

ΣΥΝΤΟΜΟ ΒΙΟΓΡΑΦΙΚΟ



Ο Νικόλαος Μπάρδης είναι Αναπληρωτής Καθηγητής Πληροφορικής και Διευθυντής του Εργαστηρίου Πληροφορικής του Τομέα Μαθηματικών και Επιστημών Μηχανικού του Τμήματος Στρατιωτικής Επιστήμης του Ανώτατου Στρατιωτικού Εκπαιδευτικού Ιδρύματος της Στρατιωτικής Σχολής Ευελπίδων. Αποφοίτησε από το Τμήμα Υπολογιστικών Μηχανημάτων, Διανοητικών Συστημάτων και Δικτύων του Εθνικού Τεχνικού Πανεπιστημίου της Ουκρανίας "Κίεβ Polytechnic Institute" ως Μηχανικός Η/Υ και Πληροφορικής με άριστα το 1995 και το 2000 του απενεμήθη ο τίτλος του Διδάκτορα Τεχνικών Επιστημών.

Έχει συνεργαστεί με τη Γενική Διεύθυνση Αμυντικής Βιομηχανίας Έρευνας και Τεχνολογίας του Υπουργείου Εθνικής Άμυνας, την Εθνική Υπηρεσία Πληροφοριών, το Υπουργείο Εσωτερικών Δημόσιας Διοίκησης και Αποκέντρωσης, το Υπουργείο Εργασίας, Κοινωνικής Ασφάλισης και Πρόνοιας, το Ινστιτούτο Εργασίας, το Εργαστήριο Δικτυακών Εφαρμογών και Πολυμέσων του ΕΚΕΦΕ ΔΗΜΟΚΡΙΤΟΣ. Έχει διδάξει ως εντεταλμένος καθηγητής Πληροφορικής στη Σχολή Ναυτικών Δοκίμων, στη Σχολή Ικάρων, στο Τμήμα Αυτοματισμού του ΤΕΙ Χαλκίδας, ΤΕΙ Αθήνας. Έχει δώσει σειρά διαλέξεων και έχει συνεργαστεί ως ερευνητής σε θέματα κρυπτογραφίας σε Πανεπιστήμια και ερευνητικά κέντρα του εξωτερικού καθώς και σε διεθνή επιστημονικά συνέδρια Στρατιωτικών Επικοινωνιών και Στρατιωτικών εφαρμογών όπως στο MILITARY COMMUNICATION της IEEE. Τα επιστημονικά του ενδιαφέροντα και οι ερευνητικές του δραστηριότητες επικεντρώνονται στα πεδία της κρυπτογραφίας, κρυπτανάλυσης, ασφάλειας των πληροφοριών, κώδικες, πληροφοριακό πόλεμο, στην ανάπτυξη συστήματος C4ISR και στις Στρατιωτικές Εφαρμογές.

Είναι μέλος του Τεχνικού Επιμελητηρίου Ελλάδος (ΤΕΕ), μέλος Technical Program Committee (TPC) του Communication Society της IEEE και μέλος της WSEAS. Το συγγραφικό του έργο σε θέματα κρυπτογραφίας ξεπερνάει τις εξήντα δημοσιεύσεις σε έγκυρα επιστημονικά περιοδικά και συνέδρια.

Προσωπικά στοιχεία

ΝΙΚΟΣ ΜΠΑΡΔΗΣ

Αναπληρωτής Καθηγητής Πληροφορικής με έμφαση τις Στρατιωτικές Εφαρμογές

Διευθυντής Εργαστηρίου Πληροφορικής

Μέλος ΔΕΠ - ΦΕΚ Γ 1210 - 23/12/2010.

E-mail : bardis@ilabsse.gr

URL : www.sse.gr

Εκπαιδευτικό έργο

«Επιστήμη των Η/Υ στις Ένοπλες Δυνάμεις» - 1^ο εξάμηνο Θεωρία.

«Βασικές Αρχές Προγραμματισμού - Αλγόριθμοι και Γλώσσες Προγραμματισμού» - 2^ο εξάμηνο - Θεωρία

«Κυβερνοπολέμος - Κρυπτογραφία και Ασφάλεια Πληροφοριών» - 7^ο εξάμηνο

«Κυβερνοπόλεμος – Πληροφοριακός Πόλεμος και C4I συστήματα» 8^ο εξάμηνο

Σημειώσεις για την διδασκαλία μαθημάτων

«ΕΠΙΣΤΗΜΗ ΤΩΝ Η/Υ με Στρατιωτικές Εφαρμογές»

«Βασικές Αρχές Προγραμματισμού - Αλγόριθμοι και Γλώσσες Προγραμματισμού με Στρατιωτικές Εφαρμογές»

«Βασικές Αρχές στην Ασφάλεια Πληροφοριών & Κρυπτογραφία – Ανάλυση και Σχεδίαση Πληροφοριακών Συστημάτων»

Ερευνητικά ενδιαφέροντα

Οι γνωστικές περιοχές ενδιαφέροντος και έρευνας με τις οποίες ασχολήθηκε ο Νίκος Μπάρδης καλύπτουν κυρίως περιοχές της ασφάλειας πληροφοριών και κρυπτογραφίας με εφαρμογές. Η ερευνητική του δραστηριότητα αναπτύσσεται στις περιοχές της Κρυπτογραφίας Πληροφοριών, Κρυπτανάλυσης Πληροφοριών, Ασφάλεια Πληροφοριών, Ασφάλειας και έλεγχος μετάδοσης δεδομένων σε τηλεπικοινωνιακά κανάλια υψηλών ταχυτήτων, εξόρυξη με την γρήγορη εύρεση πληροφοριών σε σταθερές βάσεις δεδομένων και αποθήκευση πληροφοριών, συστήματα Τεχνητής Νοημοσύνης (Νευρωνικά Δίκτυα, Ασαφής Λογική, Γενετικοί Αλγόριθμοι). Τα αποτελέσματα των παραπάνω ερευνών χρησιμοποιούνται για την ανάπτυξη κρυπτογραφικών συστημάτων, συστημάτων C4I, συστημάτων Λήψης Αποφάσεων και Έγκαιρης Προειδοποίησης.

Πιο συγκεκριμένα:

- Ανάλυση και Σύνθεση συναρτήσεων που περιέχονται στους μετασχηματισμούς των κρυπτογραφικών αλγόριθμων. Στόχος είναι η αύξηση της αποδοτικότητας των κρυπτογραφικών μετασχηματισμών, σύμφωνα με το κριτήριο της απόκτησης του μεγαλύτερου δυνατού βαθμού ασφάλειας, έχοντας ως δεδομένο την αρχιτεκτονική δομή των υπολογιστικών μέσων, τα οποία χρησιμοποιούνται στον κρυπτογραφικό αλγόριθμο.
- Επεξεργασία σύγχρονων μεθόδων για την απόκτηση συναρτήσεων κρυπτογραφικών μετασχηματισμών, οι οποίες εξασφαλίζουν υψηλό βαθμό ασφάλειας καθώς και την αποδοτική χρησιμοποίηση των μονάδων του Η/Υ.
- Επεξεργασία λογισμικού στις γλώσσες Assembly, Turbo Pascal, C++, κ.α., για την αποδοτικότερη χρησιμοποίηση των κρυπτογραφικών αλγόριθμων.
- Επεξεργασία αποδοτικότερων υπολογιστικών μέσων και ειδικών κρυπτοεπεξεργαστών (Hardware), για την γρήγορη λειτουργία των κρυπτογραφικών αλγόριθμων ασφάλειας πληροφοριών. Χρησιμοποιείται η VHDL-τεχνολογία.
- Επεξεργασία αλγόριθμων και ειδικών υλικών μέσων (Hardware) για γεννήτριες ψευδοτυχαίων και τυχαίων δυαδικών ακολουθιών.
- Επεξεργασία κυλιόμενων καταχωρητών με μη γραμμική ανάδραση (Non Linear Feedback Registers), στους οποίους αυξάνεται εκθετικά ο αριθμός των απλών πολυωνύμων σε σχέση με τους γραμμικούς κυλιόμενων καταχωρητές (Linear Feedback Registers). Τα απλά πολυώνυμα εξασφαλίζουν την μέγιστη μη περιοδικότητα των καταχωρητών.
- Σχεδίαση κωδικών για σύγχρονα συστήματα επικοινωνιών
- Σχεδίαση πρωτοκόλλων αυθεντικοποίησης χρηστών και συστημάτων.
- Επεξεργασία αποδοτικών αλγόριθμων Perfect Hash Functions, οι οποίοι εξασφαλίζουν την εύρεση πληροφορίας, σε στατικές και δυναμικές Βάσεις Δεδομένων, με μια μόνο αναζήτηση στην μνήμη (Data Wherehousing) .

- Τεχνολογίες Πληροφορικής και Τεχνητής Νοημοσύνης σε εφαρμογές στα οπτικά συστήματα (Νευρωνικά Δίκτυα, Ασαφής Λογική, Γενετικοί Αλγόριθμοι, Συστήματα Γνώσης & Έμπειρα Συστήματα)

Ερευνητικό έργο

Οι μελέτες και οι έρευνα που διεξήγαγε ο Νίκος Μπάρδης είναι προσανατολισμένα σε θέματα αξιολόγησης κρυπτογραφικών αλγορίθμων, σύνθεσης και τροποποίησης κρυπτογραφικών αλγορίθμων, ανάπτυξης συστημάτων κρυπτανάλυσης και ανάπτυξης συστημάτων αυθεντικοποίησης χρηστών σε συστήματα ασφαλείας. Μέρος των αδιαβάθμητων αποτελεσμάτων της ερευνητικής δραστηριότητας είναι: η αντικειμενική αξιολόγηση του βαθμού ασφαλείας και τροποποίηση του νέου Διεθνούς κρυπτογραφικού πρότυπου AES, η ανάπτυξη μεθοδολογίας για την καθολική κρυπτανάλυση αλγορίθμων υλοποιημένη σε υλικό επίπεδο, ο σχεδιασμός αυτόνομων ανεξάρτητων συναρτησιακών μετασχηματισμών κρυπτογραφικών αλγορίθμων με υψηλό επίπεδο ασφάλειας με τις απαιτήσεις των Ενόπλων Δυνάμεων, σχεδιασμός συστημάτων αυθεντικοποίησης, ανάπτυξη κωδίκων σε συστήματα επικοινωνιών, σχεδιασμός και ανάπτυξη συστημάτων αναζήτησης πληροφοριών σε σταθερές βάσεις δεδομένων.

ΣΥΜΜΕΤΟΧΗ ΣΕ ΕΠΙΤΡΟΠΕΣ, ΟΜΑΔΕΣ ΕΡΓΑΣΙΑΣ ΚΑΙ ΘΕΣΕΙΣ ΔΙΟΙΚΗΣΗΣ

- Αναπληρωματικό μέλος της Επιτροπής Ασφάλειας Ολυμπιακών Αγώνων εκ μέρους του Υπουργείου Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης
- Επιστημονικός Συνεργάτης σε ομάδες εργασίας σε θέματα πληροφορικής του Υπουργείου Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης
- Μέλος της ομάδας εργασίας της Γενικής Διεύθυνσης Αμυντικής Βιομηχανίας Έρευνας και Τεχνολογίας
- Μέλος ομάδας εργασίας του Εθνικού Τεχνικού Πανεπιστημίου της Ουκρανίας
- Μέλος ομάδας εργασίας του Τεχνικού Επιμελητηρίου Ελλάδας
- Μέλος της επιτροπής του Υπουργείου Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης στο ευρωπαϊκό πρόγραμμα «Κοινωνία της Πληροφορίας»
- Μέλος ομάδας εργασίας του Υπουργείου Εργασίας, Κοινωνικής Ασφάλισης και Πρόνοιας, Γενική Γραμματεία Πρόνοιας

ΔΙΑΛΕΞΕΙΣ ΣΕ ΠΑΝΕΠΙΣΤΗΜΙΑ - ΑΝΑΓΝΩΡΙΣΗ ΤΟΥ ΕΠΙΣΤΗΜΟΝΙΚΟΥ ΚΑΙ ΑΛΛΟΥ ΕΡΓΟΥ

Ο Δρ. Νικόλαος Μπάρδης προσκλήθηκε να έχει δώσει διαλέξεις και να παρουσιάσει καινοτόμες τεχνολογίες σε θέματα Ασφάλειας Πληροφοριών, κρυπτογραφίας σε εφαρμογές σε Στρατιωτικές Εφαρμογές, στο Τραπεζικό Σύστημα κ.α. από τα παρακάτω πανεπιστήμια:

1. TECHNICAL UNIVERSITY OF SOFIA στο FACULTY AUTOMATION – DEPARTMENT THEORY OF ELECTRICAL ENGINEERING τον Οκτώβριο του 2005 στην Σόφια της Βουλγαρίας
2. UNIVERSITY POLITEHNICA OF BUCHAREST – UPB τον Οκτώβριο του 2006 στο Βουκουρέστι της Ρουμανίας
3. CHINA JILIANG UNIVERSITY τον Μάιο του 2008 στο Hangzhou της Κίνας
4. IV. JAVAKHISHVILI TBILISI STATE UNIVERSITY, GEORGIA, 2010

Στο ερευνητικό έργο του Δρ. Νικόλαου Μπάρδη έχουν γίνει περισσότερες από 80 αναφορές από ερευνητές σε επιστημονικά συνέδρια, επιστημονικά περιοδικά, βιβλία, έντυπα με σταθερή περιοδικότητα έκδοσης κατά την τελευταία πενταετία.

Δημοσιευμένο έργο

ΒΙΒΛΙΑ

«Measurement and control in street lighting», C. Cepisca, N.G. Bardis. ELECTRA publication 2011

ΑΝΑΚΟΙΝΩΣΕΙΣ ΣΕ ΕΘΝΙΚΑ ΣΥΝΕΔΡΙΑ ΜΕ ΚΡΙΤΕΣ

1. **Νικόλαος Μπάρδης**, «Ο Ρόλος των Καινοτόμων Τεχνολογιών στις Ένοπλες Δυνάμεις», 3^η Διημερίδα «ΟΙ ΕΝΟΠΛΕΣ ΔΥΝΑΜΕΙΣ ΣΤΟΝ 21^ο ΑΙΩΝΑ», ΑΝΩΤΑΤΗ ΔΙΑΚΛΑΔΙΚΗ ΣΧΟΛΗ ΠΟΛΕΜΟΥ, ΘΕΣΣΑΛΟΝΙΚΗ 15-16 ΦΕΒΡΟΥΑΡΙΟΥ 2006.
2. **Νικόλαος Μπάρδης**, «Ο Αξιωματικός του 21 αιώνα», Διημερίδα ΣΣΕ, 2008
3. **Νικόλαος Μπάρδης**, «Modern Cryptanalysis and Cryptography. The Weapons of the Information Warfare» («Σύγχρονη Κρυπτανάλυση και Κρυπτογραφία. Τα Όπλα του Πληροφοριακού Πολέμου»), Επιστημονική Διημερίδα ΣΣΕ, «ΕΦΑΡΜΟΓΕΣ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗ ΣΤΡΑΤΙΩΤΙΚΗ ΕΠΙΣΤΗΜΗ», 11 - 12 Απριλίου 2011, Αμφιθέατρο ΑΛΕΞΑΝΔΡΟΣ ΞΗΡΟΣ, ΣΤΡΑΤΙΩΤΙΚΗ ΣΧΟΛΗ ΕΥΕΛΠΙΔΩΝ (ΣΣΕ)
4. **Νικόλαος Μπάρδης**, «Issues in Theoretical and Applied Cryptography in Military Applications», ΕΠΙΣΤΗΜΟΝΙΚΟ ΣΥΝΕΔΡΙΟ, Κρυπτογραφία και Εφαρμογές στις Ένοπλες Δυνάμεις, ΣΣΕ, Παρασκευή 6 Απριλίου 2012
5. **Νικόλαος Μπάρδης**, «Fast identification schemes based on Galois fields arithmetic for Military Applications», Διεθνές συνέδριο στη Σχολή με θέμα «Εφαρμογές Μαθηματικών και Πληροφορικής στη Στρατιωτική Επιστήμη», 11-12 Απριλίου 2013

Διοργάνωση Ειδικών Συνεδρίων

1. **Nikos Bardis**, Special session II: "Advanced techniques and simulations for defense application", MAMECTIS'08 Proceedings of the 10th WSEAS international conference on Mathematical methods, computational techniques and intelligent systems, 2008
2. **Nikos Bardis**, Special Session, "Advanced Techniques and Simulations for Defense Applications", the 14th WSEAS International Conference on COMMUNICATIONS, (part of the 14th WSEAS CSCC Multiconference), Corfu Island, Greece, July 23-25, 2010
3. **Nikos Bardis**, Special Session, "Advanced Techniques and Simulations for Defense Applications", 11th WSEAS International Conference on APPLICATIONS OF COMPUTER ENGINEERING (ACE '12), Vouliagmeni, Athens, Greece, March 7-9, 2012
4. **Nikos Baardis**, Special Session, "Advanced Techniques and Simulations for Defense Applications", 16th WSEAS International Conference on COMMUNICATIONS (part of CSCC '12), Kos Island, Greece, July 15-17, 2012.

ΔΙΕΘΝΗ ΣΥΝΕΔΡΙΑ ΜΕ ΚΡΙΤΕΣ

1. **Nikolaos Bardis**, Oleksandr Markovskiy. *Fast Implementation zero knowledge identification schemes using the Galois fields arithmetic*, BIHTEL 2012, IX International Symposium on Telecommunications, Sarajevo, Bosnia and Herzegovina, IEEE IEEE Catalog Number: CFP122U-USB, ISBN: 978-1-4673-4874-4
2. Christos K. Volos, **N.G. Bardis**, Ioannis M. Kyprianidis and Ioannis, N. Stouboulos, *Implementation of Mobile Robot by Using Double-Scroll Chaotic Attractors*, Recent Researches in Applications of Electrical and Computer Engineering, Proceedings of the 11th International Conference on Applications of Electrical and Computer Engineering, World Scientific and Engineering Academy and Society (WSEAS) Stevens Point, Wisconsin, USA ©2012, ISBN: 978-1-61804-074-9, 2012, pp 119-124.
3. George P. Alexandris, **Nikolaos G. Bardis**, *A penetration strategy in a competitive environment*, ACA'12 Proceedings of the 11th International conference on Applications of Electrical and Computer Engineering, World Scientific and Engineering Academy and Society (WSEAS) Stevens Point, Wisconsin, USA ©2012, ISBN: 978-1-61804-074-9, Pages 132-136
4. **Bardis, N.G.**; Doukas, N.; Markovskiy, O.P., *Burst error correction using binary multiplication without carry*, MILITARY COMMUNICATIONS CONFERENCE, 2011 – MILCOM- IEEE 2011, Baltimore 7-10 November, DOI: 10.1109/MILCOM.2011.6127681, Page(s): 305 – 309
5. Stavroulakis, P., Markovskiy, O.P., **Bardis, N.G.**, Doukas, N., *Efficient zero – Knowledge identification based on one way Boolean transformations*, GLOBECOM Communication Conference, Workshops (GC Wkshps), 2011 IEEE, Houston USA, 5-9 Dec. 2011
6. **Bardis, N.G.**, Doukas, N.; Markovskiy, O.P., *Double burst error correction method: Case of interference incidents during data transmission in wired channels*, Digital Ecosystems and Technologies Conference (DEST), 2011 Proceedings of the 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE-DEST 2011) Daejeon, Korea
7. **Nikolaos Bardis**, Nikolaos Doukas, Olexander Markovskiy, *"Efficient Burst Error Correction Method for Application in Low Frequency Channels and Data Storage Units"*, DSP/IEEE 2011 17th International Conference on Digital Signal Processing, 6-8 July 2011 Corfu, Greece.
8. **Bardis, N.G.**; Doukas, N.; Markovskiy, O.P.; *Organization of the polymorphic implementation of Rijndael on microcontrollers and smart cards*, MILITARY COMMUNICATIONS CONFERENCE, MILCOM-IEEE 2010, San Jose, CA, ISSN: 2155-7578, pp. 1783 – 1787, 2010.
9. **N.G.Bardis**, A.Drigas, A.P. Markovskyy and I.Vrettaros, *Accelerated Modular Multiplication Algorithm of Large Word Length Numbers with a Fixed Module*, Communications in Computer and Information Science 111, Knowledge Management, Information Systems, E-Learning, and Sustainability Research, Third World Summit on the Knowledge Society, WSKS 2010 Corfu, Greece, September 2010 Proceedings, Part I, Springer – Verlag Berlin Heidelberg, pp 573-581, 2010, DOI: 10.1007/978-3-642-16324-1_58
10. **N.G.Bardis**, A.Drigas, A.P. Markovskyy and I.Vrettaros, *Check Sum Optimization for Transmission and Storage of Digital Information*, Communications in Computer and Information Science 111, Knowledge Management, Information Systems, E-Learning, and Sustainability Research, Third World Summit on the Knowledge Society, WSKS 2010 Corfu, Greece, September 2010 Proceedings, Part I, Springer – Verlag

- Berlin Heidelberg, pp 582-590, 2010, DOI: 10.1007/978-3-642-16318-0_73
11. **Bardis, N.G.**; Doukas, N.; Markovskiy, O.P.; Drigas, A.; *Two level efficient user authentication scheme*, 4th IEEE International Conference on Digital Ecosystems and Technologies (DEST), Dubai, ISSN: 2150-4938, pp 470 – 474, 2010.
 12. **Nikolaos G. Bardis**, Oleksandr P. Markovskiy, Costin Cepisca, and Katerina Argiri, *Burst error control based on weighted checksum*, Proceeding ICCOM'10 Proceedings of the 14th WSEAS international conference on Communications, World Scientific and Engineering Academy and Society (WSEAS) Stevens Point, Wisconsin, USA ©2010, ISBN: 978-960-474-200-4
 13. **Nikolaos G. Bardis**, Athanasios Drigas and Oleksandr P. Markovskiy, *Performance Increase of Error Control Operation on Data Transmission*, 3rd International Conference on New Technologies, Mobility and Security, IEEE, IEEE COMMUNICATIONS SOCIETY, Egypt – Cairo, 20-23 December 2009.
 14. Costin Cepisca, **Nikolaos Bardis**, Nikolay Mihalkov, *Conditioning circuits for parametric transducers*, Proceedings of 5th International Conference on Metrology and Measurement Systems, METSIM 2009, Faculty of Electrical Engineering, Politechnica University of Bucharest, Romania, ISBN 978-606-8082-22-6, pp. 83-86, November 5-6, 2009.
 15. **Bardis N. G.**, Doukas, N., Markovskiy O.P, *Transmission Error Correction Based on the Weighted Checksum*, Proceedings of the APPLIED COMPUTING CONFERENCE 2009 (ACC '09), MATHEMATICAL METHODS AND APPLIED COMPUTING Volume II, Vouliagmeni, Athens, Greece, pp.758-763, September 28-30, 2009.
 16. Iosif Androulidakis, Vasilios Christou, **Nikolaos G. Bardis**, Ioannis Stilios, *Surveying users' practices regarding mobile phones' security features*, Electrical And Computer Engineering Series, Proceedings of the 3rd international conference on European computing conference table of contents, Tbilisi, Georgia, Pages: 25-30, Year of Publication: 2009, ISBN ~ ISSN:1790-5117 , 978-960-474-088-8, [Online], Available: <http://portal.acm.org/citation.cfm?id=1627964>.
 17. **N. G. Bardis**, A. P. Markovskiy, N. Doukas, N. V. Karadimas, *True random number generation based on environmental noise measurements for military applications*, Mathematics And Computers In Science And Engineering archive Proceedings of the 8th WSEAS international conference on Signal processing, robotics and automation, Cambridge, UK, Pages 68-73, 2009, ISBN ~ ISSN:1790-5117 , 978-960-474-054-3, [Online], Available: <http://portal.acm.org/citation.cfm?id=1558930>
 18. Doukas Nikolaos, **Bardis Nikolaos**, *Effectiveness data transmission error detection using check sum control for military application*, A Series Of Reference Books And Textbooks archive Proceedings of the 10th WSEAS international conference on Mathematical methods, computational techniques and intelligent systems, Corfu, Greece, ISBN ~ ISSN:1790-2769 , 978-960-474-012-3, 2008, pp 498-502, [Online]. Available: <http://portal.acm.org/citation.cfm?id=1562421&dl=GUIDE&coll=GUIDE>.
 19. **Nikolaos G. Bardis**, Konstantinos Ntaikos, *Design of a secure chat application based on AES cryptographic algorithm and key management*, MAMECTIS'08 Proceedings of the 10th WSEAS international conference on Mathematical methods, computational techniques and intelligent systems,

- World Scientific and Engineering Academy and Society (WSEAS) Stevens Point, Wisconsin, USA ©2008, ISBN: 978-960-474-012-3, Pages 486-491.
20. N Doukas, K Ntaikos and **N. Bardis**: Integrated Information Life-Cycle, Data Management and Secret Key Lifecycle Management for Military Applications 10th WSEAS Int. Conf. On Mathematical Methods, Computational Techniques And Intelligent Systems 2008.
 21. **Bardis N.G**, Markovskyy A.P, "Utilization of Avalanche Transformation for Increasing of Echoplex and Checksum Data Transmission Control Reliability", ISITA 2004 - INTERNATIONAL SYMPOSIUM ON INFORMATION THEORY AND ITS APPLICATIONS, IEEE / SITA, Parma, Italy, October 10-13, ISBN: 4-902087-08-1, 2004
 22. **N.G.Bardis**, M.Mitrouli, A.P.Markovskyy, "Some properties of Boolean functions and design of Cryptographically strong balanced Boolean functions" , International Conference on RECENT ADVANCES IN STATISTICAL DESIGNS AND RELATED COMBINATORICS, University of Athens, July 7-9, 2003, Athens

ΠΕΡΙΟΔΙΚΑ ΜΕ ΚΡΙΤΕΣ

1. Bogdan MARIA, Mariana BUGA, Rares MEDIANU, Costin CEPISCA, **Nikolaos BARDIS**, *Obtaining a Model of Photovoltaic Cell with Optimized Quantum Efficiency*, Scientific Bulletin of the Electrical Engineering Faculty, ISSN 1843-6188, 2011 No. 2 (16)
2. **Bardis, N.G.**; Doukas, N.; Markovskyy, O.P., *Data Transmission Errors Detection in Amplitude-Phase Modulated Channels using the Residue Number System*, COMPUTERS and SIMULATION in MODERN SCIENCE Volume III, Published by WSEAS Press, ISBN: 978-960-474-256-1, pp.33-46, 2010.
3. **Nikolaos Bardis**, Nikolaos Doukas, Oleksandr P. Markovskyy, *Fast subscriber identification based on the zero knowledge principle for multimedia content distribution*, International Journal of Multimedia Intelligence and Security, Volume 1, Number 4, pp. 363 – 377, 2010.
4. Nikolaos Doukas, Athanasios Drigas and **Nikolaos G. Bardis**, *Design of an Interactive Game for Teaching War Ethics*, Technology Enhanced Learning. Quality of Teaching and Educational Reform Communications in Computer and Information Science, Springer – Verlag Berlin Heidelberg, Volume 73, 2010, 558-564, DOI: 10.1007/978-3-642-13166-0_78
5. **Bardis N.**, Drigas A., Doukas N., & Karadimas N., *Optimised Information System Reliability Techniques for Knowledge Society Acceptance*, Int. J. Knowledge and Learning, vol. 5, no. ¾, pp. 207-221, 2009.
6. Costin CEPIȘCĂ, Sorin Dan GRIGORESCU, Stergios GANATSIOS, **Nikolaos G. BARDIS**, *Passive and Active Compensations for Current Transformers*, METROLOGIE 4/2008 (p. 5-10)
7. Nikolaos G. Bardis, Nikolaos Doukas, Konstantinos Ntaikos, *Design and Development of a Secure Military Communication based on AES Prototype Crypto Algorithm and Advanced Key Management Scheme*, WSEAS TRANSACTIONS on INFORMATION SCIENCE & APPLICATIONS, Issue 10, Volume 5, October 2008, pages 1501-1510, ISSN: 1790-0832.
8. **Nikolaos Bardis**, Nikolaos Doukas, Konstantinos Ntaikos, *A new approach of secret key management lifecycle for military applications*, WSEAS

- Transactions on Computer Research, Volume 3 , Issue 5 (November 2008), Pages 294-304, ISSN:1991-8755, [Online], Available: <http://portal.acm.org/citation.cfm?id=1481940>
9. **Bardis Nikolaos**, *Coding of checksum components for increasing the control reliability of data transmission for military applications*, WSEAS TRANSACTIONS on COMMUNICATIONS, Issue 7, Volume 11, ISSN 1109-2742, November 2008, pp. 1122-1131, [Online]. Available: <http://portal.acm.org/citation.cfm?id=1481917>.
 10. N. Doukas, A. Drigas, **N.G. Bardis**, N.V. Karadimas. Accessible Secure Information Society Applications via the Use of Optimised Cryptographic Calculations. (2008) <http://citeseerx.ist.psu.edu/viewdoc/similar?doi=10.1.1.186.436>
 11. Costas Nastoulis, Apostolos Leros, **Nikolaos Bardis**, "Banknote Recognition Based on Probabilistic Neural Network Models", WSEAS TRANSACTIONS on SYSTEMS, Issue 10, Volume 5, ISSN 1109-2777, pp: 2363 – 2366 October 2006.
 12. Nikolaos V. Karadimas, George Rigopoulos, **Nikolaos Bardis**, "Coupling Multiagent Simulation and GIS – an Application in Waste Management", WSEAS TRANSACTIONS on SYSTEMS, Issue 10, Volume 5, ISSN 1109-2777, pp: 2367 – 2371 October 2006.
 13. **Bardis N.G**, Polymenopoulos A., Markovskyy A.P, M.Mitrouli, "Methods for Design of Balanced Boolean Functions Satisfying Strict Avalanche Criterion SAC", International Journal Computer Science 12(1), 2003.
 14. **Bardis N.G**, Bardis E.G., Markovskyy A.P., C.Economou, "Hardware Implementation of Data Transmission Control based on Boolean Transformation", WSEAS TRANSACTIONS on COMMUNICATIONS, Issue 7, Volume 4, ISSN 1109-2742, pp: 363 – 371, July 2005.
 15. **Bardis N.G** , "Echoplex Error Control System using Avalanche Transformations", WSEAS TRANSACTIONS on COMMUNICATIONS, Issue 2, Volume 3, ISSN 1109-2742, pp: 741 - 745, April 2004.
 16. **Bardis N.G** , "Combinatorial method for Boolean SAC functions designing", WSEAS TRANSACTIONS on COMMUNICATIONS, Issue 2, Volume 3, ISSN 1109-2742, pp: 746 - 752, April 2004.
 17. **Bardis N.G** , "Method of designing a controlled by code generator of Balanced Boolean functions which satisfy the SAC", WSEAS TRANSACTIONS on COMMUNICATIONS, Issue 2, Volume 3, ISSN 1109-2742, pp: 753 - 757, April 2004.
 18. **Bardis N.G**, Markovskyy A.P., Andrikou D.V., "Method for Design of pseudorandom binary sequences generators on nonlinear feedback shift register (NFSR)", WSEAS TRANSACTIONS on COMMUNICATIONS, Issue 2, Volume 3, ISSN 1109-2742, pp: 758 - 763, April 2004.
 19. **Bardis N.G**, Markovskyy A.P., Mitrouli M, Polymenopoulos A. , "Methods for design of balanced Boolean functions satisfying strict avalanche criterion (SAC)", WSEAS TRANSACTIONS on COMMUNICATIONS, Issue 2, Volume 3, ISSN 1109-2742, pp: 770 - 776, April 2004.
 20. **Bardis N.G**, Mitrouli M, Maris Th.I., Orlova M.N., "Some properties of Boolean functions and design of cryptographically strong balanced Boolean functions", WSEAS TRANSACTIONS on INFORMATION SCIENCE and APPLICATIONS, Issue 2, Volume 1, ISSN 1790-0832, pp: 717 - 723, August 2004.

21. **Bardis N.G.**, Polymenopoulos A., Bardis E.G, Markovskyy A.P, "Methods for Increasing the Efficiency of the Remote User Authentication in Integrated Systems", International Journal Computer Science 12(1), 2003.
22. **Bardis N.G.**, Leros A.P., Bardis E.G., Karadimas N., "Methods and Tools for Improving Efficiency of Symmetric Cryptographic Algorithms", WSEAS RECENT ADVANCES IN COMMUNICATIONS AND COMPUTER SCIENCE, ISSN 960-8052-86-6, 2003, pp: 155- 161.
23. **N.G.Bardis**, A.Polymenopoulos, E.G.Bardis, A.P.Markovskyy, D.V.Andrikou, "An approach to determine the complexity of random and pseudo random binary sequences", WSEAS TRANSACTIONS on COMMUNICATIONS, Issue 1, Volume 1, ISSN 1109-2742, 2002, pp: 37 - 42.
24. **Bardis N.G.**, Polymenopoulos A., Leros A.P., Karadimas N., Mastorakis N.E., "Topological methods for hash algorithms efficiency increase", WSEAS TRANSACTIONS on COMMUNICATIONS, Issue 1, Volume 1, ISSN 1109-2742, 2002, pp: 13 - 18.
25. **Bardis N.G.**, Polymenopoulos A., Bardis E.G., Markovskyy A.P., Mastorakis N.E. , "Hash Algorithms: a design for parallel calculations", WSEAS TRANSACTIONS on SYSTEMS, Issue 1, Volume 1, ISSN: 1109-2777, 2002, pp. 48 - 56.[Abstract, English, Greek] [Full paper, English]
26. Polymenopoulos A., **Bardis N.G.**, Bardis E.G., Markovskaja N.A., "Design and Implementation of Boolean Balanced Functions Satisfying Strict Avalanche Criterion (SAC)", WSEAS Press - Problem in Applied Mathematics and Computational Intelligence, ISBN: 960-8052-30-0, 2001, pp. 12-16.
27. Polymenopoulos A., Bardis E.G., **Bardis N.G.**, Markovskaja N.A., "Perfect Hashing Using Linear Boolean Functions", WSEAS Press - Problem in Applied Mathematics and Computational Intelligence, ISBN: 960-8052-30-0, 2001, pp. 5-11.
28. **Bardis N.**, Markovskyy A., El Xamy Igiad, Redko S., "Method and Structure for Forming and Calculate Systems of Orthogonal Balance Boolean Functions", Bulletin of National Technical University of Ukraine (KPI), ISSN 0201-744X, ISSN 0135-1729, UDK 681.322, No.32, 1999, pp. 90-98.
29. Bardis E., **Bardis N.**, Simonenko A., "The Algorithm for Dynamic Distributing of Processes in Real Time Distributed Computer Systems". Submitting as a special issue of IMACS/IEEE, CSCC'99 International MultiConference, "Recent Advances in Signal Processing and Communications", ISBN: 960-8052-03-3, pp. 166-169, 1999.
30. Bardis E.G., **Bardis N.G.**, Markovskyy A.P., Spyropoulos A.P., "Design of Boolean Function from a Great Number of Variables Satisfying Strict Avalanche Criterion". Submitting as a special issue of IMACS/IEEE CSCC'99 International MultiConference, "Recent Advances in Signal Processing and Communications", ISBN: 960-8052-03-3, pp. 107-112, 1999.
31. Bardis E.G., **Bardis N.G.**, Markovskyy A.P, Spyropoulos A.K, "Security Analysis of Cryptographic Algorithms by means of Boolean Functions". Submitting as a special issue of IMACS/IEEE CSCC'99 International MultiConference, " Progress in Simulation, Modeling, Analysis and Synthesis of Modern Electrical and Electronic Devices and Systems", ISBN: 960-8052-08-4, pp. 382-387, 1999.
32. Bardis E.G., **Bardis N.G.**, Markovskyy A.P., Spyropoulos A.K., "High Storage Utilization of Hash Memory by Reducing of Information Redundancy for Hashing". Submitting as a special issue of IMACS/IEEE CSCC'99 International MultiConference, "Software and Hardware Engineering for the 21th Century", ISBN: 960-8052-06-8, pp. 272-276, 1999.

33. **Bardis N.G.**, Markovskyy A.P., Abu Ysbax A.N, Kishenko A.B. "Analysis of Security of Cryptographic Algorithms Using Boolean Functions". Bulletin of National Technical University of Ukraine (KPI), ISSN 0201-744X,ISSN 0135-1729, UDK 681.322, No.31, 1998, pp.24-34.
34. **Bardis N.G.**, Markovskyy A.P., Gavaagiin U. "Method for Increasing the Effectiveness and the Information Security Level of a Data Base System, based in Hash-Memory". Bulletin of National Technical University of Ukraine (KPI), ISSN 0201-744X,ISSN 0135-1729, UDK 681.322.01, No.31, 1998, pp.14-23.
35. **Bardis N.G.**, Markovskyy A.P.,Samofalov K.G., Gavaagiin U. "Method for Design Balanced SAC-Functions for Security Informations Systems". Bulletin of National Technical University of Ukraine (KPI), ISSN 0201-744X,ISSN 0135-1729, UDK 681.322, No.31, 1998, pp.03-13.
36. Bardis E., **Bardis N.**, Markovskyy A., "An Approach for Decrease the Information Redundancy in Data Base". Publication on GPNTB-UKRAINE N 2163, 1994.
37. Bardis E., **Bardis N.**, "Effect of Memory Load Factor in Efficacy and in Authenticity of Hash-Functions". Publication on GPNTB-UKRAINE N 1965, 1994