectronics, Microsystems and Nanotechnology (MMN'00), Athens, Greece, Nov. 2000.

Περίληψη:

Σε αυτή την εργασία παρουσιάζεται ο σχεδιασμός και η αντίστοιχη μεθοδολογία ενός μικροελεγκτής χαμηλής κατανάλωσης και κρίσιμης ασφάλειας (safety-critical). Αυτός ο μικροελεγκτής θα χρησιμοποιηθεί για τον έλεγχο λειτουργίας μιας φορητής αντλίας έγχυσης για ιατρικές εφαρμογές. Ένας αριθμός από μηχανισμούς ασφαλείας έχουν υλοποιηθεί για την ανίχνευση κάθε πιθανής αποτυχίας του συστήματος η οποία μπορεί να προκύψει είτε λόγω υλικού είτε λόγω προγράμματος. Μια κατάλληλη ανάθεση αυτών των μηχανισμών είτε σε υλικό είτε σε πρόγραμμα χρησιμοποιείται έτσι ώστε να υπάρξει συμβιβασμός μεταξύ των απαιτήσεων για χαμηλή κατανάλωση και ευκαμψίας του συστήματος. Επίσης έχουν πραγματοποιηθεί εκτεταμένοι μηχανισμοί επίβλεψης που εγγυώνται την ορθή λειτουργία της εφαρμογής –πρόγραμμα που εκτελείται σε αυτόν τον μικροελεγκτή

E.6 **K. Papadomanolakis, A.P. Kakarountas, V. Kokkinos, N. Sklavos, C.E. Goutis**, "*The Effect of Fault Secureness in Low-Power Multiplier Designs*", in Proc. of IEEE 2001 International Workshop on Power And Timing Modeling, Optimization and Simulation (PATMOS'01), Yverdon-Les-Bains, Switzerland, pp. 10.3, Sept. 2001.

Περίληψη:

Σε αυτή την εργασία αναδεικνύεται ο αντιφατικός χαρακτήρας του σχεδιασμού για έλεγχο σφαλμάτων και του σχεδιασμού για χαμηλή κατανάλωση ενέργειας. Οι πολλαπλασιαστές χρησιμοποιούνται ως υπόδειγμα για σύγκριση. Αναδεικνύονται τα χαρακτηριστικά κάθε τεχνικής σχεδιασμού και τα σημεία στα οποία αντιτίθενται. Η επίδραση του σχεδιασμού για έλεγχο σφαλμάτων εάν εφαρμοστεί σε ένα πολλαπλασιαστή μπορεί να του καταστρέψει τα χαρακτηριστικά χαμηλής κατανάλωσης καθώς και το αντίθετο

E.7 **K. Papadomanolakis, A.P. Kakarountas, V. Kokkinos, N. Sklavos, C.E. Goutis**, "*A Comparative Study on Fault Secure Signed Multiplication Designs*", in Proc. of 11th IFIP International Conference on Very Large Scale Integration (IFIP VLSI-SOC'01), Montpellier, France, pp. 183-188, Dec. 2001.

Περίληψη:
Σε αυτή την εργασία γίνεται συγκριτική μελέτη σχεδιασμών αυτό-εξεταζόμενων για σφάλματα πολλαπλασιαστών (προσημασμένοι). Οι μετρήσεις γίνανε τόσο για την απόδοση όσο και για την απαιτούμενη επιφάνεια ολοκλήρωσης και την τελική κατανάλωση ισχύος. Αυτό το οποίο παρατηρήθηκε είναι ότι στο πεδίο των αυτό-εξεταζόμενων από σφάλματα πολλαπλασιαστών (και κατ' επέκταση στα αριθμητικά κυκλώματα) δεν διατηρούνται οι χαρακτηρισμοί τους όπως συναντώνται στη διεθνή βιβλιογραφία

E.8 **A.P. Kakarountas, K. Papadomanolakis, V. Spiliotopoulos, S. Nikolaidis, C.E. Goutis,** "*Designing a Low-Power Fault-Tolerant Microcontroller for Medicine Infusion Devices*", in Proc. of Design, Automation & Test in Europe (DATE'02), Paris, France, pp. 205-211, March 2002.

Περίληψη:
Σε αυτή την εργασία παρουσιάζεται για πρώτη φορά ένας μικροελεγκτής ειδικού σκοπού, του οποίου ενδείκνυται η χρήση σε φορητές ιατρικές συσκευές. Παρουσιάζονται όλα τα τμήματά του αναλυτικά ενώ ιδιαίτερη αναφορά γίνεται στη δυνατότητα του για λειτουργία σε κατάσταση υψηλής ασφαλείας. Επιπλέον έχουν εφαρμοστεί τεχνικές σχεδιασμού για χαμηλή κατανάλωση επιτρέποντας τη χρήση του και σε άλλου είδους φορητές συσκευές κρίσιμης ασφαλείας

E.9 **A.P. Kakarountas, K. Papadomanolakis, S. Nikolaidis, D. Soudris, C.E. Goutis,** "*Confronting Violations of the TSCG(t) in Low-Power Design*", in Proc. of the IEEE 2002 International Symposium on Circuits and Systems (ISCAS'02), Scottsdale, Arizona, USA, pp. 2606-2609, May 2002.

Περίληψη:
Ο σχεδιασμός κυκλωμάτων ασφαλούς λειτουργίας είναι κρίσιμος σε περιπτώσεις εφαρμογών κρίσιμης ασφαλείας. Οι απαιτήσεις τέτοιων συστημάτων, όταν τα επίπεδα ασφαλείας κυμαίνονται ψηλά, απαιτούν κυκλώματα αυτό-εξέτασης πραγματικού χρόνου. Στις περιπτώσεις όμως που απαιτείται να ικανοποιηθεί και κάποιος δεύτερος παράγοντας σχεδίασης, συνήθως το αποτέλεσμα δεν καταφέρνει να ανταποκριθεί στις απαιτήσεις για υψηλή ασφάλεια. Σε αυτή την εργασία παρουσιάζονται τα συχνότερα σφάλματα που γίνονται κατά τη σχεδίαση και προτείνονται τεχνικές αποφυγής κακού σχεδιασμού

E.10 **N.D. Zervas, S. Theoharis, A.P.Kakarountas, G. Theodoridis, D. Soudris, C.E. Goutis**, "Reducing Power Consumption *through Dynamic Frequency Scaling for a Class of Digital Receivers*", in Proc. of IEEE 2000 International Workshop on Power And Timing Modeling, Optimization and Simulation (PATMOS'00), Göttingen, Germany, pp. 47-55, Sept. 2000.

Περίληψη:
Σε αυτή την εργασία προτείνεται μία τεχνική ελέγχου της κατανάλωσης ενέργειας βασισμένη στη δυναμική κλιμάκωση της συχνότητας. Η προτεινόμενη τεχνική έχει κύρια εφαρμογή στους ψηφιακούς λήπτες που πραγματοποιούν προσαρμοστική δειγματοληψία. Τέτοιου είδους κυκλώματα πραγματοποιούν υπερ-δειγματοληψία των αναλογικών εισόδων

προκειμένου να επιτύχουν συγχρονισμό σήματος. Η προτεινόμενη τεχνική «αναγκάζει» τα κυκλώματα να λειτουργήσουν μόνο στα σωστά χρονικά διαστήματα για τα οποία έχει επιτευχθεί συγχρονισμός. Τα πειραματικά αποτελέσματα απέδειξαν πως η εφαρμογή της προτεινόμενης τεχνικής επιτυγχάνει υψηλή εξοικονόμηση ενέργειας, με μικρό κόστος σε επιφάνεια και απόδοση

E.11 **N. Liveris, N.D. Zervas, A.P. Kakarountas, C.E. Goutis**, "*A code Transformation-Based Methodology for Improving I-Cache Performance*", in Proc. of 8th IEEE International Conference on Electronics, Circuits and Systems (ICECS'01), Malta, vol.II, pp.917-920, Sept. 2001.

Περίληψη:
Αυτή η εργασία επικεντρώνεται στην συμπεριφορά των I-Cache με εφαρμογή κώδικα μετατροπής υψηλού επιπέδου. Συγκεκριμένα προτείνεται ένα διάγραμμα για τις επαναληπτικές εφαρμογές της απόδοσης I-Cache που βελτιστοποιεί τις μετατροπές. Η διαδικασία της εφαρμογής των μετατροπών καθορίζεται από μια ομάδα αναλυτικών εξισώσεων που παίρνουν παραμέτρους που σχετίζονται με τον κώδικα και την δομή της I-Cache και έτσι προβλέπει τον αριθμό αποτυχιών εύρεσης της I-Cache

E.12 **K. Masselos, F. Catthoor, A.P. Kakarountas, C.E. Goutis, H. DeMan**, "*Memory Hierarchy Layer Assignment for Data Re-Use Exploitation in Multimedia Algorithms Realized on Predefined Processor Architectures*", in Proc. of 8th IEEE International Conference on Electronics, Circuits and Systems (ICECS'01), Malta, vol.I, pp.285-288, Sept. 2001.

Περίληψη:
Μια συστηματική προσέγγιση, παρουσιάζεται σε αυτή την εργασία, για την ανάθεση τύπων δεδομένων στα διάφορα επίπεδα μιας τυποποιημένης ιεραρχίας μνήμης, όπως συναντάται στους κοινούς επεξεργαστές εντολών. Η Ανάθεση Επιπέδων Ιεραρχίας Μνήμης (ΑΕΙΜ) είναι απαραίτητη για να εγγυηθεί την επιτυχή εκμετάλλευση επαναλαμβανομένων τύπων δεδομένων, κάτι που είναι ιδιαίτερα σύνηθες στις εφαρμογές πολυμέσων. Η προτεινόμενη προσέγγιση για ΑΕΙΜ λαμβάνει υπ' όψιν τα αρχιτεκτονικά χαρακτηριστικά του στοχευόμενου συστήματος, όπως την καθορισμένη ιεραρχία της φυσικής μνήμης καθώς και τις μνήμες cache και τα χαρακτηριστικά τους. Πειραματικά αποτελέσματα έδειξαν πως η εκμετάλλευση της επαναλαμβανόμενης χρήσης δεδομένων και της προτεινόμενης προσέγγισης για ΑΕΙΜ οδηγούν σε σημαντικά οφέλη στην κατανάλωση ενέργειας και στην απόδοση του συστήματος

E.13 **K.S. Papadomanolakis, A.P. Kakarountas, N. Sklavos, C.E. Goutis**, "*A Low-Power Fault-Secure Timer Implementation*", in Proc. of the IEEE 2002 International Conference on Electronics, Circuits and Systems (ICECS'02), Croatia, pp. 537-540, Sept. 2002.

Περίληψη:
Στην εργασία αυτή παρουσιάζεται ένας χρονομετρητής (timer) ασφαλούς λειτουργίας. Οι χρονομετρητές ασφαλούς λειτουργίας βασίζονται στην εισαγωγή πλεονάζουσας πληροφορίας (μέσω κυρίως υλικού – hardware) και έχουν ιδιαίτερα χαμηλές αποδόσεις. Γι' αυτό το λόγο δεν συναντώνται σε υλοποιήσεις Watchdog timers. Η προτεινόμενη δομή παρουσιάζει υψηλή απόδοση και μπορεί πολύ εύκολα να ενσωματωθεί σε ένα ολοκληρωμένο υπολογιστικό σύστημα όπου υπάρχουν υψηλές απαιτήσεις για ασφαλή λειτουργία

E.14 **A.P. Kakarountas, G. Theodoridis, K.S. Papadomanolakis, C.E. Goutis**, "*A Novel High-Speed Counter with Counting Rate Independent of the Counter's Length*", in Proc. of the IEEE 2003 International Conference on Electronics, Circuits and Systems (ICECS'03), UAE, pp. 1164 - 1167, Dec. 2003.

Περίληψη:
Οι μετρητές ανήκουν στης πλέον βασικές δομικές μονάδες των ψηφιακών συστημάτων. Προτείνουμε έναν νέο υψηλής ταχύτητας μετρητή με σταθερό ρυθμό καταμέτρησης

ανεξάρτητα από το μήκος του. Εκμεταλλευόμενοι ιδιότητες των δυαδικών συστημάτων αρίθμησης και υιοθετώντας prescaling τεχνικές παρουσιάζουμε την αρχιτεκτονική ενός κατατμημένου μετρητή. Για να πραγματοποιήσου με κατάλληλα έναν μετρητή οποιουδήποτε μεγέθους 2 σχεδιασμένες δομικές μονάδες 4-bit μετρητών χρησιμοποιούνται με συστολικό τρόπο. Ο ρυθμός καταμέτρησης καθορίζεται από την καθυστέρηση δύο βασικών πυλών 3 εισόδων η κάθε μία συν την καθυστέρηση ενός T flip-flop. Σε τεχνολογία AMS 0.6 μm επιτυγχάνεται μέγιστη συχνότητα λειτουργίας περί τα 430 Mhz

E.15 **K.S. Papadomanolakis, A.P. Kakarountas, N. Sklavos, C.E. Goutis**, "*A Fast Johnson-Mobius Encoding Scheme for Fault Secure Binary Counters*", in Design, Automation & Test in Europe (DATE'02), Paris, France, Mar. 2002.

Περίληψη:

Σε αυτή την εργασία παρουσιάζεται ένας απαριθμητής (counter) ασφαλούς λειτουργίας. Οι απαριθμητές ασφαλούς λειτουργίας βασίζονται στην εισαγωγή πλεονάζουσας πληροφορίας (μέσω κυρίως υλικού – hardware) και έχουν ιδιαίτερα χαμηλές αποδόσεις. Ο προτεινόμενος απαριθμητής βασίζεται σε έναν απαριθμητή ο οποίος κάνει χρήση κωδικοποίησης Johnson – Mobius η οποία είναι τύπου Gray. Τα αποτελέσματα είναι ιδιαίτερα ενδιαφέροντα, αφού με μικρή επιβάρυνση στην απόδοση, τελικά αποδίδει δυαδική απαρίθμηση ενώ τα χαρακτηριστικά των κωδικών Gray χρησιμοποιούνται προκειμένου να εξασφαλιστεί ο διαρκής έλεγχος της ασφαλής λειτουργίας του απαριθμητή

E.16 **D. Karatasos, A.P. Kakarountas, G. Theodoridis, C.E. Goutis**, "*A Novel Constant-Time Fault-Secure Binary Counter*", in Proc. of IEEE 2004 Internationsl Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS'04), Santorini island, Greece, Sept. 2004.

Περίληψη:

Σε αυτή την εργασία παρουσιάζεται ένας απαριθμητής (counter) ασφαλούς λειτουργίας. Οι απαριθμητές ασφαλούς λειτουργίας βασίζονται στην εισαγωγή πλεονάζουσας πληροφορίας (μέσω κυρίως υλικού – hardware) και έχουν ιδιαίτερα χαμηλές αποδόσεις. Ο προτεινόμενος απαριθμητής βασίζεται σε έναν ταχύτατο απαριθμητή ο οποίος έχει ιδιότητες οι οποίες ικανοποιούν στο έπακρο τις απαιτήσεις για ασφαλή λειτουργία. Με την προτεινόμενη τροποποίηση ο απαριθμητής επιτυγχάνει υψηλά επίπεδα ασφαλούς λειτουργίας, υψηλή απόδοση με ελάχιστο κόστος στο υλικό

E.17 **A.P. Kakarountas, V. Spiliotopoulos, S. Nikolaidis, C.E. Goutis**, "*The Impact of Low-Power Techniques on the Design of Portable Safety-Critical Systems*", in Proc. of the IEEE 2004 International Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS'04), Santorini island, Greece, September 2004.

Περίληψη:

Η εφαρμογή τυπικών τεχνικών χαμηλής κατανάλωσης ισχύος σε κρίσιμης ασφάλειας συστήματα μπορεί να οδηγήσει σε αλλοίωση των ιδιοτήτων κρίσιμης ασφάλειας του συστήματος. Όμως υπάρχουσες τεχνικές που αντιμετωπίζουν αυτή την επίδραση, θεωρώντας ότι η μέθοδος χαμηλής κατανάλωσης ισχύος εφαρμόζεται σε μικρά διαστήματα χρόνου. Έτσι, στρέφοντας την αλλοίωση των ιδιοτήτων ασφαλείας μόνο σε ελεγκτές θεωρείτο επαρκές. Παρουσιάζεται μία νέα προσέγγιση που θεωρεί τόσο τις απαιτήσεις για ασφαλή λειτουργία όσο και αυτές για χαμηλή κατανάλωση ενέργειας. Παρουσιάζονται τα πλεονεκτήματα αυτής της προσέγγισης και προσφέρεται μία σύγκριση με εναλλακτικές προσεγγίσεις

E.18 **H.E. Michail, A.P. Kakarountas, C.E. Goutis**, "*Efficient Implementation of the Keyed-Hash Message Authentication Code (HMAC) Using the SHA-1 Hash Function*", in Proc. of the IEEE 2004 International Conference on Electronics, Circuits and Systems (ICECS'04), Tel-Aviv, Israel, pp. 567-570, Dec. 2004.

Περίληψη:

Σε αυτή την εργασία παρουσιάζεται μια αποδοτική υλοποίηση, ως προς την απόδοση, του Keyed-Hash Message Authentication Code (HMAC) με χρήση της SHA-1 συνάρτησης κατακερματισμού και ανάμιξης (hash functions). Αυτός ο μηχανισμός χρησιμοποιείται για πιστοποίηση μηνυμάτων σε συνδυασμό με ένα κρυφό διαμοιραζόμενο κλειδί. Η προτεινόμενη υλοποίηση σε υλικό είναι εύκολα συνθέσιμη σε μια μεγάλη ποικιλία FPGA και ASIC τεχνολογίες. Τα αποτελέσματα των εξομοιώσεων που έγιναν με εμπορικά εργαλεία επιβεβαίωσαν την αποδοτικότητα της HMAC υλοποίησης όσον αφορά την απόδοση και τον ρυθμό μετατροπής δεδομένων (throughput) .Ειδική μέριμνα έχει ληφθεί έτσι ώστε η προτεινόμενη υλοποίηση να μην παρουσιάζει επιπλέον σχεδιαστικές πολυπλοκότητες ενώ ταυτόχρονα η λειτουργικότητα έχει παραμείνει στα επιθυμητά επίπεδα

E.19 **A.P. Kakarountas, V. Spiliotopoulos, S. Nikolaidis, C.E. Goutis**, "*COSAFE: Efficient Safety-Critical Portable System*", in Proc. of the IEEE 2004 International Workshop on Biomedical Circuits and Systems (BioCAS'04), Singapore, pp. S1.6(13-16), Dec. 2004.

Περίληψη:
Τα κρίσιμης ασφάλειας συστήματα έχουν γίνει ευρέως διαδεδομένα στις μέρες μας, ειδικά σε εφαρμογές ιατρικής και μεταφορών. Οι στόχοι των επιπέδων ασφαλούς λειτουργίας τέτοιων συστημάτων καθορίζονται πλήρως από τα διεθνή πρότυπα. Τα χαμηλά επίπεδα ασφαλούς λειτουργίας επιτυγχάνονται εύκολα και συναντώνται στις περισσότερες ιατρικές συσκευές. Σε αυτή την εργασία, προτείνεται μία αποκεντρωμένη προσέγγιση σχεδιασμού, η οποία μιμείται την δομή του νευρικού συστήματος του ανθρωπίνου σώματος και επιτυγχάνει υψηλά επίπεδα ασφαλούς λειτουργίας, τα οποία δεν συναντώνται στην αγορά λόγω της υψηλής πολυπλοκότητας σχεδιασμού και της σημαντικής αύξηση του κόστους. Αναπτύχθηκε ένας μικροελεγκτής και αποτέλεσε το όχημα αξιολόγησης της προτεινόμενης προσέγγισης. Ενσωματώθηκε σε μία εμπορική ιατρική ογκομετρική αντλία. Τα αποτελέσματα έδειξαν κάλυψη των μόνιμων σφαλμάτων και των σφαλμάτων μετάβασης κατά 99,9% και 98% αντίστοιχα. Επιπλέον, επιτεύχθηκε παράταση της ζωής της μπαταρίας κατά 36%.

E.20 **H. Michail, A.P. Kakarountas, O. Koufopavlou, C.E. Goutis**, "*A Low-Power and High-Throughput Implementation of the SHA-1 Hash Function*", in Proc. of IEEE 2005 International Symposium on Circuits and Systems (ISCAS'05), Kobe, Japan, pp. 4086-4089, May 2005.

Περίληψη:
Οι κύριες εφαρμογές των συναρτήσεων κατακερματισμού συναντώνται στα πεδία της ακεραιότητας των επικοινωνιών και της επικύρωσης της υπογραφής. Η συνάρτηση κατακερματισμού χρησιμοποιείται στο επίπεδο ασφάλειας κάθε πρωτοκόλλου επικοινωνίας. Όμως, καθώς τα πρωτόκολλα επικοινωνίας εξελίσσονται και εμφανίζονται νέες υψηλής-απόδοσης εφαρμογές, η απόδοση των συναρτήσεων κατακερματισμού τείνει να φτάσει ένα όριο. Επιπλέον, χάρη στην τάση της αγοράς να ελαχιστοποιεί τα μεγέθη των συσκευών και να αυξάνει την αυτονομία τους για να τις κάνει φορητές, πρέπει να ληφθούν υπόψη και θέματα ισχύος. Οι υπάρχουσες υλοποιήσεις Συνάρτησης Κατακερματισμού SHA-1 (η SHA-1 είναι διαδεδομένη σε πολλά πρωτόκολλα π.χ. IPSec)) περιορίζουν την απόδοση σε ένα μέγιστο της τάξης των 2 Gbps. Σε αυτή την εργασία, μία νέα υλοποίηση έρχεται να ξεπεράσει αυτό το όριο βελτιώνοντας την απόδοση κατά 53%. Επιπλέον, η κατανάλωση ισχύος διατηρείται χαμηλή σε σύγκριση με προηγούμενες εργασίες

E.21 **A.P. Kakarountas, H. Michail, C.E. Goutis**, "*Σχεδιασμός Ταχύτατων Κρυπτογραφικών Αλγορίθμων για Διαφύλαξη Απορρήτου και Ακεραιότητας Δεδομένων*", στα πρακτικά του 1ου Πανελλήνιου Συνεδρίου Ηλεκτρολόγων Μηχανικών, Αθήνα, Μάρτιος 2005.

Περίληψη:

Σε αυτή την εργασία παρουσιάζεται μία τεχνική αποδόμησης των συναρτήσεων που ανήκουν στην οικογένεια MD4, προκειμένου να επιτευχθούν ταχύτατες υλοποιήσεις. Η προτεινόμενη τεχνική, εντοπίζει τις αλληλοεξαρτήσεις των τμημάτων που απαρτίζουν το σχεδιασμό της συνάρτησης και τα αποδομεί ανά σειρά εκτέλεσης. Στο πρώτο στάδιο, εντοπίζονται τα τμήματα τα οποία μπορούν να εκτελέσουν τις διεργασίες τους παράλληλα. Αυτή η φάση επιτρέπει τη μείωση των «καταστάσεων κυνηγητού». Στο δεύτερο στάδιο, εντοπίζονται τα τμήματα τα οποία απαιτούν ως είσοδο την έξοδο κάποιου προηγούμενου. Σε αυτή την περίπτωση δημιουργείται μία αλυσίδα διασύνδεσης των τμημάτων τοποθετώντας στην αρχή αυτά που έχουν ίδιες εισόδους με τα τμήματα που εντοπίστηκαν στο πρώτο στάδιο. Διαχωρίζοντας την αλυσίδα, κάνοντας χρήση της τεχνικής διοχέτευσης (pipeline), είναι δυνατή η μείωση της συνολικής καθυστέρησης κατά 50%. Το τελικό αποτέλεσμα, είναι η εισαγωγή ενός τμήματος προ-υπολογισμού το οποίο εκμεταλλεύεται ειδικές ιδιότητες της οικογένειας MD4

E.22 **H. Michail, A.P. Kakarountas, A. Milidonis, C.E. Goutis**, "*Low Power and High Throughput Implementation of SHA-256 Hash Function*", in Proc. of International E-Conference on Computer Science (IeCCS 2005), pp. 170-173, May 2005.

Περίληψη:

Οι συναρτήσεις κατακερματισμού και ανάμιξης (hash functions) χρησιμοποιούνται στο επίπεδο ασφαλείας σχεδόν όλων των πρωτοκόλλων επικοινωνίας καθώς επίσης και σε συστήματα επιβεβαίωσης ψηφιακών υπογραφών για ηλεκτρονικές συναλλαγές. Όσο περνά ο καιρός όλο και πιο πολύπλοκες εφαρμογές δημιουργούνται οι οποίες απευθύνονται σε περισσότερους χρήστες (clients) και απαιτούν υψηλό ρυθμό μετατροπής δεδομένων(throughput). Επίσης λαμβάνοντας υπόψη την συνεχιζόμενη τάση της αγοράς να μικραίνει τις διαστάσεις και να αυξάνει την αυτονομία των συσκευών, θέματα κατανάλωσης πρέπει επίσης να ληφθούν υπόψη. Η εδώ και καιρό φημολογούμενη επιτυχής επίθεση στην ευρύτατα χρησιμοποιούμενη συνάρτηση κατακερματισμού και ανάμιξης SHA-1 πλέον επισημοποιήθηκε από ερευνητές στην Κίνα και στις Ηνωμένες Πολιτείες. Είναι προφανές ότι στο σύντομο μέλλον η απαίτηση για πιο ασφαλείς συναρτήσεις κατακερματισμού και ανάμιξης θα εδραιωθεί αλλά επίσης αυτές θα πρέπει να ικανοποιούν τις απαιτήσεις της βιομηχανίας για την καταναλούμενη ισχύ, την έκταση που καταλαμβάνει καθώς και τον ρυθμό μετατροπής δεδομένων που θα έχουν οι αντίστοιχες υλοποιήσεις τους σε υλικό. Σε αυτήν την εργασία παρουσιάζεται μια υλοποίηση της συνάρτησης κατακερματισμού και ανάμιξης SHA-256 η οποία επιτυγχάνει ρυθμό μετατροπής δεδομένων που υπερβαίνει τα 2 Gbps. Επιπλέον η προτεινόμενη υλοποίηση έχει χαμηλότερη κατανάλωση ισχύος συγκρινόμενη με τις συμβατικές υλοποιήσεις

E.23 **A.P. Kakarountas, G. Theodoridis, T. Laopoulos, C.E. Goutis**, "*A High-Speed FPGA Implementation of the SHA-1 Hash Function*", in Proc. of IEEE Third International Workshop on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS'05), Sofia, Bulgaria, pp. 211-215, Sep. 5-7, 2005.

Περίληψη:

Οι κύριες εφαρμογές των συναρτήσεων κατακερματισμού βρίσκονται στον χώρο της ακεραιότητας των επικοινωνιών και της επικύρωσης. Σε κάθε πρωτόκολλο επικοινωνίας, ειδικά στα κινητά πρωτόκολλα, χρησιμοποιείται μία συνάρτηση κατακερματισμού στο επίπεδο της ασφάλειας. Όμως, καθώς τα πρωτόκολλα επικοινωνίας εξελίσσονται και εμφανίζονται νέες υψηλής- απόδοσης εφαρμογές, η απόδοση των συναρτήσεων κατακερματισμού τείνει να φτάσει ένα όριο. Ειδικά η Συνάρτηση Κατακερματισμού SHA-1, η οποία είναι κοινή στην πλειοψηφία των ασύρματων πρωτοκόλλων (WAP, κλπ.), περιοριζόταν σε μία μέγιστη απόδοση των 2Gbps. Σε αυτή την εργασία, παρουσιάζεται μία νέα υλοποίηση που ξεπερνάει αυτό το όριο βελτιώνοντας την απόδοση κατά 37% χωρίς σημαντικές κυρώσεις στην επιφάνεια

E.24 **H.E. Michail, A.P. Kakarountas, G.N. Selimis, C.E. Goutis**, "*State-of-the-Art Implementation of SHA-1 Hash Function for Low-Power and High Throughput*", in

Proc. of IEEE 2005 International Workshop on Power And Timing Modeling, Optimization and Simulation (PATMOS'05), Leuven, Belgium, pp. 591-600, Sep. 2005.

Περίληψη:
Σε αυτή την εργασία γίνεται ειδική μελέτη για τον σχεδιασμό του κρυπτογραφικού αλγόριθμου SHA-1 με γνώμονα την κατανάλωση ενέργειας διατηρώντας την απόδοσή του υψηλή. Η προτεινόμενη υλοποίηση επέδειξε απόδοση της τάξης του 1.7Gbps ενώ η κατανάλωση ενέργειας μειώθηκε κατά 30%, καθιστώντας την ιδανική για φορητές συσκευές επικοινωνιών

E.25 **K. Aisopos, A.P. Kakarountas, H. Michail, C.E. Goutis**, "*High throughput implementation of the new Secure Hash Algorithm through partial unrolling*", in Proc. of IEEE 2005 International Workshop on Signal Processing Systems (SiPS'05), Athens, Greece, pp. 99-103, Nov. 2-4, 2005.

Περίληψη:
Μία αναλυτική μελέτη διάφορων συνδυασμών πλεονασμού υλικού για την επίτευξη του καλύτερου λόγου απόδοσης προς επιφάνεια. Η μελέτη αυτή εφαρμόστηκε στη νέα σειρά κρυπτογραφικών αλγορίθμων Secure Hash Function type 2. Τα πειραματικά αποτελέσματα επέδειξαν υψηλούς ρυθμούς μετάδοσης ενώ η απαιτούμενη επιφάνεια ολοκλήρωσης είναι μακράν η μικρότερη συγκρινόμενη με αντίστοιχης απόδοσης υλοποιήσεις του εμπορίου

E.26 **A. Brokalakis, A.P. Kakarountas, C.E. Goutis**, "*A High-Throughput Area Efficient FPGA Implementation of AES-128 Encryption*", in Proc. of IEEE 2005 International Workshop on Signal Processing Systems (SiPS'05), Athens, Greece, pp. 116-121, Nov. 2-4, 2005.

Περίληψη:
Στη συγκεκριμένη εργασία προτείνεται η υλοποίηση μιας ειδικής αρχιτεκτονικής του Advanced Encryption Standard (AES) το οποίο αποτελεί το πιο διαδεδομένο κρυπτογραφικό αλγόριθμο. Η υλοποίηση είναι ιδανική για FPGAs και παρουσιάζει απόδοση 1Gbps κάνοντας χρήση του βέλτιστου συνδυασμού πόρων για τη μικρότερη δυνατή ολοκλήρωση

E.27 **H. Michail, A. Milidonis, A.P. Kakarountas, C.E. Goutis**, "*Novel High Throughput Implementation of SHA-256 Hash Function Through Pre-Computation Technique*", in Proc. of the IEEE 2005 International Conference on Electronics, Circuits and Systems (ICECS'05), Gammarth, Tunisia, pp. 1-4, Dec. 2005.

Περίληψη:
Μία τεχνική επαναπροσδιορισμού των χρονικών εκτελέσεων των διεργασιών του νέου Secure Hash Standard type 2 παρουσιάζεται σε αυτή την εργασία. Τα αποτελέσματα είναι ενθαρρυντικά, μιας και η απαιτούμενη επιφάνεια ολοκλήρωσης παραμένει σχεδόν αμετάβλητη συγκρινόμενη με την τυπική υλοποίηση που συναντάται στο εμπόριο. Η απόδοση όμως αυξάνεται κατά 30% περίπου καθιστώντας την προτεινόμενη υλοποίηση ιδανική για φορητές συσκευές επικοινωνιών

E.28 **M. D. Galanis, G. Dimitroulakos, A. P. Kakarountas, and C.E. Goutis**, "*Speedups from Partitioning Software Kernels to FPGA Hardware in Embedded SoCs*", in Proc. of IEEE 2005 International Workshop on Signal Processing Systems (SiPS'05), Athens, Greece, pp. 485-490, Nov. 2-4, 2005.

Περίληψη:
Τεχνική αύξησης της εκτέλεσης πυρήνων λογισμικού σε ενσωματωμένα συστήματα. Η προτεινόμενη τεχνική διαχωρίζει τους πυρήνες σε «κρίσιμους» και «μη κρίσιμους». Οι «κρίσιμοι» πυρήνες ανατίθενται απ' ευθείας στο υλικό (FPGA) ενώ οι «μη κρίσιμοι» πυρήνες στο λογισμικό ενός ενσωματωμένου μικροεπεξεργαστή. Η τεχνική παρουσιάζει σημαντικά αποτελέσματα κυρίως για εφαρμογές πολυμέσων, όπου το κέρδος σε ταχύτητα ξεπερνά το 700%. Έλαβε το Best Student Paper Award στο συνέδριο.

E.29 **I. Yiakoumis, M. Papadonikolakis, H. Michail, A.P. Kakarountas, C.E. Goutis**, "*Efficient small-sized implementation of the keyed-hash message authentication code*", in Proc. of IEEE 2005 EUROCON as finalist in the IEEE Region 8 Best Student Paper Contest, Belgrade, Yugoslavia, pp. 1875-1878, Nov. 21-24, 2005.

Περίληψη:

Υλοποίηση κρυπτογραφικού αλγορίθμου για πιστοποίηση της ταυτότητας των χρηστών ενός δικτύου. Η υλοποίηση είναι βελτιστοποιημένη ως προς την επιφάνεια ολοκλήρωσης. Παρά το γεγονός ότι δεν υστερεί σε ταχύτητα από τις εμπορικές υλοποιήσεις, είναι ιδιαίτερα μικρή σε μέγεθος, επιτρέποντας έτσι την ενσωμάτωση του σχεδιασμού σε φορητά συστήματα, όπου η επιφάνεια και η κατανάλωση ενέργειας είναι κρίσιμες παράμετροι σχεδιασμού

E.30 **D.M. Schinianakis, A.P. Fournaris, A.P. Kakarountas and T. Stouraitis**, "*An RNS Architecture of an Fp Elliptic Curve Point Multiplier*", in Proc. of IEEE International Symposium on Circuits and Systems (ISCAS) 2006, Kos Island, Greece, May 21-24, 2006.

Περίληψη:

Η πρώτη υλοποίηση στη διεθνή βιβλιογραφία ενός πολλαπλασιαστή ελλειπτικών καμπύλων, ο οποίος βασίζεται σε αναπαράσταση RNS των δεδομένων. Η επιτάχυνση των υπολογισμών πραγματοποιείται σε πολλές τάξεις μεγέθους ταχύτερα (περίπου 1000 φορές ταχύτερα για 128bit μήκος δεδομένων) ενώ η επιφάνεια ολοκλήρωσης έχει διατηρηθεί αναλογικά σε λογικά επίπεδα

E.31 **F. Aisopos, K. Aisopos, D.M. Schinianakis, H.E. Michail, A.P. Kakarountas**, "*A Novel High-Throughput Implementation of a Partially Unrolled SHA-512*" in Proc. of IEEE Mediterranean Electrotechnical Conference, MELECON 2006, Malaga, Spain, pp. 61-65, May 16-19, 2006.

Περίληψη:

Μια ταχύτατη υλοποίηση του SHA-512. Η υλοποίηση βασίζεται στο πρότυπο όπως έχει προταθεί από την NSA. Η βελτιστοποίηση της υλοποίησης έγκειται στην ορθή χρονοδρομολόγηση των διεργασιών. Η επιφάνεια μετά τη βελτιστοποίηση δεν αυξάνεται σημαντικά επιτυγχάνοντας σημαντικά επικερδή λόγο απόδοσης / κόστος

E.32 **D.M. Schinianakis, A.P. Kakarountas, T. Stouraitis**, "*A New Approach to Elliptic Curve Cryptography: An RNS Architecture*" in Proc. of IEEE Mediterranean Electrotechnical Conference, MELECON 2006, Malaga, Spain, pp. 1241-1245, May 16-19, 2006.

Περίληψη:

Η παρουσίαση μιας υλοποίησης ενός κρυπτογραφικού πυρήνα για ελλειπτικές καμπύλες ο οποίος κάνει χρήση RNS αρχιτεκτονικής, Το αποτέλεσμα είναι η επίτευξη πολύ υψηλής απόδοσης χάρης στα χαρακτηριστικά των RNS αρχιτεκτονικών ενώ το μόνο μειονέκτημα είναι το επιπλέον υλικό που απαιτείται για τη μετατροπή RNS – to –binary

E.33 **H.E. Michail, A.P. Kakarountas, A.S. Milidonis, G.A. Panagiotakopoulos, V.N. Thanasoulis, C. E.Goutis**, "*Temporal and System Level Modifications for High Speed VLSI Implementations of Cryptographic Core*" in Proc. of the IEEE 2006 International Conference on Electronics, Circuits and Systems (ICECS'06), Nice, France, pp. 1180-1183, Dec. 2006.

Περίληψη:

Τεχνικές με τις οποίες μπορεί να τροποποιηθεί ένας κρυπτογραφικός αλγόριθμος και να αυξήσει την απόδοση ακόμα και 50%. Το μόνο κόστος είναι ένα ασήμαντο ποσοστό αύξησης της απαιτούμενης επιφάνειας

E.34 **A. Milidonis, N. Alachiotis, V. Porpodas, H. Michail, *A. P. Kakarountas*, and C. E. Goutis**, "*A Decoupled Architecture of Processors with Scratch-Pad Memory Hierarchy*", in Proc. of Design, Automation & Test in Europe (DATE'07), Nice, France, pp. 612-617, April 2007.

Περίληψη:
Μια αποσυζευγμένη διάταξη δύο πυρήνων, η οποία περιλαμβάνει στην αρχιτεκτονική της μνήμη scratchpad αντί της τυπικής cache. Εκμεταλλευόμενοι τα χαρακτηριστικά της αρχιτεκτονικής, τροποποιούμε κατάλληλα το λογισμικό προκειμένου να έχουμε μέγιστη αξιοποίηση των πόρων του συστήματος. Τα αποτελέσματα είναι εξαιρετικά αφού προκύπτει speedup της τάξης του 500% σε σύγκριση με την αρχιτεκτονική που χρησιμοποιεί μνήμη cache

E.35 **M. Papadonikolakis, V. Pantazis, and A.P. Kakarountas**, "*Efficient High-Performance ASIC Implementation of JPEG-LS Encoder*", in Proc. of Design, Automation & Test in Europe (DATE'07), Nice, France, pp. 159-164, April 2007.

Περίληψη:
Στη συγκεκριμένη εργασία γίνεται πλήρη τροποποίηση του αλγόριθμου κωδικοποίησης κατά JPEG-LS, προκειμένου να επιτευχθεί η βέλτιστη ταχύτητα επεξεργασίας. Η βελτιστοποίηση πραγματοποιείται σε υψηλό επίπεδο (αλγοριθμικό και RTL) προκειμένου να υπάρχουν πάντοτε δεδομένα προς κατανάλωση από τους υπολογιστικούς πόρους του συστήματος. Αναπτύχθηκε σύστημα ειδικού σκοπού προκειμένου να επαληθευτεί η σχεδίαση του νέου κωδικοποιητή

E.36 **A.P. Kakarountas, H.E. Michail, and C.E. Goutis**, "*RipeMD-160 Implementation Optimized in Terms of Throughput*", in Proc. of 3rd International Conference on Information Technology (ICIT'07), Amman, Jordan, pp. - , May 2007.

Περίληψη:
Σχεδίαση κυκλώματος το οποίο πραγματοποιεί κωδικοποίηση – αποκωδικοποίηση κατά RIPEMD-160. Το χαρακτηριστικό του στοιχείο είναι ο υψηλός ρυθμός κωδικοποίησης-αποκωδικοποίησης. Έγινε δεκτό ως ένα από τα καλύτερα άρθρα και προστέθηκε ως άρθρο σε περιοδικό.

E.37 **H.E. Michail, A.P. Kakarountas, G. Selimis and C.E. Goutis**, "*Throughput Optimization of the Cipher Message Authentication Code*", in Proc. of the 2007 IEEE Intl. Conf. on Digital Signal Processing (DSP'07), Cardiff, Wales, UK, pp. 495-498, July 2007.

Περίληψη:
Σχεδιασμός συστήματος CMAC. Είναι το πιο αποδοτικό, από άποψη ταχύτητας επεξεργασίας δεδομένων, σε όλη τη διεθνή βιβλιογραφία. Η αυξημένη ταχύτητα οφείλεται στο συγχρονισμό της επεξεργασίας με την μεταφορά των δεδομένων από την ιεραρχία μνήμης που χρησιμοποιείται από το σύστημα

E.38 **A.P. Kakarountas, H. Michail, C.E. Goutis, and C. Efstathiou**, "*Implementation of HSSec: a High-Speed Cryptographic Co-processor*", in Proc. of the 2007 IEEE Conference on Emerging Technologies and Factory Automation, (ETFA 2007), Patras, Greece, pp. 625-631, Sept. 2007.

Περίληψη:
Στη συγκεκριμένη εργασία παρουσιάζεται ένας πλήρως προγραμματιζόμενος μικροελεγκτής, ιδανικός για κρυπτογραφικές εφαρμογές. Είναι βελτιστοποιημένος για υψηλή απόδοση, ενώ επιτρέπει παράλληλη εκτέλεση δύο διαφορετικών αλγορίθμων, εκμεταλλευόμενος την ιεραρχία μνήμης αλλά και τους επεξεργαστικούς πόρους που ενσωματώνει

E.39 **A. Kakarountas, H. Michail, and C.E. Goutis** "*Integration of a Concurrent Signature Monitoring Mechanism in a System-on-a-Chip*", in Proc. of the 2007

IEEE International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS'07), Rabat, Morocco, pp. 47-51, Sept. 2007.

Περίληψη:

Παρουσιάζεται ένας προγραμματιζόμενος ελεγκτής υπογραφής κώδικα ο οποίος εξασφαλίζει την εκτέλεση του κώδικα εφαρμογής, ελέγχοντας τόσο τη συνοχή του όσο και αυστηρά χρονικά περιθώρια μέσα στα οποία θα πρέπει να αποκριθεί το σύστημα. Ο μηχανισμός αυτός είναι ενδεδειγμένος για κρίσιμα ενσωματωμένα συστήματα, όπου η ασφάλεια λειτουργίας πρέπει να παραμένει υψηλή

E.40 **A. P. Kakarountas, H.E. Michail, G. Theodoridis and C. E. Goutis** "*A Segmented High-Speed Counter Based on the Use of Redundant Bits*", in Proc. of the 16th IFIP/IEEE Conference on Very Large Scale Integration (VLSI-SOC'08), Rhodes, Greece, pp. 42 – 48, Oct. 2008.

Περίληψη:

Εισήγηση για τη χρήση ενός τμηματοποιημένου απαριθμητή δυαδικού συστήματος radix-2, ο οποίος αξιοποιεί περιττά bits, προκειμένου να επιτύχει την συντομότερη εναλλαγή των bits υψηλότερης τάξης. Αυτό έχει σαν αποτέλεσμα να δημιουργηθεί μια συστολική δομή αποτελούμενη από μονάδες των 3-bit οι οποίες με μια μικρή επιβάρυνση σε επιφάνεια επιτυγχάνουν υψηλής ταχύτητας λειτουργία. Τα αποτελέσματα δείχνουν ικανοποιητικά χαρακτηριστικά ως προς το κόστος και την επιφάνεια ολοκλήρωσης, σε σύγκριση με ανταγωνιστικές δομές απαριθμητών. Η ταχύτητα όμως που επιτυγχάνεται είναι 20%-350% υψηλότερη από τον ανταγωνισμό

E.41 **A. Milidonis, V. Porpodas, N. Alachiotis, A. Kakaroudas, H. Michail, G. Panagiotakopoulos and C.E. Goutis**, "*A Scratch-Pad Memory Accelerator for Exploiting Run-Time Reuse*", in Proc. of the 16th IFIP/IEEE Conference on Very Large Scale Integration (VLSI-SOC'08), Rhodes, Greece, pp. 271 – 276, Oct. 2008.

Περίληψη:

Μια αποσυζευγμένη διάταξη δύο πυρήνων, η οποία περιλαμβάνει στην αρχιτεκτονική της μνήμη scratchpad αντί της τυπικής cache. Εκμεταλλευόμενοι τα χαρακτηριστικά της αρχιτεκτονικής, τροποποιούμε κατάλληλα το λογισμικό προκειμένου να έχουμε μέγιστη αξιοποίηση των πόρων του συστήματος. Τα αποτελέσματα είναι εξαιρετικά αφού προκύπτει speedup της τάξης του 500% σε σύγκριση με την αρχιτεκτονική που χρησιμοποιεί μνήμη cache. Πρόκειται για μια πρωτόλεια έκδοση της Δ15

E.42 **D. Schinianakis, A. Kakarountas, T. Stouraitis, A. Skavantzos**, "*Elliptic Curve Point Multiplication in GF(2^n) Using Polynomial Residue Arithmetic*", in Proc. of the IEEE 2009 International Conference on Electronics, Circuits and Systems (ICECS'09), Medina, Tunisia, pp. 980-983, Dec. 2009.

Περίληψη:

Οι σύγχρονες εφαρμογές κρυπτογράφησης βασίζονται στην αναδυόμενη τάση για χρήση ελλειπτικών καμπυλών (ECC). Ένα δομικό στοιχείο για αυτή την κρυπτογράφηση είναι ο πολλαπλασιαστής σημείου ελλειπτικής καμπύλης. Πολλές υλοποιήσεις έχουν προταθεί, οι οποίες όμως παρουσιάζουν χαμηλή απόδοση, κυρίως λόγω της πολυπλοκότητάς τους. Σε αυτή την εργασία παρουσιάζεται μια δομή για την υλοποίηση ενός τέτοιου πολλαπλασιαστή ο οποίος βασίζεται στη χρήση αριθμητικού συστήματος υπολοίπου (RNS). Αυτό έχει σαν αποτέλεσμα να μειωθεί σημαντικά η πολυπλοκότητα και να αυξηθεί η απόδοση κατά μια τάξη μεγέθους. Πρόκειται για μια πρωτόλεια έκδοση της Δ13

E.43 **E. Hatzidimitriou, A.P. Kakarountas**, "*Implementation of a Low Cost Crypto-System for P1619 (XTS) on FPGA*", in Proc. of 11th International Workshop on Computer Science and Information Technologies (CSIT), Rethymnon, Crete, Greece, pp. 1–4, Oct. 2009.

Περίληψη:

Η πρώτη υλοποίηση του P1619 εξ ολοκλήρου σε υλικό (hardware) προκειμένου να επιτευχθεί η μεγαλύτερη ασφάλεια. Υλοποίηση του Narrow Block EME αλγορίθμου, όπως έχει προταθεί από το P1619 Working Group. Πρόκειται για ένα υπό ανάπτυξη πρότυπο του IEEE το οποίο αποσκοπεί στην ασφάλεια των δεδομένων σε αποθηκευτικά μέσα που διαμοιράζονται πολλοί χρήστες. Πρόκειται για την πρώτη υλοποίηση διεθνώς και αποτελεί σημείο αναφοράς για τις υλοποιήσεις Narrow Block βασισμένες στον EME32

E.44 **C. Chrysoulas, N. Sklavos, A.P. Kakarountas**, "*Enhancing Service Portability in Upcoming 3G UMTS Networks & Security Aspects*", in Proc. of IEEE Mediterranean Electrotechnical Conference, MELECON 2010, Valetta, Malta, pp. 420-424, April 2010.

Περίληψη:
Μελέτη όλων των συστημάτων και APIs που συνθέτουν τις υπηρεσίες Ιστού, προκειμένου να δημιουργηθεί ένα ενιαίο μοντέλο υπηρεσιών Ιστού, με κύριο στόχο την επίτευξη του υψηλότερου βαθμού ασφάλειας στην επικοινωνία. Στη μελέτη λαμβάνονται υπόψη όλες οι ετερογενείς οντότητες που δύναται να συμμετέχουν σε ένα δίκτυο 3G. Επίσης, λήφθηκε υπόψη η εξέλιξη των υπηρεσιών και των τεχνολογιών που χρησιμοποιούνται σε δίκτυα κινητής δικτύωσης. Αξιοποιώντας την προαναφερθείσα μελέτη, είναι δυνατή η υλοποίησή του προτεινόμενου μοντέλου και η διάθεση των υπηρεσιών

E.45 **E. Hatzidimitriou, A.P. Kakarountas**, "*Implementation of a P1619 Crypto-Core for Shared Storage Media*", in Proc. of IEEE Mediterranean Electrotechnical Conference, MELECON 2010, Valetta, Malta, pp. 597-601, April 2010.

Περίληψη:
Η πρώτη υλοποίηση του P1619 εξ ολοκλήρου σε υλικό (hardware) προκειμένου να επιτευχθεί η μεγαλύτερη ασφάλεια. Υλοποίηση του Wide Block XTS-AES αλγορίθμου, όπως έχει προταθεί από το P1619 Working Group. Πρόκειται για ένα υπό ανάπτυξη πρότυπο του IEEE το οποίο αποσκοπεί στην ασφάλεια των δεδομένων σε αποθηκευτικά μέσα που διαμοιράζονται πολλοί χρήστες. Πρόκειται για την πρώτη υλοποίηση διεθνώς και αποτελεί σημείο αναφοράς για τις υλοποιήσεις Wide Block βασισμένες στον XTS-AES. Ο αλγόριθμος που υλοποιείται είναι η βασική διαφορά από την εργασία E43

E.46 **E. Arvaniti, I. Mavridis, A. Kakarountas**, "*Exploration of 2D Cellular Automata as Binary Sequence Generators*", in Proc. of IEEE Computer Society Annual Symposium on VLSI, ISVLSI 2010, Lixouri Kefalonia, Greece, pp. 41-45, July 2010.

Περίληψη:
Διερεύνηση των κυψελιδικών αυτόματων 2Δ, 2 χρωμάτων (κατ' αντιστοιχία της δυαδικής λογικής) προκειμένου να εντοπιστούν γνωστές ακολουθίες (π.χ. μετρητές, LFSR κ.ο.κ.) που χρησιμοποιούνται κατά κόρο από τους σχεδιαστές ψηφιακών συστημάτων. Εντοπίστηκαν συγκεκριμένες ακολουθίες οι οποίες επαναλαμβάνουν την αρίθμηση mod(2n-1) με σταθερό βήμα 1, χρησιμοποιώντας k bits, όπου k>n. Το Παρότι απαιτούνται περισσότερα ψηφία για την απεικόνιση, η πολυπλοκότητα σχεδιασμού της γεννήτριας είναι σημαντικά μικρή με αποτέλεσμα να παρουσιάζονται σημαντικές ευκαιρίες για ένα νέο πεδίο κυκλωμάτων

E.47 **D. Tychalas, A. Kakarountas**, "*Planning and Development of the Backend Software for an Electronic Health Record Client based on the Android Platform*", in Proc. of 14th Panhellenic Conference on Informatics, PCI 2010, Tripoli, Greece, pp. 3-6, September 2010.

Περίληψη:
Η εργασία αυτή παρουσιάζει στο επίπεδο λογισμικού ενός υπό ανάπτυξη ενσωματωμένου συστήματος, την backend διεπαφή. Για την υλοποίηση της αξιοποιήθηκε η πλατφόρμα Android 2.1 και πυρήνας Linux. Στόχος ήταν η δημιουργία ενός low-cost συστήματος το

οποίο θα επιτρέπει την έξυπνη και με ασφάλεια διαχείριση δεδομένων από ένα ιατρικό φάκελο, αποκλειστικά από εξουσιοδοτημένους λειτουργούς υγείας

E.48 **E. Hatzidimitriou, A.P. Kakarountas, A. Milidonis**, "*Exploration and Enhancement of P1619-Based Crypto-Cores for Efficient Performance*", in Proc. of the IEEE 2011 International Conference on Consumer Electronics (ICCE'11), Las Vegas, Nevada, USA, pp. 369-370, Jan. 2011.

Περίληψη:
Μια μελέτη της εξέλιξης του προτύπου IEEE P1619, το οποίο αποσκοπεί στην ασφάλεια των δεδομένων σε αποθηκευτικά μέσα που διαμοιράζονται πολλοί χρήστες. Καταγράφεται η διεθνής τάση των προτεινόμενων υλοποιήσεων από ερευνητές καθώς και η παροχή έτοιμων λύσεων στην αγορά. Από την εργασία αυτή προκύπτει ότι οι λύσεις βασίζονται κατά κύριο λόγο στην αξιοποίηση των χαρακτηριστικών που προσφέρουν έτοιμες τεχνολογίες και όχι στην βελτίωση των αλγορίθμων. Προτείνεται μια λύση μετασχηματισμού των αλγορίθμων η οποία επιδεικνύει σημαντική βελτίωση έναντι του ανταγωνισμού

E.49 **A.P. Kakarountas, E. Hatzidimitriou, A. Milidonis**, "*A Survey on Throughput-Efficient Architectures for IEEE P1619 for Shared Storage Media*", in Proc. of the 16th IEEE symposium on Computers and Communications, ISCC 2011, Corfu, Greece, pp. 758-763, June 2011.

Περίληψη:
Μια μελέτη ως προς την απόδοση προτεινόμενων λύσεων για το πρότυπο IEEE P1619, το οποίο αποσκοπεί στην ασφάλεια των δεδομένων σε αποθηκευτικά μέσα που διαμοιράζονται πολλοί χρήστες. Για πρώτη φορά προτείνονται δύο εναλλακτικές αρχιτεκτονικές οι οποίες παρουσιάζουν σημαντικά βελτιωμένη απόδοση έναντι του ανταγωνισμού, σημειώνοντας μέχρι και 300% speedup δίχως επιβάρυνση σε επιφάνεια και κόστος υλοποίησης. Η μελέτη αφορά τεχνολογίες FPGA

E.50 **A.P. Kakarountas, E. Hatzidimitriou, A. Milidonis**, "*High-Throughput ASIC Implementation of an Encryption Core for Securing Shared Storage Media*", in Proc. of the 17th International Conference on Digital Signal Processing, DSP 2011, Corfu, Greece, pp. – (TC3.1), July 2011.

Περίληψη:
Σε συνέχεια της εργασίας E49, λαμβάνονται υπόψη και τεχνολογίες ολοκλήρωσης σε σιλικόνη, με τη χρήση γνωστών foundries. Με αυτό τον τρόπο η απόδοση που επιτυγχάνεται από την αξιοποίηση των προτεινόμενων αρχιτεκτονικών είναι σημαντικά υψηλότερος λόγω της πλήρης μορφοποίησης της μάσκας ολοκλήρωσης. Στην περίπτωση των τεχνολογιών FPGA, υπάρχει σημαντικός σχεδιαστικός περιορισμός λόγω των δομών τύπου CLBs και Slices που είναι προ-σχεδιασμένες στα FPGAs

E.51 **A.P. Kakarountas, I. Mavridis**, "*Efficient Exploitation of Parallel Computing on the Server-Side of Health Organizations' Intranet for Distributing Medical Images to Smart Devices*", in Proc. of the 2nd International ICST Conference on Wireless Mobile Communication and Healthcare, Mobihealth 2011, Kos Island, Greece, pp. , October 2011.

Περίληψη:
Σε αυτή την εργασία παρουσιάζεται μια αρχιτεκτονική συστήματος που αξιοποιεί τις τεχνικές της εξ αποστάσεως πρόσβασης (remote access) και της παράλληλης επεξεργασίας δεδομένων σε αρχιτεκτονική CUDA, προκειμένου να διαμορφώσει ιατρικό περιεχόμενο (στην εργασία εικόνα) προσαρμοσμένο στις ανάγκες του εκάστοτε φορέα/επαγγελματία υγείας που ζητά πρόσβαση μέσω έξυπνης συσκευής. Τα χαρακτηριστικά της συσκευής αναγνωρίζονται και το περιεχόμενο προσαρμόζεται near real-time στις απαιτήσεις του χρήστη. Επιπλέον, δεν λαμβάνει κανένα προσωπικό/κρίσιμο στοιχείο για τον ασθενή επιτυγχάνοντας παράπλευρα και υψηλού επιπέδου ασφάλεια.

Ε.52 **A.P. Kakarountas, E. Hatzidimitriou, P. Kitsos**, "*Cipher Text Stealing Integrated in Implementations of IEEE P1619 for Shared Storage Media*", accepted for inclusion in Proc. of the 6th International Symposium on Communications, Control, and Signal Processing, ISCCSP 2014, Athens, Greece, pp. - , May 2014.

Περίληψη:
Παρουσιάζεται για πρώτη φορά το mode λειτουργίας Cipher Text Stealing (CTS) όπως περιγράφεται από το διεθνές πρότυπο P1619. Αναγνωρίζονται οι αλλοιώσεις στα χαρακτηριστικά των σχεδιασμών που δεν το ενσωματώνουν και υποδεικνύει τον τρόπο με τον οποίο θα πρέπει να σχεδιάζονται οι πυρήνες P1619.

Ε.53 **A.P. Kakarountas, S. Dragoumanos, K. Kakarountas**, "*Extending Visitor's Reality at Museums*", accepted for inclusion in Proc. of the 5th International Conference on Information, Intelligence, Systems and Applications, IISA 2014, Chania, Greece, pp. - , July 2014.

Περίληψη:
Μια καινοτόμος εργασία που αναφέρεται σε μια ολοκληρωμένη λύση επαύξησης πραγματικότητας στα μουσεία προσφέροντας υλικό στον επισκέπτη γύρω από το έκθεμα, χωρίς να αποσπάται πλέον από πινακίδες. Στην προτεινόμενη λύση, περιλαμβάνεται ενσωματωμένο σύστημα αναγνώρισης του προσώπου του επισκέπτη και των χαρακτηριστικών του και υπολογισμού της γωνίας θέασης, προκειμένου να διαμορφωθεί κατάλληλα η υπέρθεση των πληροφοριών στην βιτρίνα του εκθέματος. Η υπέρθεση επιτυγχάνεται με ψευδο-ολογραφική προβολή από μικρο-προβολέα.

Ε.54 **P. Christodoulou, I. Diamantis, S. Dragoumanos, A.P. Kakarountas**, "*A Marketing Tool Based on Games for Smart Devices*", accepted for inclusion in Proc. of the 18th Panhellenic Conference on Informatics (PCI 2014), Athens, Greece, pp. - , October 2014.

Περίληψη:
Πρόκειται για εργασία σε εξέλιξη (work-in-progress) κατά την οποία αξιοποιούνται γνώσεις mobile computing και marketing προκειμένου να εισαχθεί στην αγορά της διαφήμισης ένα νέο εργαλείο προώθησης και προσβολής. Αντικείμενο της εργασίας είναι η δημιουργία ενός απλού παιχνιδιού που εκτυλίσσεται τόσο στον εικονικό κόσμο μιας έξυπνης συσκευής, όσο και στον πραγματικό κόσμο. Όταν ολοκληρώνεται μια αποστολή στον εικονικό κόσμο ακολουθεί μια συμπληρωματική στον πραγματικό. Ακολουθούνται όλοι οι κανόνες gamification, με επιβραβεύσεις και στους δύο κόσμους, και τεχνικές παρότρυνσης. Το έργο αυτό είναι μέρος ενός μεγαλύτερου έργου, όπου θα δημιουργηθεί ένα δίκτυο διασυνδεδεμένων ενσωματωμένων συστημάτων για την παρουσίαση πιο σύνθετων παιγνίων.

ΣΤ. Άλλες Δημοσιεύσεις (Συνέδρια δίχως κριτές, Μη επιστημονικά περιοδικά, Τεχνικές αναφορές κ.λ.π.)

ΣΤ.1. ***Athanasios Kakarountas****, "Greek Chapter Starts Its Life Cycle with Distinguished Lecturer Talk", IEEE Consumer Electronics Magazine, pp. 15, Jan. 2012.*

Περίληψη:
Σε αυτό το άρθρο παρουσιάζεται η έναρξη του IEEE Consumer Electronics Society – Greece Section με εναρκτήρια ομιλία του Dr. Tomas Coughlin σχετικά με τα συστήματα αποθήκευσης δεδομένων.

ΣΤ.2. ***Athanasios Kakarountas****, «Η εποχή της αυτοδιάγνωσης», The Economist (ένθετο περιοδικό της εφημερίδας «Η Καθημερινή»), σελ. 92, τεύχος 46, Δεκ. 2007*

Περίληψη:

Σε αυτή την εργασία παρουσιάζεται μια ανασκόπηση των συστημάτων που ασχολούνται με την καθημερινή υποστήριξη ασθενών και την ανάγκη για υψηλή αξιοπιστία. Προτείνεται ως λύση που προσφέρει υψηλή αξιοπιστία η υιοθέτηση σχεδιασμού κυκλωμάτων και επιλογής της αρχιτεκτονικής των συστημάτων, ο οποίος βασίζεται σε κωδικοποίηση ανίχνευσης/διόρθωσης σφαλμάτων. Αυτά τα κυκλώματα πρέπει να είναι πλήρως αυτό-εξεταζόμενα (totally self-checking) και ως παράδειγμα επιτυχούς εφαρμογής (proof of concept) γίνεται αναφορά στο πρόγραμμα CoSafe και το προϊόν της Micrel Medical Devices S.A., την αντλία έγχυσης ινσουλίνης Rythmic pump.

Ζ. Εργασίες που έχουν υποβληθεί

Ζ.1 ***A.P. Kakarountas,*** *"P1619 – Hardware Implementations review from an architectural perspective", IEEE Transactions on Circuits and Systems II*
Περίληψη:
Σε αυτή την εργασία επιχειρείται μια ανασκόπηση των προτεινόμενων σποραδικά αρχιτεκτονικών και κυκλωμάτων στην διεθνή βιβλιογραφία και η ανάδειξη εκείνων των χαρακτηριστικών που θα πρέπει να αξιοποιηθούν από ένα σχεδιαστή συστημάτων ή τον κατασκευαστή μέσων αποθήκευσης δεδομένων, προκειμένου να επιτευχθούν στόχοι σχεδίασης που έχει θέσει (π.χ. χαμηλό κόστος, υψηλή απόδοση). Σχετίζεται με όλες τις εργασίες που έχουν υποβληθεί για το P1619 πρότυπο.

Ζ.2 ***A.P. Kakarountas****, "Disappearing computing for Elderly Assisted Living", MobiHealth 2014, 3-5 November 2014, Athens*
Περίληψη:
Σε αυτή την εργασία παρουσιάζεται ένα σύστημα συσκευών (ενσωματωμένων συστημάτων) που ενσωματώνεται στην καθημερινότητα ηλικιωμένων προκειμένου να τους βοηθήσουν στην καθημερινότητά τους και εισάγοντας στη ζωή τους με ήπιο τρόπο υπηρεσίες ιστού. Οι συσκευές έχουν «μεταμφιεστεί» σε συσκευές με τις οποίες έχει συνηθίσει κάποιος ηλικιωμένος την χρήση και κατά συνέπεια α) δεν τις απορρίπτει, β) είναι εξοικειωμένος. Η ανοικτή αρχιτεκτονική επιτρέπει την δημιουργία ενός συστήματος που παρουσιάζει μεγάλο βαθμό διασυνδεσιμότητας και υποστήριξης πλήθους εφαρμογών.

Ζ.3 ***A.P. Kakarountas****, I. Mavridis, "Remote Parallel Processing for Displaying Medical Images on Smart Devices", IEEE Transactions on Biomedical Engineering (To be submission on July)*
Περίληψη:
Αυτή η εργασία αποτελεί την ολοκλήρωση της εργασίας Ε51. Προτείνεται συγκεκριμένο σύστημα το οποίο παρέχει απομακρυσμένη και διαβαθμισμένη πρόσβαση σε ιατρικά δεδομένα (στην περίπτωση που μελετάται στην εργασία, ιατρικές εικόνες) και τροποποιεί την παρεχόμενη πληροφορία με βάση α) την ανάλυση της συσκευής που αιτείται την απόκτηση της συσκευής, β) το πρότυπο της χώρας από όπου γίνεται η αίτηση, γ) την διαβάθμιση ασφαλείας που έχει ο χρήστης και όλα αυτά χωρίς να παρέχεται αυτούσια η πληροφορία αλλά σαν προσαρμοζόμενη εικονική οθόνη στον οικείο οργανισμό υγείας. Ιδιαίτερη αναφορά γίνεται στην παράλληλη επεξεργασία (που επιτυγχάνεται με αρχιτεκτονική CUDA) και την ποιότητα της επικοινωνίας.

Ζ.4 ***A.P. Kakarountas****, S. Dragoumanos, K. Kakarountas, "Extending Visitor's Reality at Museums", Int. J. of Computational Intelligence Studies, Special Issue on: "Computational Intelligence in Cultural Informatics" (To be submission on September)*
Περίληψη:
Αυτή η εργασία αποτελεί την επέκταση της εργασίας Ε53, που αναφέρεται σε μια ολοκληρωμένη λύση επαύξησης πραγματικότητας στα μουσεία προσφέροντας υλικό στον επισκέπτη γύρω από το έκθεμα, χωρίς να αποσπάται πλέον από πινακίδες. Στην προτεινόμενη

λύση, περιλαμβάνεται ενσωματωμένο σύστημα αναγνώρισης του προσώπου του επισκέπτη και των χαρακτηριστικών του και υπολογισμού της γωνίας θέασης, προκειμένου να διαμορφωθεί κατάλληλα η υπέρθεση των πληροφοριών στην βιτρίνα του εκθέματος. Η υπέρθεση επιτυγχάνεται με ψευδο-ολογραφική προβολή από μικρο-προβολέα

Z.5 ***A.P. Kakarountas****, "Cellular Automat for Single Step Forward Counters", IEEE Transactions on Computers (To be submitted on August)*
Περίληψη:
Αυτή η εργασία βασίζεται στα ευρήματα της εργασίας Ε46, και προσαρμόζει το σχεδιασμό που παρουσιάστηκε στην εργασία Ε14, προκειμένου να παρουσιαστεί για πρώτη φορά στην βιβλιογραφία ένας ταχύτατος απαριθμητής. Το βήμα μέτρησης είναι +1 και παράγει την δυαδική ακολουθία αξιοποιώντας μια τελείως διαφορετική κωδικοποίηση (κυψελιδικό αυτόματο) η οποία όμως είναι διαχωρίσιμη (seperable) με αποτέλεσμα να μην υπεισέρχεται καθυστέρηση αποκωδικοποίησης.

Z.6 ***A.P. Kakarountas****, H.E. Michail, "Hardware Exploration of SHA-1 like Hash Cores Tolerant to Power Attacks", DATE 2014 (To be submitted on September)*
Περίληψη:
Σε αυτή την εργασία πραγματοποιείται μελέτη του SHA-1 κρυπτογραφικού αλγορίθμου και των ομοειδών του και το πόσο εκτεθειμένοι είναι σε επιθέσεις τύπου Power Attack, Differential Power Attack κ.ο.κ. Επιχειρείται μια χαρτογράφηση των αναγκών σε ασφάλεια και η πρόταση λύσεων σε FPGA και ASIC τεχνολογίες.

Z.7 ***A.P. Kakarountas****, H.E. Michail, "SHA-256 Hardware Exploration for FPGA and ASIC Technologies", DATE 2014 (To be submitted on September)*
Περίληψη:
Σε αυτή την εργασία πραγματοποιείται μελέτη του SHA-256 κρυπτογραφικού αλγορίθμου και των ομοειδών του και το πόσο εκτεθειμένοι είναι σε επιθέσεις τύπου Power Attack, Differential Power Attack κ.ο.κ. Επιχειρείται μια χαρτογράφηση των αναγκών σε ασφάλεια και η πρόταση λύσεων σε FPGA και ASIC τεχνολογίες.

Z.8 S. Dragoumanos, ***A.P. Kakarountas****, "Interactivity with gestures (Part I)", IEEE Consumer Electronics Society's Magazine (To be submitted on October)*
Περίληψη:
Πρόκειται για μια σειρά 2 εκπαιδευτικών εργασιών, με τις οποίες μπορεί κάποιος εύκολα και γρήγορα να αξιοποιήσει σύγχρονες τεχνολογίες προκειμένου να δημιουργήσει απλά User Interfaces για ενσωματωμένα συστήματα (αλλά και γενικής χρήσης υπολογιστικά συστήματα) με τη χρήση χειρονομιών. (Πρόκειται για το πρώτο μέρος)

Z.9 ***A.P. Kakarountas****, E. Arvaniti, S. Dragoumanos, "Brain-Computing for on an Embedded Portable System for Disabled Patients due to Neurological Cause", IEEE Transactions on Biomedical Engineering (To be submission on October)*
Περίληψη:
Σε αυτή την εργασία παρουσιάζονται τα αποτελέσματα 5-ετούς έρευνας σε θέματα αναγνώρισης μοτίβων εγκεφαλικής δραστηριότητας με τη χρήση ειδικών αισθητήρων και συσκευών. Αξιοποιώντας επιπλέον μια κάμερα ενσωματωμένη σε ένα απλό σύστημα εισόδου-εξόδου με τον χρήστη, ανιχνεύεται η προσήλωση ενός ασθενή (ο οποίος έχει αδυναμία κίνησης και επικοινωνίας λόγω νευρολογικών αιτίων) προς μια κατεύθυνση και την αντίστοιχη κίνηση ενός επιλογέα σε ένα εικονικό πληκτρολόγιο. Μπορεί με αυτό τον τρόπο να συντάξει λέξεις και στο τέλος να τις ακούσει με μηχανική φωνή. Η εργασία απέσπασε βραβείο το 2012.

Z.10 S. Dragoumanos, ***A.P. Kakarountas****, "Interactivity with gestures (Part II)", IEEE Consumer Electronics Society's Magazine (To be submitted on November)*

Περίληψη:
Πρόκειται για μια σειρά 2 εκπαιδευτικών εργασιών, με τις οποίες μπορεί κάποιος εύκολα και γρήγορα να αξιοποιήσει σύγχρονες τεχνολογίες προκειμένου να δημιουργήσει απλά User Interfaces για ενσωματωμένα συστήματα (αλλά και γενικής χρήσης υπολογιστικά συστήματα) με τη χρήση χειρονομιών. (Πρόκειται για το δεύτερο μέρος)

ΧΙΙ. ΑΝΑΦΟΡΕΣ ΣΤΟ ΕΡΓΟ ΑΠΟ ΑΛΛΟΥΣ ΕΡΕΥΝΗΤΕΣ

Αναφορές στο ερευνητικό έργο: 427 - (Publish or Perish: h-index=12, g-index=18) – πηγή αναζήτησης Google Scholar

ΔΗΜΟΣΙΕΥΣΕΙΣ ΣΕ ΔΙΕΘΝΗ ΠΕΡΙΟΔΙΚΑ ΜΕ ΚΡΙΤΕΣ

Δ.2 **A. Milidonis, G. Dimitroulakos, M. D. Galanis, A. P. Kakarountas, G. Theodoridis, C.Goutis, and F.Catthoor**, "A Framework for Data Partitioning for C++ Data-Intensive Applications", *Journal of Design Automation for Embedded Systems*, Springer Science+Business Media B.V., Vol. 9, No. 2, pp. 101-121, June. 2005.

Αναφορές από:

1. L. Bisdounis, S. Blionas, E. Macii, S. Nikolaidis and R. Zafalon, "Implementation Strategy and Results of an Energy-Aware System-on-Chip for 5 GHz WLAN Applications", Journal of Low Power Electronics, ASP, Vol. 2, No. 1, pp. 18-26, 2006.

Δ.3 **M.D. Galanis, A. Milidonis, A.P. Kakarountas, and C.E. Goutis**, "A Design Flow for Speeding-up DSP Applications in Heterogeneous Reconfigurable Systems", *Microelectronics Journal, Elsevier*, vol 37, pp. 554-564, 2006.

Αναφορές από:

1. Ratnakar, AR.; MengChu Zhou, "An ultrasound system for tumor detection in soft tissues using low transient pulse," Automation Science and Engineering (CASE), 2011 IEEE Conference on, vol., no., pp.684,689, 24-27 Aug. 2011 (doi: 10.1109/CASE.2011.6042478)
2. Jian Wen Wang, Zheng Feng Wang, Peng Li, "The Research and Realization of Capacitive Current on Line Measurement Based on DSP", in Applied Mechanics and Materials, Trans. Tech. Publications, vol 195-196, pp. 195-199, Aug. 2012 (10.4028/www.scientific.net/AMM.195-196.195)
3. Ratnakar, AR.; Zhou, M., "An Ultrasound System for Tumor Detection in Soft Tissues Using Low Transient Pulse," Systems Journal, IEEE , vol.PP, no.99, pp.1,10. doi: 10.1109/JSYST.2013.2295254

Δ.4 **A.P. Kakarountas, H. Michail, A. Milidonis, G. Theodoridis, C.E Goutis**, "High-Speed FPGA Implementation of Secure Hash Algorithm for IPSec and VPN Applications", Journal of

Supercomputing, Springer Science + Business Media, vol. 37, pp. 179–195, 2006

Αναφορές από:

1. Nalini C. Iyer and Sagarika Mandal, “Implementation of Secure Hash Algorithm-1 using FPGA”, in International Journal of Information and Computation Technology, Volume 3, Number 8, pp. 757-764, 2013.

2. Mohsen Bahramali, Jin Jiang, Arash Reyhani-Masoleh, “A Fault Detection Scheme for the FPGA Implementation of SHA-1 and SHA-512 Round Computations”, in Journal of Electronic Testing (JETTA), Springer, Volume 27, Issue 4, pp 517-530, Aug. 2011.

3. Je-Hoon LEE, Sang-Choon KIM, Young-Jun SONG, “High-Speed FPGA Implementation of the SHA-1 Hash Function”, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E94-A, No.9, pp.1873-1876, 2011.

4. Isobe, T.; Tsutsumi, S.; Seto, K.; Aoshima, K.; Kariya, K., "10 Gbps implementation of TLS/SSL accelerator on FPGA," Quality of Service (IWQoS), 2010 18th International Workshop on , vol., no., pp.1,6, 16-18 June 2010 (doi: 10.1109/IWQoS.2010.5542723)

5. Jianhua He; Hu Chen; Huaqiang Huang, "A compatible SHA series design based on FPGA," Electrical Engineering/Electronics Computer Telecommunications and Information Technology (ECTI-CON), 2010 International Conference on , vol., no., pp.380,384, 19-21 May 2010

6. S. Collange, Y.S. Dandass, M. Daumas, D. Defour, “Using Graphics Processors for Parallelizing Hash-Based Data Carving”, in Proc of 42nd Hawaii International Conference on System Sciences (HICSS 2009), pp.1-10, 5-8 Jan. 2009.

7. Y.S. Dandass, N.J. Necaise, S.R. Thomas, “An Empirical Analysis of Disk Sector Hashes for Data Carving”, in Journal of Digital Forensic Practice, Vol. 2, Is. 2, Ap. 2008, pp. 95-104.

8. Wesley James Holland. A framework for automatically generating optimized digital designs from C-language loops. Master Thesis, Electrical & Computer Engineering, Mississippi State University, Mississippi, USA. May 2008.

9. Yoginder S. Dandass, “Using FPGAs to Parallelize Dictionary Attacks for Password Cracking”, in Proc of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), pp. 485-485, Jan. 2008.

Δ.6 **I. Yiakoumis, M. Papadonikolakis, H.E. Michail, A.P. Kakarountas, C.E. Goutis** “Maximizing the hash function of authentication codes”, IEEE Potentials, vol. 25, iss. 2, pp. 9–12, 2006

Αναφορές από:

1. Je-Hoon LEE, Sang-Choon KIM, Young-Jun SONG, “High-Speed FPGA Implementation of the SHA-1 Hash Function”, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E94-A, No.9, pp.1873-1876, 2011.

2. Eun-Hee Lee, Je-Hoon Lee, Il-Hwan Park and Kyoung-Rok Cho, “Implementation of

high-speed SHA-1 architecture", IEICE Electron. Express, Vol. 6, No. 16, pp. 1174-1179, 2009.

3. (*) Michail, H.E.; Kakarountas, AP.; Milidonis, AS.; Goutis, C.E., "A Top-Down Design Methodology for Ultrahigh-Performance Hashing Cores," Dependable and Secure Computing, IEEE Transactions on , vol.6, no.4, pp.255,268, Oct.-Dec. 2009 (doi: 10.1109/TDSC.2008.15)

Δ.7 **H.E. Michail, A.P. Kakarountas, C.E. Goutis** "Server Side Hashing Core Exceeding 3 Gbps of Throughput", International Journal of Network Security (special issue), Vol. 1, Nos. 1/2/3, pp. 43–53, 2007.

Αναφορές από:

1. Jingcheng Gao, Jing Liu, Bharat Rajan, Rahul Nori, Bo Fu, Yang Xiao, Wei Liang and C. L. Philip Chen, "SCADA communication and security issues", in Security and Communication Networks, John Wiley & Sons, Ltd, Volume 7, Issue 1, pp. 175–194, January 2014 (10.1002/sec.698)

2. Yang Xiao, Ke Meng and Daisuke Takahashi, "Accountability using flow-net: design, implementation, and performance evaluation", in Security and Communication Networks, Special Issue: Focus on Security and privacy in emerging information technologies, John Wiley & Sons, Ltd, Volume 5, Issue 1, pp. 29–49, January 2012. (doi: 10.1002/sec.348)

3. Alina Olteanu, Yang Xiao, Jing Liu, Thomas M. Chen, "Studying Non-intrusive Tracing in the Internet", in Proc of Quality, Reliability, Security and Robustness in Heterogeneous Networks, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Volume 74, 2012, pp 58-74.

4. Yang Xiao, Songqing Yue, Bo Fu and Suat Ozdemir, "GlobalView: building global view with log files in a distributed/networked system for accountability", in Security and Communication Networks, John Wiley & Sons, Ltd, online version, Sep. 2011 (10.1002/sec.374)

5. Yanping Zhang, Yang Xiao, Kaveh Ghaboosi, Jingyuan Zhang and Hongmei Deng, "A survey of cyber crimes", Security and Communication Networks, John Wiley & Sons, Ltd, Volume 5, Issue 4, pp. 422–437, Apr. 2011 (10.1002/sec.331)

6. Zhifeng Xiao and Yang Xiao, "Accountable MapReduce in Cloud Computing", .in Proc. of the The First International Workshop on Security in Computers, Networking and Communications, pp. 1099-1104, 2011.

7. Yang Xiao, Daisuke Takahashi, Jing Liu, Hongmei Deng, Jingyuan Zhang, "Wireless telemedicine and m-health: technologies, applications and research issues", International Journal of Sensor Networks, Vol. 10, N. 4/2011, pp. 202-236, 2011 (doi: 10.1504/IJSNET.2011.042770).

8. Yang Xiao; Ke Meng; Takahashi, D., "Implementation and evaluation of accountability using flow-net in wireless networks," MILITARY COMMUNICATIONS CONFERENCE,

2010 - MILCOM 2010 , vol., no., pp.7,12, Oct. 31 2010-Nov. 3 2010 (doi: 10.1109/MILCOM.2010.5680278)

Δ.9 **G. N. Selimis, A.P. Kakarountas, A. P. Fournaris, A. Milidonis and O.Koufopavlou**, "A Low Power Design for SBOX Cryptographic Primitive of Advanced Encryption Standard for Mobile End-Users", in Journal of Low Power Electronics, ASP, vol.3, no.3, pp. 327-336, 2007.

Αναφορές από:

1. Jia Hao Kong, Li-Minn Ang, and Kah Phooi Seng, "A Very Compact AES-SPIHT Selective Encryption Computer Architecture Design with Improved S-Box", in Journal of Engineering, Hindawi, Volume 2013 (2013), Article ID 785126, 26 pages, 2013 (DOI: 10.1155/2013/785126)

2. Ioanna Tsekoura, "Design exploration of application specific instruction set cryptographic processors for resources constrained systems", Master Thesis, University of Patras, Greece, 2010. See more at: http://nemertes.lis.upatras.gr/jspui/handle/10889/3905#sthash.lmVQDwaJ.dpuf"

3. (*) Selimis, G.; Fournaris, A; Kostopoulos, G.; Koufopavlou, O., "Software and Hardware Issues in Smart Card Technology," Communications Surveys & Tutorials, IEEE , vol.11, no.3, pp.143,152, 3rd Quarter 2009 (doi: 10.1109/SURV.2009.090310)

Δ.10 **H.E. Michail, A. P. Kakarountas, A. S. Milidonis and C. E. Goutis**, "A Top-Down Design Methodology for Implementing Ultra High-Speed Hashing Cores", IEEE Transactions on Dependable and Secure Computing, vol.6, is.4, pp.255-268, 2009

Αναφορές από:

1. Jae-woon Kim; Hu-ung Lee; Youjip Won, "Design for high throughput SHA-1 hash function on FPGA," Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on , vol., no., pp.403,404, 4-6 July 2012 (doi: 10.1109/ICUFN.2012.6261737)

2. (*) H.E. Michail,G.S. Athanasiou, G. Theodoridis, C.E. Goutis, "On the development of high-throughput and area-efficient multi-mode cryptographic hash designs in FPGAs", Integration, the VLSI Journal, Elsevier, Volume 47, Issue 4, pp. 387–407, 2014.

3. (*) George S. Athanasiou, Harris E. Michail, George Theodoridis, Costas E. Goutis, "High-performance FPGA implementations of the cryptographic hash function JH", IET Computers & Digital Techniques, Volume 7, Issue 1, pp. 29 – 40, 2013

4. (*) George S. Athanasiou, George Theodoridis, Costas E. Goutis, Harris E. Michail, T. Kasparis, "A SYSTEMATIC FLOW FOR DEVELOPING TOTALLY SELF-CHECKING ARCHITECTURES FOR SHA-1 AND SHA-2 CRYPTOGRAPHIC HASH FAMILIES", IET Computers & Digital Techniques, Volume 7, Issue 1, pp. 29 – 40, 2013

5. (*) George S. Athanasiou, Elias Tsigkas, Harris E. Michail, George Theodoridis, Costas E. Goutis, “Throughput/Area Trade-Offs of Loop-Unrolling, Functional, and Structural Pipeline for Skein Hash Function”, Computer Science & Engineering: An International Journal (CSEIJ), Vol. 3, No. 1, pp. 1 – 21, 2013

6. Shice Ni, Yong Dou, Kai Chen, Lin Deng, “Design and Implementation of Novel Flexible Crypto Coprocessor and Its Application in Security Protocol”, Communications in Computer and Information Science, Book Series: Computer Engineering and Technology, Springer, Volume 396, pp 61-72, 2013.

7. (*) Harris E. Michail, George S. Athanasiou, Vassilis Kelefouras, George Theodoridis, Costas E. Goutis, “On the exploitation of a high-throughput SHA-256 FPGA design for HMAC”, ACM Transactions on Reconfigurable Technology and Systems (TRETS), Volume 5 Issue 1, March 2012

8. Eun-Gu Jung, Daewan Han, Jeong-Gun Lee, “Low Area and High Speed SHA-1 Implementation”, ISOCC 2011 Conference, pp. 365-367, 2011.

9. A.G. Voyiatzis, K. G. Stefanidis, D.N. Serpanos, “Increasing lifetime of cryptographic keys on smartphone platforms with the controlled randomness protocol”, in Proc. of WESS '11 Proceedings of the Workshop on Embedded Systems Security, 2011.

10. Anh-Tuan HOANG, Katsuhiro YAMAZAKI, Shigeru OYANAGI, “Pipelining a Multi-Mode SHA-384/512 Core with High Area Performance Rate”, IEICE TRANSACTIONS on Information and Systems, Vol.E92-D, No.10, pp.2034-2042, 2009.

Δ.11 **M. Papadonikolakis, A.P. Kakarountas, C.E. Goutis**, “Efficient High-Performance Implementation of JPEG-LS Encoder”, in Journal of Real-Time Processing, Springer. vol. 3, no. 4, pp 303-310, 2008.

Αναφορές από:

Δ.12 **A. Milidonis, V. Porpodas, N. Alachiotis, A. P. Kakarountas, H. Michail, G. Panagiotakopoulos and C. E. Goutis**, “Low Power Architecture with Scratch-Pad Memory for Accelerating Embedded Applications with Run Time Reuse”, IET Computers & Digital Techniques, IET, vol. 3, is. 1, pp.109-123, 2009.

Αναφορές από:

Δ.13 **D.M. Schinianakis, A.P. Fournaris, A.P. Kakarountas and T. Stouraitis**, “An RNS Architecture of an Fp Elliptic Curve Point Multiplier”, IEEE Transactions on Circuits and Systems I, vol.56, no.6, pp. 1202-1213, June 2009.

Αναφορές από:

1. S. Sharifi, M. Esmaeildoust, M. Taheri, and K. Navi, “Efficient Implementation of RNS Montgomery Multiplication Using Balanced RNS Bases”, in Journal of mathematics and computer science, Nonlinear Analysis Group, Volume 12, Issue 1, pp. 51–64, Aug 2014

Δ.14 **A.P. Kakarountas, H.E. Michail, C.E. Goutis, A.M. Rjoub**, “High-Throughput Implementation of RipeMD-160”, International Journal for Internet Technology and Secured Transactions, Inderscience Ltd, vol. 1, no. 3/4, pp. 309 – 316, 2009.

Αναφορές από:

Δ.15 **A. Milidonis, N. Alachiotis, V. Porpodas, H. Michail, G. Panagiotakopoulos, A.P. Kakarountas, C.E. Goutis**, “Decoupled Processors Architecture for Accelerating Data Intensive Applications using Scratch-Pad Memory Hierarchy”, Journal of Signal Processing Systems. Springer Science + Business Media, LLC, vol. 59, no.3, pp. 281-296, 2010.

Αναφορές από:

Δ.16 **H.E. Michail, A.P. Kakarountas, D. Schinianakis, G. Selimis, C.E. Goutis**, “Cipher Block based Authentication Module: A Hardware Design Perspective”, Journal of Circuits, Systems and Computers, World Scientific Publishing, Vol. 20, No. 2, pp. 163-184, 2011.

Αναφορές από:

Υπάρχουν επίσης πολλές και για τα υπόλοιπα περιοδικά, όμως στέλνω αυτή την έκδοση προς αποφυγή της καταληκτικής ημερομηνίας που δόθηκε.

(*) αναφορά από συν-συγγραφέα

Άλλες Αναφορές (σε Βιβλία, Διπλώματα Ευρεσιτεχνίας, Συνέδρια, κλπ)

(ενδεικτικά)

1. M. Favalli, C. Metra, “*Problems due to open faults in the interconnections of self-checking data paths*”, in Proc. of Design, Automation & Test in Europe (DATE’02), Paris, France, pp. 205-211, March 2002.

2. Stefan G. Block, David R. Rueveni, "*Logic built-in self test (BIST)*", United States Patent 6904554
3. L. Sekanina, "*Evolution of Polymorphic Self-Checking Circuits,*" in *Evolvable Systems: From Biology to Hardware*, Springer Berlin / Heidelberg, p. 186-197, ISBN 978-3-540-74625-6.
4. L. Sekanina, "*Design and Analysis of a New Self-Testing Adder Which Utilizes Polymorphic Gates,*" in Proc of 2007 IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems (DDECS 2007), Gliwice, Poland. pp. 243-246, 2007.
5. Y. Rajasree, Y. Vishnu Priya, N. R. Alamelu, "Self Checking and Fault Tolerant Digital Design", in International Journal of Information Technology and Knowledge Management, Vol. 2, No. 2, pp. 283-288, 2009.
6. D. Marienfeld, E. S. Sogomonyan, V. Otcheretnij and M. Gossel, "*A New Self-Checking and Code-Disjoint Non-Restoring Array Divider*", in Proc. of the 12th IEEE international Symposium on on-Line Testing, pp. 23-25, July, 2006.
7. D. Marienfeld, E.S. Sogomonyan, V. Ocheretnij, and M. Gossel, "*New Self-checking Output-Duplicated Booth Multiplier with High Fault Coverage for Soft Errors*", in Proc of 14th Asian Test Symposium, pp. 76-81, December, 2005.
8. D. Roberts, T. Austin, D. Blauww and T. Mudge, "*Error Analysis for the Support of Robust Voltage Scaling*", in Proc of International Symposium on Quality Electronic Design (ISQED'05), pp. 65-70, March, 2005.
9. D. Marienfeld, E.S. Sogomonyan, V. Ocheretnij and M. Gossel, "*A New Self-Checking Multiplier by Use of a Code-Disjoint Sum-Bit Duplicated Adder*", in Proc of the Ninth IEEE European Test Symposium, (ETS'04), pp. 30-35, Vol. 00, May, 2004.
10. L.D. HUNG, M. TAKADA, Y. GE, and S. SAKAI, "A Cost-effective Technique to Mitigate Soft Errors in Logic Circuits", TECHNICAL REPORT OF IEICE. 2004.
11. Yannick Monnet. Etude et modelisation de circuits resistants aux attaques non intrusives par injection de fautes. PhD Thesis, Institut National Polytechnique de Grenoble, France, 2007.
12. C. Bolchini, L. Pomante, F. Salice, and D. Sciuto, "*The design of reliable devices for mission-critical applications*", in IEEE Transactions on Instrumentation and Measurement, Vol. 52, Iss. 6, pp. 1703- 1712, December 2003.
13. E. Brockmeyer, M. Miranda, F. Catthoor, and H. Corporaal, "*Layer Assignment Techniques for Low Energy in Multi-Layered Memory Organisations*", in Proc. of Design, Automation & Test in Europe (DATE'03), Germany, pp. 1-6, 2003.
14. D. Soudris, G. Theodoridis, K. Katis, A. Thanailakis, and C.E. Goutis, "*Structure and Techniques of the Low-Power Design Flow*", IC&D Report of LPGD Project, July, 2000.
15. N.D. Zervas, M. Perakis, D. Soudris, E.G. Metaxakis, A. Tzimas, G.A. Kalivas, C.E. Goutis, "*Low-Power Design of Direct Conversion Baseband DECT Receiver*", in IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, Vol. 48, Iss. 12, pp.1121-1131, December 2001.
16. M. Jayapala, F. Barat, P. Op de Beeck, F. Catthoor, G. Deconick, "*Loop Cache (Buffer) Organization: Energy Analysis and Partitioning*", Technical Report K.U.Leuven/ESAT, Jan 22, 2002.
17. M. Jayapala, F. Barat, P. Op de Beeck, F. Cathoor and R. Lawereins, "*Low Energy Clustered Instruction Fetch and Split A Loop Cache Architecture For Long instruction Word Processors*", Workshop on Compilers and Operating Systems for Low Power COLP'01, held in conjunction with PACT'01, Barcelona, Spain, September, 2001.
18. B. Geelen, V. Ferentinos, F. Catthoor, G. Lafruit, D. Verkest, R. Lauwereins, and T. Stouraitis, "*Modeling and exploiting spatial locality trade-offs in wavelet-based applications under varying resource requirements*", in ACM Transactions on Embedded Computing Systems (TECS), Vol. 9, Is. 3 pp. 1-26, Feb. 2010.
19. Bert Geelen. Low-Power, Wavelet-based Applications in Dynamic Environments. PhD Thesis, Katholieke Universiteit Leuven, Belgium, December 2008.

20. B. Geelen, V. Ferentinos, F. Catthoor, S. Toulatos, G. Lafruit, T. Stouraitis, R. Lauwereins, D. Verkest, "*Exploiting Varying Resource Requirements in Wavelet-based Applications in Dynamic Execution Environments*", in Journal of Signal Processing Systems for Signal, Image, and Video Technology (formerly the Journal of VLSI Signal Processing Systems for Signal, Image, and Video Technology). Springer Science + Business Media, LLC, 2008.
21. I. Issenin, N. Dutt, "*Using FORAY Models to Enable MPSoC Memory Optimizations*," in International Journal of Parallel Programming, Springer Science+Business Media, LLC, pp. vol. 36, no. 1, 93-113, Feb. 2008. (DOI: 10.1007/s10766-007-0041-6).
22. Ilya Michailovich Issenin. Multiprocessor System-on-Chip Data Memory Customization for Embedded Array-Intensive Applications, PhD Dissertation, UNIVERSITY OF CALIFORNIA, IRVINE, 2007.
23. E. Brockmeyer, B. Durinck, H. Corporaal, and F. Catthoor, Chapter 7 "Layer Assignment Techniques for Low Energy in Multi-Layered Memory Organizations, in *Designing Embedded Processors*, Springer, Netherlands, pp.157-190, July 2007.
24. S. Yoo, A. Bouchhima, W. Cesario, A. Jerraya, L. Gauthier, Chapter 11 "*Low-Power SoC with Power-Aware Operating Systems Generation*", in Low-Power Processors and Systems on Chip, CRC Francis & Taylor, 2006, ISBN: 0-8493-6700-X
25. B. Geelen, A. Ferentinos, F. Catthoor, A. Vandecappelle, G. Lafruit, T. Stouraitis, R. Lauwereins, and D. Verkest, "*Software-controlled scratchpad mapping strategies for wavelet-based applications*". In: IEEE 2006 Workshop on Signal Processing Systems (SiPS 2006). pp.365-370; (2-4 October 2006; Banff, Canada.)
26. B. Geelen, G. Lafruit, V. Ferentinos, R. Lauwereins and D. Verkest, "*Memory Hierarchy Energy Cost of a Direct Filtering Implementation of the Wavelet Transform*", in Proc of IEEE 2005 International Workshop on Power And Timing Modeling, Optimization and Simulation (PATMOS'05), Leuven, Belgium, pp. 107-116, Sep. 2005.
27. M. Miranda, E. Brockmeyer, T. van Meeuwen, C. Ghez, and F. Catthoor, Chapter 12 "Low-Power Data Storage and Communication for SoC", in *Low-Power Processors and Systems on Chips*, CRC Press, pp.12.1-12.19, 2005.
28. B. Geelen, E. Brockmeyer, G. Lafruit, R. Lauwereins, D. Verkest, "*Exploration of system-level trade-offs for application mapping in multiprocessor system-on-chips*", in Proc of Research in Microelectronics and Electronics, 2005 PhD, pp. 222-225, July, 2005.
29. Low-Power Electronics Design, Chapter 29, Eds. Laurie Kelly, Christian Piguet, CRC Press, 2004, ISBN 0849319412.
30. A. Papanikolaou, M. Miranda, and F. Catthoor, "*Overcoming the 'Memory Wall' by improved system design exploration and a link to process technology options*", in Proceedings of the 1st Conference on Computing Frontiers (CF'04), Ischia, Italy, April, 2004.
31. Edgar Armando Catalan Salgado, Alpha- Beta Simple Associative Memories , PhD Dissertation, Instituto Politecnico Nacional, CENTRO DE INVESTIGACIÓN EN COMPUTACIÓN, Mexico, July 2006.
32. M. en C. Maria Elena Acevedo Mosqueda, Alpha- Beta Bidirectional Associative Memories , PhD Dissertation, Instituto Politecnico Nacional, CENTRO DE INVESTIGACIÓN EN COMPUTACIÓN, Mexico, July 2006.
33. Y. Lu, G. Shou, Y. Hu, Z. Guo, "*The Research and Efficient FPGA Implementation of Ghash Core for GMAC*", in Proc. of International Conference on E-Business and Information System Security (EBISS '09), Wuhan, pp. 1-5, May 23-24 May 2009.
34. Chhailadeep Kaur. Message Authentication Code (MAC) Technique for Providing Message Integrity in e-Governance. Master Thesis, Computer Science, Punjabi University, Patiala, India. 2008.

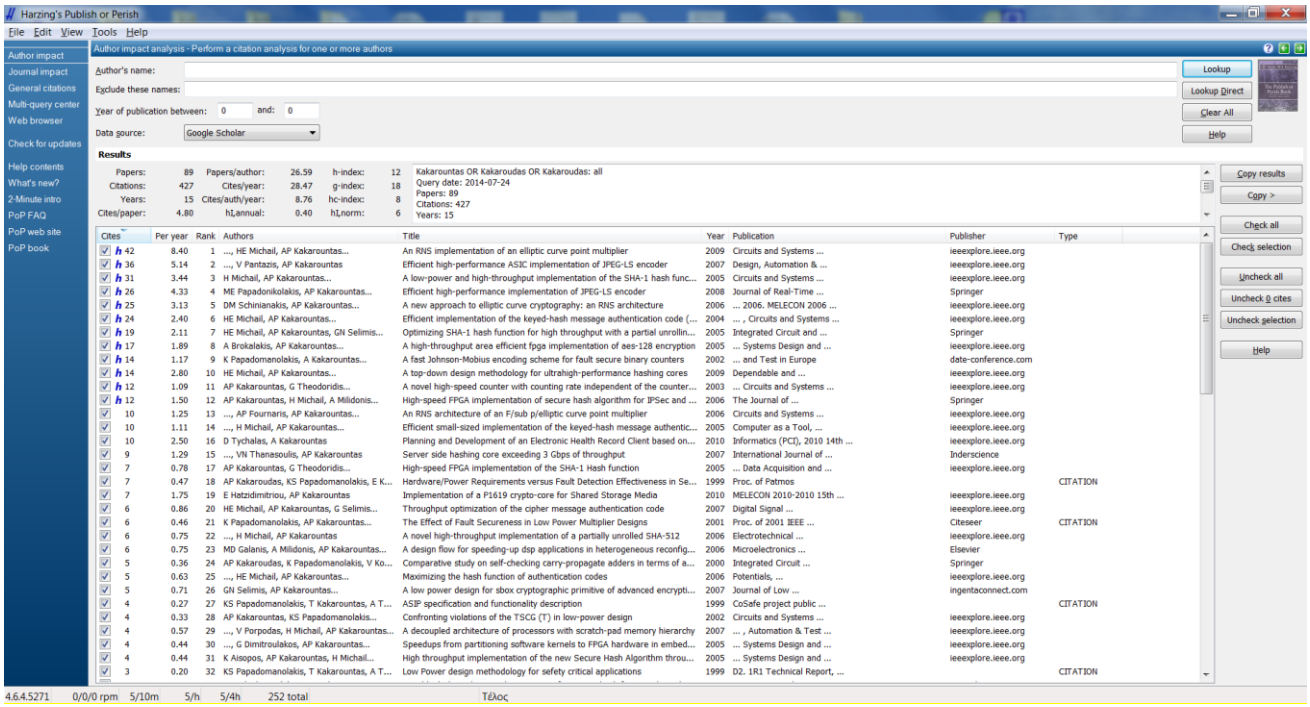
35. N. Wang, J. Chen, Y. Huang, and T. Chan, "*IPSec-based key management in mobile IP networks*", in Proc. of the 12th WSEAS international Conference on Communications, Heraklion, Greece, pp. 190-195, 23-25 July 2008.
36. Tzu-wei Chan. An IPSec-Based Security Algorithm for Mobile IP Networks. Department and Graduate Institute of Information and Communication Engineering. 2005-08-28. http://ethesys.lib.cyut.edu.tw/ETD-db/ETD-browse/browse?first_letter=C .
37. N.-C. Wang, J.-S. Chen, Y.-F. Huang, T.-W. Chan, "*An IPSec-Based Key Management Algorithm for Mobile IP Networks*", WSEAS Transactions on Communications, Vol. 7, Is. 8, pp. 892-901 , 2008.
38. M. Kim, J. Ryou, S. Jun, "*Compact Implementation of SHA-1 Hash Function for Mobile Trusted Module*" in Proc. of the 9th International Workshop in Information Security Applications (WISA'08), Jeju Island, Korea, pp. 292-304, September 23-25, 2008.
39. M. Kim, J. Ryou, "*Power Efficient Hardware Architecture of SHA-1 Algorithm for Trusted Mobile Computing,*" in Proc of the 9th International Conference (ICICS 2007), Zhengzhou, China, pp. 375-385, December 12-15, 2007.
40. Mooseop Kim, Youngse Kim, Jaecheol Ryou, and Sungik Jun, "*Efficient Implementation of the Keyed-Hash Message Authentication Code Based on SHA-1 Algorithm for Mobile Trusted Computing,*", in Proc. of 2007 ATC, Hong Kong, China, July 11-13, pp. 410-419, Publishers: Springer-Verlag Berlin Heidelberg 2007.
41. I. Pooters, "*An Approach to full User Data Integrity Protection in UMTS Access Networks*", 4th Twente Student Conference on IT , Enschede, The Netherlands, January 2006.
42. E. Khan, M.W. El-Kharashi, F. Gebali, M. Abd-El-Barr, "*A reconfigurable hardware unit for the HMAC algorithm*", in Proc of ITI 3rd International Conference on Information and Communications Technology, pp. 861-874, December 2005.
43. N.-C. Wang and Z.-W. Chan, "*An IPSec-Based Key Management Algorithm for Mobile IP Networks*", in Proc of the 2005 Symposium on Digital Life and Internet Technologies (DLAIT'2005), Tainan, Taiwan, ROC, 3D-5, June 2-3, 2005.
44. Esam Ali Hasan Khan. Design and Performance Analysis of a Reconfigurable, Unified HMAC-Hash Unit for IPSec Authentication. PhD Dissertation, University of Victoria, 2005.
45. Yong Ki Lee, Miroslav Knezevic, and Ingrid M.R. Verbauwhede, "*Chapter 5: Hardware Design for Hash Functions*", in Secure Integrated Circuits and Systems, Springer Science+Business Media, pp. 79-104, 2010. ISBN: 978-0-387-71827-9.
46. Han Lin, Han Jun, Zeng Yang, Huang Wei, "*Security processor used in RSA / SHA encryption unit design reuse*", Journal of Wuhan University: Natural Science, vol. 54 No. 05, pp. 615–618, 2008.
47. M. Zeghid, B. Bouallegue, M. Machhou, A. Baganne, R. Tourki, "*Architectural design features of a programmable high throughput reconfigurable SHA-2 processor*", in Journal of Information Assurance and Security, Dynamic Publishers, Vol. 2, pp. 147-158 , 2008.
48. GUO Wen-ping, LIU Zheng-lin, CHEN Yi-cheng, ZOU Xue-cheng, "*A High Throughput and Low-Power Implementation of the SHA-1 Hash Function*", Microelectronics and Computer, vol 25, no 5, pp. 76–79, 2008.
49. Jingtao Sun, Qiuyu Zhang, Zhanting Yuan, Wenhan Huang, Xiaowen Yan and Jianshe Dong, "*Research of Spam Filtering System Based on LSA and SHA*", in Proc of the 5th International Symposium on Neural Networks (ISNN 2008), pp. 331-340, Beijing, China, September 24-28, 2008. Proc Part II (Lecture Notes in Computer Science 5264/2008, ISBN 978-3-540-87733-2, DOI: 10.1007/978-3-540-87734-9_38).
50. Changyao Chen, Xiufen Fu, Shaohua Teng, Peijiang Liu, Baixing Chen, "*A cooperative browser-level web caching system based on chord*", in Proc of the 12th International

Conference on Computer Supported Cooperative Work in Design (CSCWD 2008), pp. 93 – 97, 16-18 April 2008.
51. Y. K. Lee, H. Chan and I. Verbauwhede, "*Design Methodology for Throughput Optimum Architectures of Hash Algorithms of the MD4-class*," in Journal of Signal Processing Systems for Signal, Image, and Video Technology (formerly the Journal of VLSI Signal Processing Systems for Signal, Image, and Video Technology). Springer Science + Business Media, LLC, vol. 53, pp. 89-102, 2008.
52. SUN Nan-nan, HAN Yin-he, XU Du, "*An implementation of SHA-1 algorithm based on unrolling loops architecture,*" in INFORMATION TECHNOLOGY, vol.31, no.3, pp.29-31, 2007.
53. GU Ye-hua, ZENG Xiao-yang, HAN Jun, ZHANG Zhang, "*A High-performance and Low-cost VLSI Implementation of the SHA-1 Hash Function,*" in JOURNAL OF CHINESE COMPUTER SYSTEMS, vol.28, no.5, pp.940-943, 2007.
54. Y. Gu, X. Zeng, J. Han, J. Zhao, "*A Low-cost and High-performance SoC Design for OMA DRM2 Applications,*", in Proc. of the 2007 IEEE International Symposium on Circuits and Systems (ISCAS'07), New Orleans, USA, pp. 3510-3513, 27-30 May 2007.
55. Y.K. Lee, H. Chan and I. Verbauwhede, "*Iteration Bound Analysis and Throughput Optimum Architecture of SHA-256 (384,512) for Hardware Implementations*," in Proc. of the 8th International Workshop in Information Security Applications (WISA'07), August 17-19, 2007.
56. M. Zeghida, B. Bouallegue, A. Baganne, M. Machhout, R. Tourki, "*A Reconfigurable Implementation of the New Secure Hash Algorithm,*" The Second International Conference on Availability, Reliability and Security (ARES 2007), pp. 281-285, 2007.
57. Y. K., Lee, H., Chan and I. Verbauwhede, "*Throughput Optimized SHA-1 Architecture Using Unfolding Transformation*", in Proceedings of the IEEE 17th international Conference on Application-Specific Systems, Architectures and Processors (ASAP'06) - Volume 00, pp. 354-359, September 2006.
58. I. Pooters, "*An Approach to full User Data Integrity Protection in UMTS Access Networks*", 4th Twente Student Conference on IT , Enschede, The Netherlands, January 2006.
59. M. Juliato, C. Gebotys, R. Elbaz, "*Efficient fault tolerant SHA-2 hash functions for space applications*", in Proc of IEEE Aerospace Conference (AERO 2009), pp.1-16, March 2009.
60. R. Chaves, G. Kuzmanov, L. Sousa, S. Vassiliadis, "*Cost-Efficient SHA Hardware Accelerators*", in IEEE Transactions on Very Large Scale Integration (VLSI) Systems. IEEE, vol. 16, is. 8, pp: 999 – 1008, Aug. 2008.
61. M. Kim, J. Ryou, S. Jun, "*Compact Implementation of SHA-1 Hash Function for Mobile Trusted Module*" in Proc. of the 9th International Workshop in Information Security Applications (WISA'08), Jeju Island, Korea, pp. 292-304, September 23-25, 2008.
62. Ricardo Jorge FERNANDES CHAVES. Secure Computing on Reconfigurable Systems. PhD Thesis, Technische Universiteit Delft, The Netherlands, December 2007.
63. M. Kim, J. Ryou, "*Power Efficient Hardware Architecture of SHA-1 Algorithm for Trusted Mobile Computing,*" in Proc of the 9th International Conference (ICICS 2007), Zhengzhou, China, pp. 375-385, December 12-15, 2007.
64. Mooseop Kim, Youngse Kim, Jaecheol Ryou, and Sungik Jun, "*Efficient Implementation of the Keyed-Hash Message Authentication Code Based on SHA-1 Algorithm for Mobile Trusted Computing,*", in Proc. of 2007 ATC, Hong Kong, China, July 11-13, pp. 410-419, Publishers: Springer-Verlag Berlin Heidelberg 2007.
65. R. Chaves, G. Kuzmanov, L. Sousa and S. Vassiliadis, "*Improving SHA-2 Hardware Implementations*", in Proc. of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2006), Yokohama, Japan, October, pp. 298–310, 2006.

66. Y. Choi, M. Kim, T. Kim, H. Kim, "*Low power implementation of SHA-1 algorithm for RFID system*", in Proc. of 2006 IEEE Tenth International Symposium on Consumer Electronics (ISCE'06), pp 1-5, 2006.
67. Zeghid Medien, et al., "*Design and Hardware Implementation of QoSS-AES Processor for Multimedia applications*", in TRANSACTIONS ON DATA PRIVACY, Vol. 3, pp. 43—64, 2010.
68. Kimmo Jarvinen. Studies on High-Speed Hardware Implementation of Cryptographic Algorithms, PhD Dissertation, Helsinki University of Technology, May 2008.
69. WU Peng, LI Kai-cheng, "*Research on implementation of Rijndael Algorithm based on FPGA,*" in RAILWAY COMPUTER APPLICATION, vol.16, no.3, pp.46-48, 2007.
70. James S. Grabowski, Amr Youssef, "*An FPGA implementation of AES with support for counter and feedback modes*", in Proc. of the International Conference on Microelectronics (ICM 2007), Cairo, Egypt, pp. 39 – 42, 29-31 Dec. 2007.
71. WANG Youren, WANG Li, YAO Rui, ZHANG Zhai, CUI Jiang, "*Dynamically Reconfigurable Encryption System of the AES*", WUHAN UNIVERSITY JOURNAL OF NATURAL SCIENCES, vol.11, no.6, pp.1569-1572, 2006.
72. Li Wang, Youren Wang, Rui Yao, and Zhai Zhang, "*Hardware Implementation of AES Based on Genetic Algorithm,*", in L. Jiao et al. (Eds.): ICNC 2006, Part II, LNCS 4222, pp. 904 – 907, 2006.
73. W. Jigang, T. Srikanthan, G. Chen, "*Algorithmic Aspects of Hardware/Software Partitioning: 1D Search Algorithms*", in IEEE Transactions on Computers, Vol. 59, No.4, pp. 532-544, Apr. 2010.
74. W. Jigang, T. Srikanthan, T. Jiao, "*Algorithmic aspects for functional partitioning and scheduling in hardware/software co-design*", in Design Automation for Embedded Systems, Springer Netherlands, vol. 12, no. 4, pp. 345-375, 2008.
75. S.-S. Ang, G. A. Constantinides, W. Luk, P. Y. K. Cheung, "*Custom parallel caching schemes for hardware-accelerated image compression*," in Journal of Real-Time Image Processing. Springer Science + Business Media, LLC, vol. 3, pp. 289-302, 2008.
76. W. Jigang, T. Srikanthan, G. Chen, "*One-dimensional Search Algorithms for Hardware/Software Partitioning,*" in 5th IEEE/ACM International Conference on Formal Methods and Models for Codesign (MEMOCODE 2007), pp. 149-158, 2007.
77. Y. Wang, Q. Zhao, L. Jiang, and Yi Shao, "Ultra High Throughput Implementations for MD5 Hash Algorithm on FPGA", in Proc. of Second International Conference, HPCA 2009, Shanghai, China, pp. 433-441, 10-12 Aug. 2009.
78. H.A. Tuan, K. Yamazaki, S. Oyanagi, "*Multi-stage Pipelining MD5 Implementations on FPGA with Data Forwarding*", in IPSJ Online Transactions, Information Processing Socity in Japan (IPSJ), Vol. 2, pp. 15-26, Jan. 2009.
79. P. Kitsos, Chapter 17 "System-on-Chip Design of the Whirlpool Hash Function", in *Handbook of Research on Wireless Security*, Eds. Yan Zhang, Jun Zheng, Miao Ma, Idea Group Inc (IGI), 2008, pp 256-270. ISBN:159904899X
80. A. P. Fournaris, O. Koufopavlou, Chapter 4 "Hardware Design Issues in Elliptic Curve Cryptography for Wireless Systems", in *Wireless Security and Cryptography*, Eds N. Sklavos, X. Zhang, CRC Press, 2007, ISBN 0-8493-8771-X.
81. Ralf Laue, Sorin A. Huss, "*Parallel Memory Architecture for Elliptic Curve Cryptography over GF(p) Aimed at Efficient FPGA Implementation*," in Journal of Signal Processing Systems for Signal, Image, and Video Technology (formerly the Journal of VLSI Signal Processing Systems for Signal, Image, and Video Technology), Springer Science + Business Media, LLC, vol. 51, pp. 39-55, 2007. DOI: 10.1007/s11265-007-0135-9.
82. Alexander Skavantzos, Mohammad Abdallah, Thanos Stouraitis, "Large Dynamic Range RNS Systems and their Residue to Binary Converters", in Journal of Circuits, Systems, and Computers (JCSC), World Scientific Publishers, vol. 16, no. 2, pp. 267-286, April 2007.

83. Przemyslaw Zalewski. FPGA design and performance analysis of SHA-512, Whirlpool and PHASH hashing functions. Master Thesis, Computer Engineering, Rochester Institute of Technology, Rochester, New York, USA. May 2008.
84. M. Zeghida, B. Bouallegue, A. Baganne, M. Machhout, R. Tourki, "*A Reconfigurable Implementation of the New Secure Hash Algorithm,*" The Second International Conference on Availability, Reliability and Security (ARES 2007), pp. 281-285, 2007.
85. Robert Szerwinski. Efficient Cryptography on Graphics Hardware. Diploma Thesis, Department of Electrical Engineering & Information Sciences, Ruhr-University Bochum, Germany. February 15th, 2008.
86. Rooju Gnyanesh Chokshi. Residue Number System Enhancements for Programmable Processors. Master Thesis, Arizona State University, U.S.A. December 2008.
87. J. Chu, M. Benaissa, "*GF(2m) multiplier using Polynomial Residue Number System*", in Proc of IEEE Asia Pacific Conference on Circuits and Systems (APCCAS 2008), pp.1514-1517, Nov. 30 2008-Dec. 3 2008.
88. Robert Szerwinski, Tim Guneysu, "*Exploiting the Power of GPUs for Asymmetric Cryptography*", in Proc of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2008), Washington, DC, USA, August 10-13, pp. 79-99, 2008.
89. P.V. Ananda Mohan, "*New reverse converters for the moduli set* $\{2^{n-3},2^{n-1},2^{n+1},2^{n+3}\}$", in AEU - International Journal of Electronics and Communications, In Press, Available online 21 December 2007.
90. Hakim Khali, Ahcene Farah, "Cost-Effective Implementations of GF(p) Elliptic Curve Cryptography Computations", in International Journal of Computer Science and Network Security (IJCSNS), vol.7, no.8, pp. 29-37, August 2007.
91. S. Bandyopadhyay, T.H. Feng, H.D. Patel, E.A. Lee, "A Scratchpad Memory Allocation Scheme for Dataflow Models", Technical Report No. UCB/EECS-2008-104, Electrical Engineering and Computer Sciences, University of California at Berkeley.
92. Giorgos Nikiforos, "*FPGA implementation of a Cache Controller with Configurable Scratchpad Space*", Institute of Computer Science (ICS), Foundation for Research and Technology – Hellas (FORTH), Technical Report FORTH-ICS/TR-402, Jan. 2010.
93. Z. Xiaoyu, C. Xinkai, Li Xiaowen, J. Hanjun, Z. Chun, W. Zhihua, "Key Optimization Techniques in JPEG-LS IP Core Design", in Journal of Electronics (China), Springer, vol.27, no.1 pp. 94-98, Jan. 2010.
94. A. Benoit, H. Kosch, V. Rehn-Sonigo, and Y. Robert, "Multi-Criteria Scheduling of Pipeline Workflows (and Application To the JPEG Encoder)", in International Journal of High Performance Computing Applications, Vol. 23, Is. 2, pp. 171-187, May 2009.
95. Rehn Sonigo. Multi-criteria Mapping and Scheduling of Workflow Applications onto Heterogeneous Platforms. PhD Thesis, Université de Lyon, France, July 2009.
96. X. Chen, X. Zhang, L. Zhang, X. Li, N. Qi, H. Jiang, Z. Wang, "*A Wireless Capsule Endoscope System With Low-Power Controlling and Processing ASIC*", in IEEE Transactions on Biomedical Circuits and Systems, vol.3, no.1, pp.11-22, Feb. 2009.
97. XU Yan-ling, LIU Bei, "*Dynamic Rate Control Scheme for JPEG-LS Image Compression*", in Journal of Computer Engineering, Vol. 34, No. 7, pp 238-239, April 2008.
98. X. Chen, X. Zhang, L. Zhang, N. Qi, H. Jiang, Z. Wang, "*A wireless capsule endoscopic system with a low-power controlling and processing ASIC*", in Proc of IEEE Asian Solid-State Circuits Conference (A-SSCC 2008), pp.321-324, 3-5 Nov. 2008.
99. Anne Benoit, Harald Kosch, Veronika Rehn-Sonigo, and Yves Robert "*Bi-criteria Pipeline Mappings for Parallel Image Processing*", in Proc of the 8th International Conference of Computational Science (ICCS 2008), pp. 215-225, Kraków, Poland, June 23-25, 2008.
100. Yu-yu Lee. A High-Speed Lossless/Lossy Embedded Image Compression Codec with Rate Control Mechanism for High-End LCD Applications. Master Thesis, National Central University, China. 2008.

101. Lee Yu-yu. A High-Speed Lossless/Lossy Embedded Image Compression Codec with Rate Control Mechanism for High-End LCD Applications. Master Thesis, National Central University, Taiwan (R.O.C.), 2007.
102. Anne Benoit, Harald Kosch, Veronika Rehn-Sonigo, Yves Robert, "Bi-criteria Pipeline Mappings for Parallel Image Processing", Raporte de Recherche, ISSN 0249-6399 ISRN INRIA/RR--6410--FR+ENG.
103. Raymond Sbrusch. Authenticated Messaging in Wireless Sensor Networks Used for Surveillance. Master Thesis, The University of Houston-Clear Lake, Texas, USA, 2008.
104. R. Sbrusch, T.A. Yang, Chapter 20 "Message Authentication in Surveillance Networks", in *Security in RFID and Sensor Networks*, Eds. Yan Zhang and Paris Kitsos, CRC Press, pp. 419-443.
105. Ronald L. Rivest, "The MD6 hash function - A proposal to NIST for SHA-3", Report – Submission package for MD6 for the NIST SHA-3 hash function competition. Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology (MIT). April 16, 2009
106. David S. H. Rosenthal, "*Bit Preservation: A Solved Problem?*", in Proc of iPRES2008, London, UK, September 2008
107. Ryuji Hada, Kazuya Tanigawa, Tetsuo Hironaka, "*A back-end compiler with fast compilation for VLIW based dynamic reconfigurable processor*", WSEAS Transactions on Computers archive, Vol. 7, Is. 9, pp. 1515-1524 , 2008.
108. Y.-K. Chen, S. Y. Kung, "Trend and Challenge on System-on-a-Chip Designs", in Journal of VLSI Signal Processing, Springer Science + Business Media, LLC, vol. 53, pp. 217-229, 2008. DOI: 10.1007/s11265-007-0129-7
109. Ammar Aljer. Co-design et Raffinement en B: BHDL Tool, plateforme pour la conception de composante numériques. Université des Sciences and Technologies de Lille. 21 Dec. 2004.



ΧΙΙΙ. ΑΛΛΑ ΣΤΟΙΧΕΙΑ

Κατά την συνεργασία του Δρ. Κακαρούντα με το **Τμήμα Πληροφορικής με Εφαρμογές στη**

Βιοϊατρική, Πανεπιστήμιο Θεσσαλίας, πραγματοποιήθηκαν πολλές δράσεις με τον διττό στόχο της προβολής και της εξωστρέφειας του Τμήματος προς την αγορά εργασίας και τον ακαδημαϊκό χώρο.

Ημερίδες:

- Στις 27-28 Φεβρουαρίου 2013, πραγματοποιήθηκε η πέμπτη επιστημονική δι-ημερίδα του Student Branch του Τμήματος, με τίτλο «Biomedical Engineering: trends, Research and Technologies».
- Στις 21-22 Μαρτίου 2012, πραγματοποιήθηκε η τέταρτη επιστημονική δι-ημερίδα του Student Branch του Τμήματος, με τίτλο «Ελεύθερο ή Ανοικτό; Λογισμικό ή Υλικό; Όταν η δημιουργία περνάει από τα χέρια μας».
- Στις 7 Απριλίου 2011, πραγματοποιήθηκε η τρίτη επιστημονική ημερίδα του Student Branch του Τμήματος, με τίτλο «Ενσωματωμένα Συστήματα υπολογιστών και εφαρμογές στη Βιοϊατρική».
- Στις 22 Απριλίου 2010, πραγματοποιήθηκε η δεύτερη επιστημονική ημερίδα του Student Branch του Τμήματος, με τίτλο «Τηλεϊατρική και Νέες Προοπτικές».
- Στις 19 Μαρτίου 2009, πραγματοποιήθηκε ημερίδα ενημέρωσης για το Corallia.
- Στις 19 Μαρτίου 2009, πραγματοποιήθηκε η πρώτη επιστημονική ημερίδα του Student Branch του Τμήματος, με τίτλο «Πληροφοριακά Συστήματα Υγείας».

Προσκλήσεις για διαλέξεις:

- Πρόσκληση και διάλεξη του Δρ. Βασίλειου Κόκκινου με τίτλο «Engineering in Presurgical Evaluation for Epilepsy Surgery», στις 19 Νοεμβρίου 2010, στο Τμήμα Πληροφορικής με Εφαρμογές στη Βιοϊατρική,
- Διοργάνωση ARM seminar-workshop στο Τμήμα, με προσκεκλημένο από την ARM Ltd (Joe Bungo, ARM Senior Application Engineer), στις 8 Σεπτεμβρίου 2009.

Αναγνωρίσεις - Συνεργασίες:

- Βραβείο «IEEE Outstanding Branch Counselor and Advisor Award Recognition Program» 2012, ως University of Central Greece IEEE Student Branch Counselor
- Exemplary Student Branch για το University of Central Greece - IEEE Student Branch για 3 συναπτά έτη (2011, 2012, 2013).
- Επιλογή φοιτητών μας από το Corallia Cluster για συμμετοχή στο US Education Trip με πλήρη χρηματοδότηση του ταξιδιού τους.
- Συμμετοχή του IEEE Student Branch στη διοργάνωση του Athens Job Fair και την εθελοντική υποστήριξη του Athens Digital Week για την επίτευξη της εξωστρέφειας του Τμήματος.

Εργασίες όπου εμφανίζεται το Affiliation του Τμήματος:

Δ16, Ε46, Ε47, Ε51

Κατά την συνεργασία του Δρ. Κακαρούντα με τα τμήματα **Εφαρμογών Πληροφορικής στη Διοίκηση και στην Οικονομία (ΕΠΔΟ) και το Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών (ΤΠΤ) του ΤΕΙ Ιονίων Νήσων**, πραγματοποιήθηκαν πολλές δράσεις με

τον διττό στόχο της προβολής και της εξωστρέφειας του Παραρτήματος Λευκάδας προς την αγορά εργασίας και τον ακαδημαϊκό χώρο, καθώς και την οργάνωση των Τμημάτων του Παραρτήματος Λευκάδας προκειμένου να λειτουργούν εύρυθμα και σύμφωνα με το ν. 4009/2011.

Ημερίδες:

- Διοργάνωση του 1ου Open Coffee στα Ιόνια Νησιά, Λευκάδα (05/04/2012).
- Διοργάνωση εκδηλώσεων για την 5η Παγόσμια Εβδομάδα Επιχειρηματικότητας, με συνεδρίες τεχνολογικές και ομιλίες για την καινοτομία (GEW 2012).
- Διοργάνωση εκδηλώσεων για την 4η Παγόσμια Εβδομάδα Επιχειρηματικότητας, με συνεδρίες τεχνολογικές και ομιλίες για την καινοτομία (GEW 2011).

Διδακτικό και Διοικητικό έργο:

Λόγω περιορισμένων πόρων του Ιδρύματος για πρόσληψη έκτακτου εκπαιδευτικού προσωπικού, η μέση απασχόληση [για τα Ακ. Έτη 2011-2012 (εαρ. Εξάμηνο) και 2012-2013] για διδασκαλία ανέρχονταν στις **26 ώρες/εβδομάδα** (παρά την συμβατική υποχρέωση για 7 ώρες – μειωμένη στο 50% λόγω ανάθεσης χρεών προϊσταμένου Τμήματος). Συνολικά η μέση απασχόληση σε διδακτικό και διοικητικό έργο ξεπερνούσε τις **50 ώρες/εβδομάδα**.

Πραγματοποίηση 1ης Εσωτερικής Αξιολόγησης για το ΕΠΔΟ, σύμφωνα με τα πρότυπα της ΑΔΙΠ. Συμμετοχή σε όλες τις Επιτροπές και σε όσους Διαγωνισμούς αφορούν το Παράρτημα Λευκάδας. Σύνταξη οργανογράμματος και ανάθεση εργασιών σε ομάδες εργασίας. Δημιουργία άτυπων εργαστηρίων ανά θεματική ενότητα και οργάνωση των πρώτων ερευνητικών ομάδων. Αναβάθμιση συστήματος σε Ηλεκτρονική Γραμματεία (Μητρώο), επαναλειτουργία βιβλιοθήκης, αναβάθμιση συστήματος e-class, σχεδίαση νέας σελίδας τμήματος (δεν ολοκληρώθηκε λόγω Σχεδίου Αθηνά). Τα αποτελέσματα της οργάνωσης που περιγράφηκε, άρχισαν να φαίνονται το 2014, οπότε και ανακοινώθηκαν οι πρώτες δημοσιεύσεις των ερευνητικών ομάδων (βλ. δημοσιεύσεις).

Επιπλέον συμμετείχε ενεργά στις διαδικασίες για την μεταφορά της Φοιτητικής Λέσχης και στην αναζήτηση νέας έδρας για το Παράρτημα Λευκάδας (έχουν ήδη ξεκινήσει οι εργασίες για το νέο κτίριο – παραχώρηση χρήσης από το Δήμο Λευκάδας).

Από τον Μάιο 2013, με Προεδρικό Διάταγμα (Π.Δ. 103/2013) αποφασίστηκε η μετακίνηση του ΤΠΤ στο ΤΕΙ Ηπείρου (Άρτα) και η συγχώνευση του ΕΠΔΟ, με το Τμήμα Διοίκησης Επιχειρήσεων (Ληξούρι) και η δημιουργία νέου Τμήματος Διοίκησης Επιχειρήσεων με έδρα την Λευκάδα. Από τον Μάιο 2013 έως τον Σεπτέμβριο 2013 ολοκληρώθηκε όλη η διαδικασία μετακίνησης φοιτητών στο ΤΕΙ Ηπείρου και η παράδοση-παραλαβή της διοίκησης προκειμένου να λειτουργήσει το νέο Τμήμα.

Εργασίες όπου εμφανίζεται το Affiliation του Τμήματος:

E45, E48, E49, E50, E52, E53, E54

Κατά την θητεία του Δρ. Κακαρούντα στην προεδρεία του **IEEE Consumer Electronics Society – Greece Chapter**, πραγματοποιήθηκαν δράσεις προβολής του IEEE και του CE Society, καθώς και στην δικτύωση των μελών στην Ελλάδα.

Ημερίδες – Προσκλήσεις για ομιλία:

- Ομιλία της Ι. Καρύδη (MBA), με τίτλο « Total Quality in Consumer Electronics Production» στις 16/12/2013, στο ΤΕΙ Ιονίων Νήσων, Λευκάδα.
- Ομιλία του Δρ. Αθ. Κακαρούντα, με τίτλο «Open Hardware + Arduino workshop » στις

12/06/2013, στο ΤΕΙ Ιονίων Νήσων, Λευκάδα.

- Ομιλία του Δρ. Αθ. Κακαρούντα, με τίτλο «Consumer Electronics - a market worth discovering» στις 16/12/2012, στο κτίριο Innohub, Πάτρα.
- Διοργάνωση του 2ου εργαστηριακού κύκλου στα Ενσωματωμένα Συστήματα (συν-διοργάνωση IEEE Consumer Electronics Society – Greece Chapter και Τ.Ε.Ι. Ιονίων Νήσων) στις 29/03/2012.
- Ομιλία της Nikis Lambropoulos (MBA), με τίτλο « Management of Innovation as the only mean for development in times of crisis» στις 18/05/2012, στο κτίριο Β του Πανεπιστημίου Πατρών.
- Διοργάνωση του 1ου εργαστηριακού κύκλου στα Ενσωματωμένα Συστήματα (συν-διοργάνωση IEEE Consumer Electronics Society – Greece Chapter και Τ.Ε.Ι. Ιονίων Νήσων) στις 30/11/2011.
- Ομιλία του IEEE Distinguished Lecturer Tomas Coughlin, με τίτλο «Consumer Digital Storage—Personal, Shared, Hierarchical and Virtual» στις 12/09/2011, στο κτίριο του Corallia Cluster, Αθήνα.