Βιογραφικό Σημείωμα

28 Νοεμβρίου 2018

Προσωπικά Στοιχεία

Όνομα:	Γιάννης
Επώνυμο:	Σταματίου
Όνομα γονέων:	Κωνσταντίνος και Μαρία
Τρέχουσα θέση:	Καθηγητής, Τμήμα Διοίκησης Επιχειρήσεων, Πανεπιστήμιο Πάτρας και Σύμβουλος του Τομέα Ασφάλειας Πληροφοριακών Συστημάτων στο Ινστιτούτο Τεχνολογίας Υπολογιστών και Εκδόσεων - <<ΔΙΟΦΑΝΤΟΣ>>
Ημερομηνία γέννησης:	17 Ιανουαρίου 1968 στο Βόλο
Οικογενειακή κατάσταση:	Συζευγμένος με την Ευγενία Γεωργίου-Φωτεινής Θεοδοσοπούλου, με ένα παιδί
Διεύθυνση:	Πανεπιστήμιο Πάτρας, Τμήμα Διοίκησης Επιχειρήσεων, Ρίο, Πάτρα, 26504
Ηλεκτρονική διεύθυνση:	stamatiu@ceid.upatras.gr

Επαγγελματική κατάσταση

Από τον Ιανουάριο του 2011 έως και σήμερα υπηρετεί στο Πανεπιστήμιο Πάτρας, Τμήμα Διοίκησης Επιχειρήσεων, ως Καθηγητής. Πριν τη θέση αυτή, υπηρέτησε από το 2005 έως και τέλος του 2011 στο Πανεπιστήμιο Ιωαννίνων, Τμήμα Μαθηματικών, ως Επίκουρος Καθηγητής ενώ από 2003 έως και τέλος του 2004 είχε υπηρετήσει στο Πανεπιστήμιο Αιγαίου, Τμήμα Μαθηματικών, ως Επίκουρος Καθηγητής.

Από αρχές Μαρτίου του 2015 έως και τέλος Ιουλίου του 2015 ήταν προσκεκλημένος, με εκπαιδευτική άδεια, στο Department of Business Informatics, Faculty of Economics and Business Administration, Goethe University, Frankfurt, Germany. Η συνεργασία του με την εκεί ερευνητική ομάδα του Καθηγητή Kai Rannenberg επικεντρώθηκε σε θέματα προστασίας της ιδιωτικότητας με χρήση τεχνολογιών PETs (Privacy Enhancing Technologies) και, ειδικότερα, της τεχνολογίας Privacy-ABCs.

Επιβλέψεις διδακτορικών διατριβών

΄Εχει επιβλέψει τις εξής περατωθείσες διδακτορικές διατριβές:

- Απόστολος Τσιάκαλος, *Ασφάλεια Πληροφοριακών Συστημάτων: Μαθηματικές Αναλύσεις*, Τμήμα Μαθηματικών, Πανεπιστήμιο Ιωαννίνων, 2014.
- Παντελής Καμμάς, *Μαθηματικά μοντέλα ανάλυσης εισβολών σε δίκτυα υπολογιστών με χρήση των χαρακτηριστικών αποδοτικότητας των δικτύων*, Τμήμα Μαθηματικών, Πανεπιστήμιο Ιωαννίνων, 2010.

Σπουδές

Αποφοίτησε από το τμήμα Μηχανικών Ηλεκτρονικών Υπολογιστών και Πληροφορικής του Πανεπιστημίου Πάτρας με βαθμό <<άριστα>> 8.86/10, τον Ιούνιο του 1990. Τον Ιούνιο του 1991 ξεκίνησε στο ίδιο τμήμα μεταπτυχιακές σπουδές υπό την επίβλεψη του Καθηγητή κ. Ελευθέριου Κυρούση στην περιοχή των Θεμελιώσεων της Επιστήμης των Υπολογιστών και το Δεκέμβριο του 1997 υπερασπίστηκε με επιτυχία τη διδακτορική του διατριβή. Καθ' όλη τη διάρκεια των μεταπτυχιακών σπουδών του υπήρξε υπότροφος (ΕΜΥ) του Ιδρύματος Κρατικών Υποτροφιών. Το 1999 περάτωσε σπουδές στο Ελληνικό Ανοικτό Πανεπιστήμιο στη Θεματική Ενότητα <<Ανοικτή και εξ Αποστάσεως Εκπαίδευση>> και έλαβε Πιστοποιητικό Μεταπτυχιακής Επιμόρφωσης με βαθμό <<άριστα>> 9.1/10.

Διπλωματική Εργασία

Η διπλωματική του εργασία εκπονήθηκε υπό την εποπτεία του Καθηγητή κ. Αθανάσιου Τσακαλίδη και είχε τίτλο *Επαναξύγιση από τη Ρίζα προς τα Φύλλα των Red-Black Δέντρων και η Συμπεριφορά τους σε Περιβάλλοντα Παράλληλης Επεξεργασίας*.

Διδακτορική Διατριβή

Το Δεκέμβριο του 1997 υπερασπίστηκε με επιτυχία τη διδακτορική του διατριβή που πραγματοποιήθηκε υπό την επίβλεψη του Καθηγητή κ. Ελευθέριου Κυρούση και είχε τίτλο *Θεωρία και Εφαρμογές Προβλημάτων Ικανοποίησης Περιορισμών, Κατανεμημένο περιβάλλον-Παράλληλοι και τυχαιοποιημένοι αλγόριθμοι-Μη μονότονοι συλλογισμοί* και το Φεβρουάριο του 1998 ορκίστηκε διδάκτορας.

Μεταδιδακτορικές σπουδές

Από το Σεπτέμβριο του 1998 μέχρι το Σεπτέμβριο του 1999 ήταν μεταδιδακτορικός υπότροφος στο Πανεπιστήμιο του Carleton στην Ottawa του Καναδά. Είχε λάβει μία υποτροφία ΝΑΤΟ μέσω του Ελληνικού Υπουργείου Εθνικής Οικονομίας (αριθμός υποτροφίας 106384/ΔΟΟ 1222/2-7-98) και μία υποτροφία από το Καναδικό έργο MITACS με τον τίτλο CANCCOM (Complex Adaptive Networks for Computing and Communication). Κατά τη διάρκεια των μεταδιδακτορικών του σπουδών, εκτός από την ερευνητική του δραστηριότητα, δίδαξε και μαθήματα για Προγραμματισμό Συστημάτων με χρήση αντικειμενοστραφούς προγραμματισμού, στη γλώσσα C++.

Προσκλήσεις για ομιλία ή ερευνητική συνεργασία μέσα από ανταγωνιστικά προγράμματ

- Προσκεκλημένος ομιλητής στο PI4EST, the 8th International Summer School on Privacy and Identity Management for Emerging Services and Technologies. This Summer School is hosted by PI.lab in Nijmegen, the Netherlands on 17-21 June 2013.
- Πρόσκληση για παρουσίαση της πιλοτικής εφαρμογής του ερευνητικού έργου ABC4Trust ως εφαρμογή αριστείας στο CYBER SECURITY & PRIVACY EU FORUM 2013 (CSP EU FORUM), Brussels: 18-19 April, 2013.
- Προσκεκλημένος ομιλητής στο 6th Panhellenic Conference on Informatics with international participation (PCI 2012) με θέμα τις τεχνολογίες *Privacy by Design* με έμφαση στα Attribute Based Credentials και τις εφαρμογές τους.
- Μόνος ερευνητής του έργου *Dynamically Reconfigurable block ciphers through parallel substitution box construction*, contract no. HPRI-1999-CT-00071. Το έργο υλοποιήθηκε από 8 Σεπτεμβρίου έως 20 Σεπτεμβρίου 2008 στις εγκαταστάσεις του Barcelona Supercomputing

Center (BSC), που είναι μέλος του Ευρωπαϊκού οργανισμού HPC-Europa για High Performance Computing. Στα πλαίσια του έργου αναπτύχθηκε παράλληλο λογισμικό κατασκευής s-boxes με υψηλή μη γραμμικότητα, με χρήση της βιβλιοθήκης MPICH στον παράλληλο υπολογιστή του BSC MareNostrum (10240 processing cores, BladeCenter JS21 Cluster, PPC 970, 2.3 GHz, Myrinet).

- Ένας εκ των κύριων ομιλητών στις ημερίδες *Τεχνολογικής Καινοτομίας και Αριστείας* του *Περιφερειακού Πόλου Καινοτομίας Δυτικής Ελλάδος*, 22-25 Σεπτεμβρίου 2008, Πάτρα. Τίτλοι ομιλιών:

  - *Ο Άξονας Ασφάλειας Πληροφοριακών Συστημάτων και Δικτύων.*
  - *Συστήματα υποστήριξης ηλεκτρονικής ψηφοφορίας: απαιτήσεις και τεχνικές αντιμετώπισής τους - η πλατφόρμα ΠΝΥΚΑ.*

- Προσκεκλημένος ομιλητής στο 2ο Επιστημονικό Συμπόσιο Φοιτητών του τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου, με θέμα *Ασφάλεια και Προστασία της Ιδιωτικότητας στην Κοινωνία της Πληροφορίας*, 23-24 Νοεμβρίου 2007. Τίτλος ομιλίας:

  - *A Trust-centered Approach for Building E-voting Systems.*

- Σεπτέμβριος 2002: Προσκεκλημένος ομιλητής στο Πανεπιστήμιο του Liverpool, Τμήμα Επιστήμης των Υπολογιστών, για να δώσει ομιλίες στα πλαίσια ερευνητικού σεμιναρίου του τμήματος. Το θέμα των ομιλιών ήταν τα κατωφλικά φαινόμενα στην Επιστήμη των Υπολογιστών και της Φυσικής.

- Αύγουστος 2002: Προσκεκλημένος ομιλητής στο workshop *Random Structures* στο Isaac Newton Institute for Mathematical Sciences, Cambridge, με θέμα την διατήρηση τυχαιότητας σε αλγόριθμους διαχείρισης τυχαίων συνδυαστικών δομών.

- Ιούλιος 2001: Προσκλεκλημένος ομιλητής στο *Τρίτο Πανελλήνιο Συμπόσιο Λογικής* (με διεθνείς συμμετοχές) που πραγματοποιήθηκε στα Ανώγεια, στο Ηράκλειο της Κρητης. Η ομιλία του ήταν γύρω από θεωρητικά ζητήματα και εφαρμογές του Προβλήματος Ικανοποίησης Περιορισμών.

- Δεκέμβριος 1996: Επισκέπτης στο Ινστιτούτο Πληροφορικής Max-Planck στο Ζααρμπρούκεν της Γερμανίας για δέκα ημέρες. Παρουσίασε την ερευνητική του δραστηριότητα επάνω στην υπολογιστική πολυπλοκότητα παράλληλης επίλυσης στο Πρόβλημα Ικανοποίησης Περιορισμών καθώς επίσης και της επιβολής Μερικής Τοπικής Συνέπειας σε Δίκτυα Περιορισμών.

- Δεκέμβριος 1993: Επισκέπτης στο Πανεπιστήμιο της Καρλσρούης στη Γερμανία, για μία εβδομάδα. Παρουσίασε την ερευνητική του δραστηριότητα στο Πρόβλημα Ικανοποίησης Περιορισμών.

Προσκλήσεις για διδασκαλία σε διεθνή σχολεία

- Προσκεκλημένος στο *4th AIT Annual Workshop on PRactical AspeCts of SEcurity - PRACSE 2009* που διοργάνωσε το Athens Information Technology (AIT) center στην Αθήνα από 11/6/2009 έως 12/6/2009. Το θέμα της ομιλίας ήταν το εξής:

- Principles of good block-cipher design: the S-box parameter.

- Προσκεκλημένος στο *2nd AIT Annual Workshop on PRactical AspeCts of SEcurity - PRACSE 2007* που διοργάνωσε το Athens Information Technology (AIT) center στην Αθήνα από 2/11/2007 έως και 3/11/2007. Το θέμα της ομιλίας ήταν το εξής:

  - A trust-centered approach for building e-voting systems.

- Προσκεκλημένος στο *1st AIT Annual Workshop on PRactical AspeCts of SEcurity - PRACSE 2006* που διοργάνωσε το Athens Information Technology (AIT) center στην Αθήνα από 16/6/2006 έως και 17/6/2006. Τα θέματα των δύο ομιλιών που δόθηκαν ήταν τα εξής:

  - *AUTHENTICATION PROTOCOLS:* Notions of Authentication, Basic techniques and Typical Attacks.
  - *EVALUATION OF REAL WORLD PROTOCOL STANDARDS:* IPSec, SSH, SSL, Kerberos.

- Προσκεκλημένος να διδάξει μία ενότητα σχετικά με *Κατωφλικά Φαινόμενα στην Επιστήμη των Υπολογιστών* στο *The Logic and Interaction Programme*, 28 Ιανουαρίου - 1 Μαρτίου 2002, που έλαβε χώρα στη Μασσαλία, Γαλλία, και συνδιοργανώθηκε από το *Institut de Mathematiques de Luminy (IML)* και το *Laboratoire d' Informatique Fondamentale de Marseille (LIF)*.

Προσκλήσεις για κρίση ερευνητικών εργασιών σε διεθνή περιοδικά

- Πρόσκληση για κρίση άρθρων στο Mathematical Reviews της American Mathematical Society (AMS).

- Τακτικός κριτής στα περιοδικά Computers & Security, Theoretical Computer Science, SIAM journal on Computing, Discrete Mathematics, Computer Magazine IEEE, Transactions on Computers IEEE, Journal of Systems and Software.

Συμμετοχή σε επιτροπές προγράμματος συνεδρίων

- Μέλος της επιστημονικής επιτροπής του συνεδρίου *2nd ANNUAL ICT SECURITY WORLD CONGRESS*.

- Μέλος της επιτροπής προγράμματος του *European Intelligence and Security Informatics Conference (EISIC) 2016*.

- Μέλος της επιτροπής προγράμματος του *12th International Conference on e-Commerce 2015 (EC 2015)*.

- Μέλος της επιτροπής προγράμματος του *European Intelligence and Security Informatics Conference (EISIC 2015)*.

- Μέλος της επιτροποής προγράμματος του *2015 IEEE International Conference on Intelligence and Security Informatics (IEEE ISI 2015)*.

- Μέλος της επιτροπής προγράμματος του *The Ninth International Conference on Digital Society (ICDS 2015)*.

- Organizing chair (υπεύθυνος διοργάνωσης) του *9th International IFIP Summer School on Privacy and Identity Management for the Future Internet in the Age of Globalization.* που έλαβε χώρα στις εγκαταστάσεις του ΙΤΥΕ στην Πάτρα από 7 έως και 12 Σεπτεμβρίου 2014. Ο κ. Σταματίου συμμετείχε και ως κύριος ομιλητής ενός WORKSHOP με θέμα την χρήση ψηφιακών πιστοποιητικών με προστασία της ιδιωτικότητας των κατόχων τους.
- Μέλος της επιτροπής προγράμματος του *European Intelligence and Security Informatics Conference (EISIC 2014)*.
- Μέλος της επιτροπής προγράμματος του *CYBER SECURITY & PRIVACY EU FORUM 2014 (CSP FORUM 2014)*.
- Μέλος της επιτροπής προγράμματος του *Annual Privacy Forum 2014 (APF 2014)*.
- Μέλος της επιτροπής προγράμματος του *2014 International Workshop on Computer Software and Services (CSS 2014)* που πραγματοποιήθηκε στα πλαίσια του *6th FTRA International Conference on Computer Science and its Applications (CSA-14)*.
- Μέλος της επιτροπής προγράμματος του *6th FTRA International Symposium on Advances in Computing, Communications, Security, and Applications (ACSA-14)* που πραγματοποιήθηκε στα πλαίσια του *6th FTRA International Conference on Computer Science and its Applications (CSA-14)*.
- Μέλος της επιτροπής προγράμματος του *13th International Conference on Cryptology and Network Security (CANS-2014)*.
- Μέλος της επιτροπής προγράμματος του Special Session on Trusted Computing for Critical Information Infrastructures - T(CI)2. The event was held in conjunction with the 4th International Conference on Information, Intelligence, Systems and Applications - IISA2013, 10-12 July 2013.
- Μέλος της επιτροπής προγράμματος του *European Intelligence and Security Informatics Conference (EISIC 2013)*.
- Μέλος της επιτροπής προγράμματος του *The IADIS e-Commerce 2013 conference*.
- Μέλος της επιτροπής προγράμματος του *Fourth International Conference on Technical and Legal Aspects of the e-Society 2012 (CYBERLAWS 2013)*.
- Μέλος της επιτροπής προγράμματος του *Sixth International Conference on Sensor Technologies and Applications - SENSORCOMM 2012.*
- Μέλος της επιτροπής προγράμματος του *Third International Conference on Technical and Legal Aspects of the e-Society 2012 (CYBERLAWS 2012)*.
- Μέλος της επιτροπής προγράμματος του *IEEE Symposium on Wireless Technology & Applications 2012 (ISWTA 2012)*.
- Μέλος της επιτροπής προγράμματος του *International Symposium on Foundation of Open Source Intelligence and Security Informatics, 2012 (FOSINT-SI 2012)*.
- Μέλος της επιτροπής προγράμματος του *The IADIS e-Commerce 2012 conference*.
- Μέλος της επιτροπής προγράμματος του *European Intelligence and Security Informatics Conference (EISIC 2012)*.

- Μέλος της επιτροπής προγράμματος του *7th IEEE International Workshop on Wireless and Sensor Networks Security (IEEE WSNS 2011)*.
- Μέλος της επιτροπής προγράμματος του *7th European Conference on Computer Network Defense* (EC2ND 2011).
- Μέλος της επιτροπής προγράμματος του *The 5th International Conference on Information Security and Assurance* (ISA 2011).
- Μέλος της επιτροπής προγράμματος του *7th International Conference on Global Security, Safety & Sustainability (ICGS^{3}11)*.
- Μέλος της επιτροπής προγράμματος του *The IADIS e-Commerce 2011 conference*.
- Μέλος της επιτροπής προγράμματος του *Second International Conference on Security-enriched Urban Computing and Smart Grid (SUComS)* 2011.
- Μέλος της επιτροπής προγράμματος του *4th IFIP International Conference on New Technologies, Mobility and Security (NTMS 2011)*, Security Track.
- Μέλος της επιτροπής προγράμματος του *The Sixth IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'10)*
- Μέλος της επιτροπής προγράμματος του *First International Conference on Security-enriched Urban Computing and Smart Grid (SUComS)* 2010.
- Μέλος της επιτροπής προγράμματος του *Webit eGov Summit*, 2010, organized by the eAcademy, eEducation Institute of Bulgaria.
- Μέλος της επιτροπής προγράμματος του *APSIPA (Asia-Pacific Signal and Information Processing Association) Annual Summit and Conference 2010*.
- Μέλος της επιτροπής προγράμματος του *Seventh European Workshop on Public Key Services, Applications and Infrastructures* (EUROPKI 2010).
- Μέλος της επιτροπής προγράμματος του *15th European Symposium on Research in Computer Security* (ESORICS 2010).
- Μέλος της επιτροπής προγράμματος του *The IADIS e-Commerce 2010 conference*.
- Μέλος της επιτροπής προγράμματος του *2nd International Conference on Advanced Science and Technology* (AST 2010).
- Μέλος της επιτροπής προγράμματος του *The 4th International Conference on Information Security and Assurance* (ISA 2010).
- Προσκεκλημένος το Δεκέμβριο 2009 ως rapporteur στην κρίση Ευρωπαϊκών έργων του 7ου πλαισίου στην πρόσκληση *PHOTONICS*.
- Μέλος της επιτροπής προγράμματος του *International Conference on Information Security and Cryptology (Inscrypt)*, Inscrypt 2009, Inscrypt 2010.
- Μέλος της επιτροπής προγράμματος του *1st International Conference on Sensor Networks Applications, Experimentation and Logistics (SENSAPPEAL 2009)*.

- Μέλος της Επιτροπής Προγράμματος του *2009 International Conference on Security and Cryptography* (SECRYPT 2009).
- Μέλος της Επιτροπής Προγράμματος του *Fifth International Conference on Security and Privacy in Communication Networks (SecureComm 2009)*.
- Μέλος της Επιτροπής Προγράμματος του *2009 International Conference on Security Technology (SecTech 2009)*, *2010 International Conference on Security Technology (SecTech 2010)*.
- Προσκεκλημένος δύο φορές (2006 και 2007) ως ειδικός σε θέματα κρυπτογραφίας και ασφάλειας πληροφοριακών συστημάτων για κρίση Ευρωπαϊκών έργων του 7ου πλαισίου.
- Μέλος της Επιτροπής Προγράμματος (Programm Committee) στο ECAI 2008 Workshop *The Quest for Approximate and Exact Equilibria in Games* (ExCalibur).
- Μέλος της Επιτροπής Προγράμματος (Programm Committee) στο συνέδριο SECRYPT (International Conference on Security and Cryptography) 2008. SECRYPT is part of ICETE, the *International Joint Conference on e-Business and Telecommunications*.
- Μέλος της Επιτροπής Προγράμματος (Program Committee) στο 5th European PKI Workshop (EUROPKI 2008).
- Μέλος της Επιτροπής Προγράμματος (Program Committee) στο IADIS Conference on e-Commerce 2007.
- Μέλος της Επιτροπής Προγράμματος (Program Committee) στο 6th International Conference on AD-HOC Networks & Wireless (ADHOC-NOW 2006).
- Μέλος της Επιτροπής Προγράμματος (Program Committee) στο Inscrypt (formerly CISC - Conference on Information Security and Cryptology) (CISC 2006, INSCRYPT 2007).
- Μέλος της Επιτροπής Προγράμματος (Program Committee) στο International Workshop on Information Security Applications (WISA 2005, WISA 2006, WISA 2007).
- Μέλος της Επιτροπής Προγράμματος (Program Committee) και επικεφαλής της Οργανωτικής Επιτροπής (Organizing Committee) στο 9ο Colloquium on Structural Information and Communication Complexity (SIROCCO '02).
- Μέλος της Οργανωτικής Επιτροπής (Organizing Committee) στο Third Annual European Symposium on Algorithms (ESA '95).
- Μέλος της Οργανωτικής Επιτροπής στο 2ο Colloquium on Structural Information and Communication Complexity (SIROCCO '95).

Συστάσεις

- Professor Svante Janson, Uppsala University, Department of Mathematics P. O. Box 480 S-751 06 Uppsala, Sweden.
  e-mail: svante.janson@math.uu.se, tel.: +46 18 4713188, fax.: +46 18 4713201.
- Professor Lefteris Kirousis, University of Patras, School of Engineering, Department of Computer Engineering and Informatics, 26500 Rio, Patras, Greece.
  e-mail: kirousis@ceid.upatras.gr, tel.: +30 61 99 77 02, fax.: +30 61 99 19 09.

- Professor Evangelos Kranakis, Carleton University, School of Computer Science, 1125 Colonel By Drive, Ottawa, Ontario, K1S 5B6, Canada.
  e-mail: kranakis@scs.carleton.ca, tel.: (613) 520-4330, fax.: (613) 520-4334.

- Professor Danny Krizanc, Wesleyan University, Mathematics Department, Computer Science Group, Middletown, CT 06459 USA.
  email: dkrizanc@wesleyan.edu, tel.: 860-685-2186, fax.: 860-685-2571.

- Professor David Peleg, Faculty of Mathematics and Computer Science, The Weizmann Institute of Science, Rehovot 76100, Israel.
  e-mail: peleg@wisdom.weizmann.ac.il, tel.: +972-8-934-3478, fax.: +972-8-934-4122.

Εμπειρία σε ερευνητικά και αναπτυξιακά έργα

- Μέλος της Ομάδας Έργου του έργου: «ΣΧΕΔΙΑΣΜΟΣ ΚΑΙ ΕΦΑΡΜΟΓΗ ΜΕΘΟΔΟΛΟΓΙΑΣ ΓΙΑ ΤΗΝ ΣΥΜΜΟΡΦΩΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ ΣΤΗΝ ΟΔΗΓΙΑ (ΕΕ) 2016/679 ΠΕΡΙ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ» (80281 - Ε.Υ. Β. Βουτσινάς), στο πλαίσιο του οποίου εφαρμόσθηκε μεθοδολογία για την συμμόρφωση με τον Κανονισμό 2016/679, ανάμεσα σε άλλες εταιρίες και σε: 11 Ψυχιατρικές Κλινικές, 2 Γενικές Κλινικές και 1 Μονάδα Αιμοκάθαρσης.

- **Ευρωπαϊκό έργο Privacy Flag (HORIZON 2020). Χρόνος εκτέλεσης έργου: Απρίλιος 2015 - Απρίλιος 2018.** Το έργο αυτό θα διερευνήσει και θα εκμεταλλευτεί τις δυνατότητες του crowdsourcing, των Τεχνολογιών Πληροφορικής και Επικοινωνιών καθώς και νομικών εμπειρογνωμόνων με στόχο την προστασία της ιδιωτικότητας των πολιτών όταν επισκέπτονται ιστοσελίδες, όταν χρησιμοποιούν εφαρμογές smartphone (Apps), ή όταν ζουν και κινούνται σε μια έξυπνη πόλη. Θα επιτρέψει στους πολίτες να παρακολουθούν και να ελέγχουν τυχόν παραβιάσεις της ιδιωτικότητάς τους σε πραγματικό χρόνο με τα εξής: μία φιλική προς το χρήστη εφαρμογή που θα διατίθεται ως εφαρμογή smartphone, ένα ειδικό web browser add-on, και μια δημόσια προσπελάσιμη ιστοσελίδα που θα περιέχει μία δυναμικά εξελισσόμενη βάση γνώσης με γνωστούς κινδύνους για τα δεδομένων και τξμ ιδιωτικότητα των πολιτών.

- **Ευρωπαϊκό έργο IoT Lab (FP7). Χρόνος εκτέλεσης έργου: Οκτώβριος 2013 - Σεπτέμβριος 2016.** Το έργο IoT Lab έχεις ως στόχο την ανάπτυξη μιας πλατφόρμας crowdsourcing βασισμένης στο Internet of Things (IoT) για τη διεξαγωγή διεπιστημονικής έρευνας μέσω της αλληλεπίδρασης της πλατφόρμας με χρήστες που προσφέρουν διάφορα δεδομένα από το χώρο που βρίσκονται και κινούνται. Η πλατφόρμα αυτή δίνει την ευκαιρία στους χρήστες του διαδικτύου να συμμετάσχουν ενεργά στη διενέργεια σημαντικών πειραμάτων και να συνεισφέρεουν, με το μεγάλο όγκο δεδομένων που συλλογικά προσφέρουν, στην εξαγωγή χρήσιμων συμπερασμάτων. Ιδιαίτερη έμφαση έχει δοθεί στην ασφάλεια των δεδομένων των χρηστών καθώς και στην προστασία της ιδιωτικότητάς τους.

- **Ευρωπαϊκό έργο IP ABC4Trust. Χρόνος εκτέλεσης έργου: Νοέμβριος 2010 - Φεβρουάριος 2015.** Με στόχο την εξάλειψη των αρνητικών στοιχείων των σημερινών μεθόδων ψηφιακής ταυτοποίησης (κυρίως η αποκάλυψη όλων των στοιχείων του κατόχου του ψηφιακού πιστοποιητικού), βρίσκεται σε εξέλιξη τα τελευταία χρόνια μία νέα γραμμή έρευνας για δημιουργία ψηφιακών πιστοποιητικών βασισμένων στην αποκάλυψη επιλεγμένων χαρακτηριστικών ταυτότητας του χρήστη. Η έρευνα αυτή έχει οδηγήσει στη δημιουργία των Attribute-based Credentials (ABCs) τα οποία είναι ψηφιακά πιστοποιητικά που επιτρέπουν στον κάτοχό τους να αποκαλύψει, επιλεκτικά και υπό το δικό του έλεγχο, μόνο τις πληροφορίες που

απαιτούνται από την υπηρεσία που επιθυμεί να χρησιμοποιήσει, χωρίς να δώσει τα πλήρη στοιχεία της ταυτότητας του, προστατεύοντας με αυτόν τον τρόπο τα προσωπικά δεδομένα του χρήστη και την ιδιωτικότητά του. Αυτά τα πιστοποιητικά μπορούν, συνεπώς, να αποτελέσουν τον ακρογωνιαίο λίθο μιας αξιόπιστης, έμπιστης και συγχρόνως ασφαλούς ψηφιακής κοινωνίας όπου κάθε χρήστης θα μπορεί να αποκαλύπτει μόνο τα στοιχεία της ταυτότητάς του που κάθε φορά επιθυμεί ή πρέπει να αποκαλύψει. Το ABC4Trust είναι ένα ευρωπαϊκό πρόγραμμα (https://abc4trust.eu/) του οποίου κύριος στόχος είναι να εξετάσει τη διαλειτουργικότητα των υπαρχουσών τεχνολογιών ABCs και να τις εφαρμόσει σε δύο πιλοτικές εφαρμογές. Το ΙΤΥΕ συμμετείχε ως εταίρος του έργου ABC4Trust και ήταν υπεύθυνος οργανισμός για μια από τις δύο πιλοτικές εφαρμογές του έργου στο πεδίο των ηλεκτρονικών αξιολογήσεων μαθημάτων στα πανεπιστήμια με προστασία της ιδιωτικότητας των συμμετεχόντων. Ο κ. Σταματίου είχε την τεχνική και επιστημονική ευθύνη του έργου, από την πλευρά του ΙΤΥΕ, με συμμετοχή σε όλες τις συναντήσεις του έργου καθώς και στις συναντήσεις για την κρίση του. Τα αποτελέσματα του έργου έχουν κριθεί ως άριστα (από τους reviewers της ΕΕ καθώς και διεθνείς οργανιστμούς) και έχουν τύχει πολλών διεθνών διακρίσεων και διεθνούς προβολής με σημαντική συμμετοχή του ΙΤΥΕ και του κ. Σταματίου.

- **Πιστοποίηση ορθότητας και ασφάλειας ηλεκτρονικών παιχνιδιών της εταιρείας INTRALOT. Χρόνος εκτέλεσης έργου: Απρίλιος 2012 - Μάρτιος 2014.** Στο έργο αυτό ο κ. Σταματίου είχε την ευθύνη της διενέργειας ελέγχων ορθότητας μαθηματικών υπολογισμών (βασισμένων σε διακριτά μαθηματικά, συνδυαστική και στατιστική) καθώς και ασφάλειας των παικτών σε διαδικτυακά παιχνίδια που υπέβαλλε στο ΙΤΥΕ η εταιρία INTRALOT με στόχο την εφαρμογή τους από τον ΟΠΑΠ>

- **Περιφερειακός Πόλος Καινοτομίας Δυτικής Ελλάδας (ΠΠΚ-ΔΕ). Χρόνος εκτέλεσης έργου: 2007-2008.** Ο Περιφερειακός Πόλος Καινοτομίας Δυτικής Ελλάδας (ΠΠΚ-ΔΕ) είναι μια ένωση φορέων του δημόσιου και ιδιωτικού τομέα, με στόχο την ανάπτυξη, προώθηση και εκμετάλλευση της καινοτομίας στην Περιφέρεια Δυτικής Ελλάδας (ΠΔΕ). Κεντρικός στόχος είναι η οργάνωση και ισχυροποίηση των δεσμών μεταξύ των Ερευνητικών / Τεχνολογικών & Επιχειρηματικών Φορέων της ΠΔΕ με σκοπό την εκπόνηση ενεργειών που ενισχύουν τις τεχνολογικές και καινοτομικές επιδόσεις της Περιφέρειας. Αποτέλεσμα των προσπαθειών στα πλαίσια του έργου αυτού ήταν η *Περιφερειακή Τεχνολογική Πλατφόρμα του ΠΠΚ-ΔΕ* (http://www.westplatform.gr/) για την προαγωγή της εφαρμοσμένης έρευνας στην περιοχή των βιομηχανικών συστημάτων & επικοινωνιών, του βιομηχανικού ελέγχου, των ενσωματωμένων συστημάτων και της ασφαλείας πληροφοριακών συστημάτων και δικτύων. Ο κ. Σταματίου συμμετείχε ως κύριος ερευνητής στον τέταρτο άξονα, της Ασφάλειας Πληροφοριακών Συστημάτων και Δικτύων και η συμμετοχή του επικεντρώθηκε σε θέματα κρυπτογραφίας και ασφάλειας καθώς και της εφαρμογής αυτών για την υποστήριξη της ασφαλούς λειτουργίας επιχειρήσεων και οργανισμών.

- **΄Ερευνα και Ανάπτυξη Συστημάτων Ηλεκτρονικής Ψηφοφορίας βασισμένων σε Τυπικές Μεθόδους Σχεδίασης και Διαχείρισης Κινδύνων με εστίαση στην Προσέλκυση της Εμπιστοσύνης του Πολίτη - ΠΝΥΚΑ (http://www.pnyka.cti.gr). Χρόνος εκτέλεσης έργου: 2006 - 2008.** Το ερευνητικό/αναπτυξιακό έργο ΠΝΥΚΑ, με χρηματοδότηση από την Γενική Γραμματεία ΄Ερευνας και Τεχνολογίας, υλοποιήθηκε από το Ερευνητικό Ακαδημαϊκό Ινστιτούτο Τεχνολογίας Υπολογιστών (ΕΑ ΙΤΥ) σε συνεργασία με την εταιρία EXPERTNET Προηγμένες Εφαρμογές ΑΕ στο πλαίσιο ενός ερευνητικού προγράμματος της ΓΓΕΤ. Στόχος ήταν η σχεδίαση και υλοποίηση ενός ολοκληρωμένου συστήματος υποστήριξης ηλεκτρονικής ψηφοφορίας μέσω Internet, με έμφαση στην προστασία της ιδιωτικότητας του πολίτη. Το σύστημα ΠΝΥΚΑ

υποστηρίζει όλα τα στάδια μιας ηλεκτρονικής ψηφοφορίας όπως εγγραφή/πιστοποίηση, υποβολή ψήφου, καταμέτρηση αποτελεσμάτων και επαλήθευση. Για τη μεγιστοποίηση του βαθμού προστασίας της ιδιωτικότητας του ψηφοφόρου, το σύστημα ενσωματώνει πολλές τεχνολογικές καινοτομίες όπως πλήρως κατανεμημένη αρχιτεκτονική, ομομορφική κρυπτογράφηση κατωφλίου, συσκευές υλικού για την αποθήκευση των κλειδιών κλπ. και έχει αναπτυχθεί εξ' ολοκλήρου με εργαλεία ανοικτού κώδικα έτσι ώστε να διευκολύνεται η επαληθευσιμότητά του. Μπορεί, επίσης, να παραμετροποιηθεί για να υποστηρίξει διαφορετικές μορφές ψηφοφορίας, από απλές διαδικασίες έκφρασης γνώμης μέχρι εκλογές και δημοψηφίσματα μεγάλης κλίμακας. Ο σχεδιασμός του συστήματος έγινε με τη χρήση τυπικών μεθόδων ανάλυσης και διαχείρισης κινδύνων όπως το πλαίσιο CORAS δίνοντας έτσι έμφαση στην προσέλκυση της δημόσιας εμπιστοσύνης. Το σύστημα εφαρμόστηκε με επιτυχία σε μια δοκιμαστική ηλεκτρονική ψηφοφορία μεταξύ των μελών του ΤΕΕ Δυτικής Ελλάδας ενώ συμμετείχε παράλληλα στο διαγωνισμό e-voting που διοργάνωσε το Competence Center for Electronic Voting and Participation (http://www.e-voting-competition.at/) με χορηγό τον αυστριακό οργανισμό Internet Foundation Austria (IFA) όπου και απέσπασε το πρώτο βραβείο.

- **Τεχνικός σύμβουλος της EXPERTNET Προηγμένες Εφαρμογές ΑΕ σε έργα με κύρια συνιστώσα την ασφάλεια πληροφοριακών συστημάτων. Χρόνος συνεργασίας: 2004-2007**. Ο κ. Σταματίου διατέλεσε τεχνικός σύμβουλος σε τέσσερα έργα σχετικά με την ασφάλεια πληροφοριακών συστημάτων και την ηλεκτρονική διακυβέρνηση. **(i) IST STREP έργο e-Mayor:** Στόχος του έργου ήταν η δημιουργία μίας ολοκληρωμένης πλατφόρμας για τη σύνδεση δημαρχείων (σε ευρωπαϊκό επίπεδο) και την υποστήριξη ασφαλούς ανταλλαγής εγγράφων μεταξύ τους (με χρήση κατάλληλων κρυπτογραφικών τεχνικών και Υποδομών Δημόσιου Κλειδιού - PKI). **(ii) IST eTen έργο Selis:** Το έργο αυτό είχε ως στόχο την υλοποίηση μίας πλατφόρμας διαχείρισης ηλεκτρονικών τιμολογίων με ασφάλεια στηριγμένη σε Υποδομή Δημόσιου Κλειδιού - PKI και κατάλληλα κρυπτογραφικά πρωτόκολλα. **(iii) IST IP έργο Intelcities:** Ο στόχος του έργου ήταν η δημιουργία ενός ανοικτού συστήματος, που καλείται *e-city Platform*, για την υποστήριξη λειτουργιών ηλεκτρονικής διακυβέρνυσης με ασφάλεια και διαλειτουργικότητα. **(iv) Έργο υποστηριζόμενο από ΓΓΕΤ, Bioathletics:** Το έργο αυτό είχε ως στοχο τη δημιουργία συστήματος βιομετρικού ελέγχου εισερχομένων σε αθλητικούς χώρους με βάση τα χαρακτηριστικά των δακτυλικών τους αποτυπωμάτων

- **Παιγνίδια πρόβλεψης αριθμών EXTRA 5 και SUPER 3 του ΟΠΑΠ. Χρόνος εκτέλεσης έργου: 2001-2002.** Στα πλαίσια του έργου αυτού, ο κ. Σταματίου σχεδίασε το λογισμικό και την αρχιτεκτονική υλικού του ενός συστήματος γένεσης τυχαιων αριθμών για τα νέα παιγνίδια του ΟΠΑΠ EXTRA 5 και SUPER 3. Επιπρόσθετα, υλοποίησε τα πιο κρίσιμα κρυπτογραφικά μέρη του συστήματος και διεύθυνε ομάδα προγραμματιστών του ΕΑΙΤΥ που επιτέλεσε την τελική ολοκλήρωση.

  Το σύστημα γένεσης των αριθμών που σχεδίασε ο κ. Σταματίου περιλαμβάνει τα πιο κάτω κύρια μέρη:

  1. Τρεις γενήτριες πραγματικά τυχαίων αριθμών (μία βασισμένη σε shot-noise σε δίοδο zener, μία βασισμένη σε θερμικό θόρυβο σε αντίσταση και μία βασισμένη στην τυχαιότητα στη διαφορά φάσης μεταξύ δύο πηγών χρονισμού στο motherboard του υπολογιστή).
  2. Δύο κρυπτογραφικά ασφαλείς γενήτριες ψευδοτυχαίων αριθμών, BBS και RSA, και δύο βασισμένες σε κατάλληλα τροποποιημένους block ciphers. Επίσης, συμπειλήφθηκαν και οι αλγόριθμοι Τους αλγόριθμους M και B για την πολύπλεξη της εξόδου των

παραπάνω αλγορίθμων. (Οι M και B περιγράφονται στο βιβλίο Seminumerical Algorithms του Knuth.)

Τη σχεδίαση και υλοποίηση συμπληρώνουν, μεταξύ άλλων, ειδικά σχήματα bit-commitment, επεξεργασίας seeds (σχήμα Naor-Reingold), signature verification, cross-verification των παραγόμενων αριθμών μέσα από την εγγραφή τους σε CD-ROM αμέσως μετά την παργωγή τους, και πιστοποίησης της ταυτότητας των υπολογιστών που παράγουν τους αριθμούς των κληρώσεων.

- **IST έργο "ASPIS". Χρόνος εκτέλεσης έργου: 2000-2002.** Το Ευρωπαϊκό αυτό έργο είχε ως στόχο την παραγωγή ενός ολοκληρωμένου συστήματος για την προστασία DVD-ROM από αντιγραφή το οποίο περιλαμβάνει μηχανισμούς υψηλής ασφάλειας για την φυσική προστασία του DVD-ROM από αντιγραφή (το οποίο είναι ήδη πατέντα της εταιρίας MLS που είναι και η εταιρία υπεύθυνη του έργου) και για την προστασία των δεδομένων του (κατά την αποθήκευση και τη μεταφορά τους). Πιο συγκεκριμένα, η ομάδα την οποία διευθύνει ο κ. Σταματίου είχε αναλάβει τα υποέργα της κρυπτογράφησης/αποκρυπτογράφησης δεδομένων με αλγοριθμικά παραγόμενους Feistel κρυπταλγόριθμους βασισμένους στη μεθοδολογία σχεδίασης του CAST-128, της υδατογράφησης ψηφιακών αρχείων ήχου (audio watermarking) και τη δημιουργία ειδικών βιβλιοθηκών λογισμικού κρυπτογραφίας δημόσιου κλειδιού και αλγόριθμων κρυπτανάλυσης με χρήση Ελλειπτικών Καμπυλών για το χτίσιμο ασφαλών εφαρμογών ηλεκτρονικού εμπορίου.

  Πέρα από την επίβλεψη της ομάδας, ανέλαβε και περάττωσε προσωπικά το μέρος της κατασκευής των εφαρμογών κρυπτογράφησης/αποκρυπτογράφησης όπου σχεδίασε και υλοποίηση ένα γενικό κρυπταλγόριθμο block με επαναπροσδιορίσιμα (reconfigurable) κουτιά αντικατάστασης (substitution boxes ή s-boxes) που βασίζεται στην παραγωγή και συνδυασμό Boolean συναρτήσεων bent έτσι ώστε οι κρυπταλγόριθμοι να είναι ανθεκτικοί στη γραμμική και διαφορική κρυπτανάλυση. Στο κομμάτι της υδατογράφησης ψηφιακών αρχείων ήχου, σχεδίασε και υλοποίησε το μέρος της δημιουργίας του ψηφιακού υδατογραφήματος με χρήση της θεωρίας κατωφλικών φαινομένων σε υπολογιστικά δύσκολα προβλήματα έτσι ώστε τα υδατογραφήματα να αντιπροσωπεύουν στιγμιότυπα των προβλημάτων αυτών. Πιο συγκεκριμένα, χρησιμοποίησε το NP-πλήρες πρόβλημα του χρωματισμού ενός γραφήματος με 3 το πολύ χρώματα (3-COLORING) για να δημιουργεί στιγμιότυπα (γραφήματα) του προβλήματος που έχουν ένα συγκεκριμένο χρωματισμό και που βρίσκονται στην περιοχή που, πειραματικά, διαφαίνεται να συσσωρεύονται πολλά δύσκολα να επιλυθούν στιγμιότυπα. Γνώση του χρωματισμού, συνεπάγεται ταυτοποίηση του χρήστη. Τέλος, είχε μεγάλη συμμετοχή στο μέρος της σχεδίασης και υλοποίησης του λογισμικού κρυπτογραφίας ελλειπτικών καμπυλών με καλές κρυπτογραφικές ιδιότητες, χρησιμοποιώντας την τεχνική του Μιγαδικού Πολλαπλασιασμού (Complex Multiplication) με αριθμητική μιγαδικών αριθμών απεριόριστης ακρίβειας.

- **IST έργο "CORAS". Χρόνος εκτέλεσης έργου: 2000-2003**: Αυτό το έργο είχε ως στόχο την ανάπτυξη και τη δοκιμή μιας ολοκληρωμένης μεθοδολογίας ανάλυσης ασφάλειας και επικινδυνότητας σε εφαρμογές όπου η ασφάλεια είναι σημαντική απαίτηση (π.χ. εφαρμογές τηλεϊατρικών υπηρεσιών). Η μεθοδολογία αυτή στηρίζεται σε ημιτυπική μοντελοποίηση (semiformal modeling) και την προσαρμογή μεθόδων ανάλυσης ρίσκου σε εφαρμογές υψηλής επικινδυνότητας (safety analysis) όπως είναι, για παράδειγμα, η ανάλυση ρίσκου σε έναν πυρηνικό αντιδραστήρα. Στο έργο αυτό, το EAITY μαζί με δύο άλλους συνεργάτες του έργου, (το Ινστιτούτο Τεχνολογίας και Έρευνας (ITE) στο Ηράκλειο Κρήτης και η NCT-National Centre for Telemedicine της Νορβηγίας), θα σχεδιάσει και θα διευθύνει τις

δοκιμές ανάλυσης ασφάλειας στο δίκτυο υποστήριξης τηλεϊατρικών εφαρμογών HYGEIANET που αναπτύχθηκε από το ΙΤΕ και το οποίο συνδέει τα νοσοκομεία και τα κέντρα υγείας σε όλη την Κρήτη. Οι δοκιμές θα επικεντρώσουν στην παραγωγή ημιτυπικών μοντέλων (με χρήση παραλλαγών της UML, Universal Modeling Language) δύο εφαρμογών του δικτύου τηλεϊατρικής στα οποία υπάρχουν υψηλές απαιτήσεις ασφάλειας: της εφαρμογής ATTRACT παρακολούθησης από απόσταση της πορεία ασθματικών παιδιών και της εφαρμογής ΤηλεΚαρδιολογίας που υποστήρίζει διάγνωση και παρακολούθηση από απόσταση καρδιακών ασθενειών. Τα μοντέλα που θα παραχθούν θα υποστούν ανάλυση με χρήση της μεθοδολογίας του έργου και τα αποτελέσματα θα κοινοποιηθούν και θα αναλυθούν στους γιατρούς στο Πανεπιστημιακό Νοσοκομείο Ηρακλείου, ώστε να τους βοηθήσουν να κατανοήσουν καλύτερα τι σημαίνει ασφάλεια και πώς αυτή επιτυγχάνεται στις εφαρμογές που χρησιμοποιούν καθυμερινα, καθώς και στους τεχνικούς που ανάπτυξαν τις εφαρμογές τηλεϊατρικής έτσι ώστε να τους βοηθήσουν να τις κάνουν ασφαλέστερες. Τέλος τα αποτελέσματα αυτά θα αξιολογηθούν από τους συνεργάτες του CORAS με βάση κριτήρια που έχουν καθοριστεί από το ΕΑΙΤΥ έτσι ώστε να βελτιωθεί η μεθοδολογία.

- **΄Εργο "ΣΤΟΙΧΗΜΑ". Χρόνος εκτέλεσης έργου: 2000-2002.**: Στο έργο αυτό, ο στόχος του ΕΑΙΤΥ ήταν να σχεδιάσει και να υλοποιήσει ένα πολυχρηστικό λογισμικό δειχείρισης ρίσκου για ιδιωτική εταιρία που υποστηρίζεί παγνίδια πρόγνωσης σε αθλητικά γεγονότα. Το λογισμικό αυτό θα έπρεπε να αναγνωρίζει και να επισημαίνει καταστάσεις που τείνουν να δημιουργηθούν και που πιθανόν να οδηγήσουν την εταιρία σε σημαντική οικονομική ζημιά. μταν ο σχεδιαστής του λογισμικού και, επιπρόσθετα, υλοποίησε τη βάση δεδομένων (βασισμένη σε δομή B-trees με τα φύλλα σε διπλά διασυνδεδεμένη λίστα) και το σύστημα συλλογής και στατιστικής επεξεργασίας εισερχόμενων δεδομένων). Το λογισμικό υλοποιήθηκε με χρήση του C++ Builder Enterprise 4.0 της Borland σε περιβάλλον WINDOWS NT.

  Η βάση δεδομένων που υλοποίησε με χρήση των B-trees και με εκμετάλλευση της κύριας μνήμης για συχνά προσπελασόμενα δεδομένα (σχήμα cache LRU), φτάνει ταχύτητες που ξεπερνούν κατά τάξεις μεγέθους την απόδοση του προηγούμενου συστήματος της εταιρίας που βασιζόταν σε εμπορικό πακέτο διαχείρισης βάσεων δεδομένων. Επιπρόσθετα, το στατιστικό κομμάτι του λογισμικού υλοποιεί διάφορους ελέγχους στατιστικής τυχαιότητας και παράγει έναν αριθμό από στατιστικά δεδομένα χρήσιμα για την πρόβλεψη της πορείας του παιγνιδιού. Τέλος υλοποίησε και ένα μέρος δημιουργίας και γρήγορης (λόγω των B-trees) εκτέλεσης "what-if" σεναρίων για έλεγχο επικίνδυνων εξελίξεων, για την εταιρία, του διαγωνισμού.

- **΄Εργο "ΚΕΝΟ" (Στιγμιαίο Lotto). Χρόνος εκτέλεσης έργου: 1997-1998.**: Ο κ. Σταματίου ήταν ο μόνος σχεδιαστής και προγραμματιστής μίας εφαρμογής γένεσης *κρυπτογραφικά ασφαλών ψευδοτυχαίων αριθμών* που ανέλαβε το ΕΑΙΤΥ για μία ιδιωτική εταιρία υποστήριξης κρατικών παιγνιδιών τύχης και πρόγνωσης αθλητικών γεγονότων. Το λογισμικό δοκιμάστηκε με χρήση διάφορων στατιστικών ελέγχων που υλοποιήθηκαν ειδικά για το σκοπό αυτό και στο τέλος εκδόθηκε πιστοποιητικό τυχαιότητας από τον Διευθυντή του ΕΑΙΤΥ Καθηγητή κ. Π. Σπυράκη. Το λογισμικό υλοποιούσε τις γεννήτριες BBS (από τους Blum-Blum-Shub, γεννήτρια που βασίζεται στα τετραγωνικά υπόλοιπα) και RSA (από τους Rivest-Shamir-Adleman, που βασίζεται στη συνάρτηση κρυπτογράφησης RSA) σε συνδυασμό της εξόδου τους με τον αλγόριθμο M του Knuth και αποτελούταν από μέρη που έτρεχαν σε UNIX, DOS, VAX και επικοινωνούσαν μέσω TCP/IP για να ανταλάξουν πληροφορίες ηλεκτρονικής υπογραφής και να τροφοδοτούν με ψευδοτυχαίους αριθμούς τον κεντρικό υπολογιστή της εταιρίας.

Κεφάλαια σε βιβλία

- C. Katsimpiri, P.E. Nastou, P.M. Pardalos, and Y.C. Stamatiou. The Ubiquitous Lambert Function and its Classes in Sciences and Engineering. In *P.M. Pardalos and T.M. Rassias (eds.) Contributions in Mathematics and Engineering, In Honor of Constantin Caratheodory*. Springer, Expected in 2016.

- P.E. Nastou, D. Nastouli, P.M. Pardalos, and Y.C. Stamatiou. A Method for Creating Private and Anonymous Digital Territories using Attribute-Based Credential Technologies. In *N. Darras and M.T. Rassias (eds.) Computation, Cryptography, and Network Security*, pp. 399-412, Springer 2015.

- P.E. Nastou, P. Pardalos, P. Spirakis, and Y.C. Stamatiou. On the Design of Agent Agreement Protocol Using Linear Error-Correcting Codes. Chapter in book titled *Applications of Mathematics and Informatics to Science and Engineering*, Series: Springer Optimization and Its Applications, Vol. 91, Springer-Verlag, 2014.

- E. Konstantinou, P. Nastou, Y. Stamatiou, C. Zaroliagis, Securing Embedded Computing Systems through Elliptic Curve Cryptography, Encyclopedia of Embedded Computing Systems. IGI Global, Chapter 20, pp. 402-419, 2013.

- Π. Νάστου, Π. Σπυράκης, και Γ. Σταματίου, *Πρώτοι αριθμοί, διακριτός λογάριθμος, και παραγοντοποίηση: Θεωρία και Αλγόριθμοι*, κεφάλαιο σε συλλογικό τόμο με τίτλο *Σύγχρονη Κρυπτογραφία: Θεωρία και Εφαρμογές*, με επιμελητές του τόμου τους Καθηγητές Mike Burmester, Στέφανο Γκρίτζαλη, Σωκράτη Κάτσικα, και Βασίλειο Χρυσικόπουλο, Εκδόσεις Παπασωτηρίου, 2010.

- Χ. Μανωλόπουλος, Δ. Σοφοτάσιος, Π. Σπυράκης, και Γ. Σταματίου, Ζητήματα προστασίας της ιδιωτικότητας σε συστήματα Ηλεκτρονικής Ψηφοφορίας. Κεφάλαιο σε συλλογικό τόμο με τίτλο *Προστασία της Ιδιωτικότητας στις Τεχνολογίες Πληροφορικής και Επικοινωνιών: Τεχνικά και Νομικά Θέματα*, Εκδόσεις Παπασωτηρίου, 2010.

- E. Makri and Y.C. Stamatiou, *Deterministic and randomized key pre-distribution schemes for mobile ad-hoc networks: foundations and example constructions*. Chapter 4 in book titled *From Problem Toward Solution: Wireless Sensor Networks Security*, Nova Science Publishers, pp. 211-233, 2009.

- E.C. Laskari, G.C. Meletiou, Y.C. Stamatiou, and M.N. Vrahatis, *Cryptography and Cryptanalysis through Computational Intelligence*, included in a book title Computational Intelligence in Information Assurance and Security, bublished by Nova Science Publishers.

- D. Koukopoulos and Y.C. Stamatiou, *Digital Audio Watermarking Techniques for MP3 Audio Files*. Chapter included in a book titled *Digital Audio Watermarking Techniques and Technologies: Applications and Benchmarking*, IGI Global, pp. 205-228, 2008.

- P.E. Nastou and Y.C. Stamatiou, *An on chip, CAST-128 based block cipher with dynamically reconfigurable s-boxes generated in parallel*, in book titled *Embedded Cryptographic Hardware: Methodologies & Architectures*, Nova Science Publishers, NY, USA, pp. 135-152, 2004.

- Ketil Stølen, Folker den Braber, Theo Dimitrakos, Rune Fredriksen, Bjørn Axel Gran, Siv-Hilde Houmb, Yannis C. Stamatiou, and Jan Øyvind Aagedal. Model-based risk assessment in a component-based software engineering process using the CORAS approach to identify security risks. Chapter 11 in book titled *Business CBSE* (Component-Based Software Engineering), pp. 189-207, Kluwer Academic Publishers, 2003.

- B.B. Boutsinas, Y.C. Stamatiou, and G. Pavlides, *Massively Parallel Support for Nonmonotonic Reasoning*, *Parallel Processing for AI 3*, James Geller, Hiroaki Kitano and Christian Suttner (eds.), Elsevier Publishers, pp. 41-66, 1997.

Συγγραφή βιβλίων

1. Σ. Ρεντούλης και Γ.Κ. Σταματίου, *ΟΥΤΟΠΙΑ: Ένα υπολογιστικό περιβάλλον ανάπτυξης και μελέτης τεχνητής ζωής*, υπό έκδοση CTI Press/Νέα Γράμματα, αναμενόμενο το 2009.

2. Γ.Κ. Σταματίου, *Αρχές Συνδυαστικής*, Εκδόσεις Ελληνικού Ανοικτού Πανεπιστημίου, 2005.

3. Π. Νάστου, Π. Σπυράκης, και Γ.Κ. Σταματίου, *Σύγχρονη κρυπτογραφία: Μια ξέγνοιαστη διαδρομή στα μονοπάτια της*, CTI Press/Νέα Γράμματα, 2004.

4. Χ. Μπούρας, Λ.Μ. Κυρούσης, Π. Σπυράκης, και Γ.Κ. Σταματίου, *Εισαγωγή στους Γράφους: Θεωρία, Προβλήματα και Λύσεις*, Εκδόσεις GUTENBERG, ISBN 960-01-0815-3, 1999.

Συγγραφή σημειώσεων για διεθνή επιστημονικά σχολεία

Yannis Stamatiou, *Threshold Phenomena: The Computer Scientist's Point of View*, σημειώσεις 50 σελίδων για τη διδασκαλία της ενότητας *Κατωφλικά Φαινόμενα στην Επιστήμη των Υπολογιστών* στο *The LOGIC AND INTERACTION Programme*, 28 Ιανουαρίου - 1 Μαρτίου 2002, που έλαβε χώρα στη Μασαλλία, Γαλλία, και συνδιοργανώθηκε από το *Institut de Mathematiques de Luminy (IML)* και το *Laboratoire d' Informatique Fondamentale de Marseille (LIF)*.

Ανάπτυξη λογισμικού ανοικτού κώδικα

1. Βιβλιοθήκη υλοποίησης κρυπτογραφικών συστημάτων με βάση τις Ελλειπτικές Καμπύλες. Η βιβλιοθήκη περιλαβάνει κώδικα για τη δημιουργία ελλειπτικών καμπυλών με βάση τη μέθοδο του Μιγαδικού Πολλαπλασιασμού (Complex Multiplication Method), για την εύρεση σημείων επάνω σε αυτές, για την εκτέλεση βασικών αλγεβρικών πράξεων μεταξύ σημείων της καμπύλης καθώς και για τον έλεγχο της κρυπτογραφικής ασφάλειας των καμπυλών αυτών.

   Η βιβλιοθήκη αναπτύχθηκε από κοινού από τον κ. Ζαρολιάγκη, την κ. Κωνσταντίνου και τον κ. Σταματίου. Είναι γραμμένη σε ANSI C και είναι εύκολα μεταφέρσιμη σε οποιοδήποτε υπολογιστικό σύστημα.

   Η βιβλιοθήκη, μαζί με εγχειρίδιο εγκατάστασης και παραδείγματα χρήσης της, είναι διαθέσιμη στην ιστοσελίδα http://www.ceid.upatras.gr/faculty/zaro/software/ecc-lib/

2. Βιβλιοθήκη αυτόματης παραγωγής S-box (substitution box) βασισμένων σε λογικές συναρτήσεις bent. Η βιβλιοθήκη περιλαμβάνει κώδικα για την κατασκευή S-box για ενσωμάτωσή τους σε κρυπταλγόριθμους block με στήλες που αποτελούνται από λογικές συναρτήσεις μέγιστης μη γραμμικότητας, οι οποίες καλούνται bent. Ο κώδικας περιλαμβάνει και διαδικασίες για τον υπολογισμό γραμμικού συνδυασμού λογικών συναρτήσεων, για το γρήγορο υπολογισμό του Walsh-Hadamard μετασχηματισμού, για τον έλεγχο μη γραμμικότητας λογικών συναρτήσεων και s-box καθώς και για τον υπολογισμό ενός αριθμού παραμέτρων χρήσιμων για την την εκτίμηση της ασφάλειας των παραγόμενων S-box.

   Η βιβλιοθήκη έχει αναπτυχθεί από τον κ. Σταματίου στη γλώσσα προγραμματισμού C και σε περιβάλλον Borland C/C++ 5.0 και είναι διαθέσιμη σε κάθε ενδιαφερόμενο.

Διακρίσεις

- Πρώτο βραβείο για το πληροφοριακό σύστημα ύποστήριξης ηλεκτρονικών ψηφοφοριών μεγάλης κλίμακας *ΠΝΥΚΑ* στον πανευρωπαϊκό διαγωνισμό συστημάτων eVoting που έλαβε χώρα στο Bregenz της Αυστρίας τον Αύγουστο του 2008. Ο κ. Σταματίου ήταν κύριος ερευνητής στην ομάδα έργου με σημαντική συμμετοχή στη σχεδίαση και υλοποιήση του συστήματος.

- Βραβείο ERICSSON για το 2006 για την προπτυχιακή εργασία με τίτλο *Υλοποίηση Εξομοιωτή Κάρτας SIM Κινητών Τηλεφώνων και Πειραματισμοί με Κρυπτογραφικές Εφαρμογές*, που εκπονήθηκε από τον κ. Δημήτρη Μενδρινό στο Ελληνικό Ανοικτό Πανεπιστήμιο υπό την επίβλεψη του κ. Σταματίου.

- Best poster award at *Twenty-Third Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing - PODC 2004*.

Ερευνητικές δημοσιεύσεις σε διεθνή περιοδικά με κριτές[1]

1. N. Giovanopoulos, P.E. Nastou, P.M. Pardalos, and Y.C. Stamatiou. A Secret Key Information Hiding in Digital Images Protocol based on Steganographic Methods in Image Frequency Domain. To appear at *International Journal of Applied & Experimental Mathematics, Graphy Publications*, 2017.

2. A.D. Avgerou, P. Nastou, D. Nastouli, P. Pardalos and Y.C. Stamatiou. On the Deployment of Citizens' Privacy Preserving Collective Intelligent eBusiness Models in Smart Cities. *International Journal of Security and Its Applications (IJSIA)*, Vol. 10, No 2, pp. 171-184, February 2016.

   (Εκτεταμένη έκδοση της εργασίας Σ[6].)

3. A.D. Avgerou and Y.C. Stamatiou. Privacy Awareness Diffusion in Social Networks. *IEEE Security & Privacy Journal*, vol.13, no. 6, pp. 44-50, Nov.-Dec. 2015. Also posted at `http://stc-social-networking.ieee.net/featured-articles`, at the site of the Special Technical Community (STC) on Social Networking, as a featured article for December 2015, selected by the editorial board as "interesting and promising" (as stated at the site) article.

4. P.E. Nastou, V. Papadinas, P. Pardalos, and Y.C. Stamatiou. On a new edge function on complete weighted graphs and its application for locating Hamiltonian cycles of small weight. *Optimization Letters*, pp. 1-18, Springer, 2015.

5. C. Manolopoulos, D. Sofotassios, P. Spirakis, and Y.C. Stamatiou. A Framework for Protecting Voters' Privacy in Electronic Voting Procedures. *Journal of Cases on Information Technology (JCIT)*, Vol. 15, No. 2, pp. 1-33, 2013.

6. P.E. Nastou, P. Spirakis, Y.C. Stamatiou and A. Tsiakalos. On the Derivation of a Closed-Form Expression for the Solutions of Generalized Abel Differential Equations. *International Journal of Differential Equations*, Hindawi Press, Volume 2013, June 2013.

7. P.E. Nastou and Y.C. Stamatiou. Distributed Computation of SBoxes with Strong Security Properties. *International Journal of Security and Its Applications*, Vol. 6, No. 2, 2012.

[1] Εκτός από τη δημοσίευση με τους κ. Βουτσινά και κ. Παυλίδη, έχει συμμετάσχει μόνο σε εργασίες με αλφαβητική αναγραφή των ονομάτων.

8. P. Nastou, Y.C. Stamatiou, and A. Tsiakalos. Solving a Class of ODEs Arising in the Analysis of a Computer Security Process using Generalized Hyper-Lambert Functions. *International Journal of Applied Mathematics and Computation*, Vol 4 No. 3, pp. 67-76, 2012.

9. H. Antonopoulou, N. Glinos, and Y. C. Stamatiou. An identity derived from the solution of a class of differential equations for the evolution of a key agreement protocol. *Journal of Discrete Mathematical Sciences & Cryptography*, Taylor & Francis Group and TARU publications, Vol 14, No. 6, pp. 515–520, 2011.

10. P. Kammas, C. Manolopoulos, and Y.C. Stamatiou, Modelling of Long Term Viability of Financial Agents Based on their Short Range Economic Behaviour. Global Business & Economics Anthology Volume II, Issue 1, pp. 159-171, December 2011.

11. D. Kalles, A. Papagelis, Y.C. Stamatiou: Consolidating a Heuristic for Incremental Decision Tree Learning through asymptotic Analysis. International Journal on Artificial Intelligence Tools 20(1): 29-52 (2011).

12. P. Kammas, T. Komninos, and Y.C. Stamatiou, Queuing theory based models for studying intrusion evolution and elimination in computer networks, Journal of Information Assurance and Security (JIAS), Special Issue on Intrusion and Malware Detection, Volume 4, Issue 3, pp. 200-208, June 2009.

    (Σύμπτυξη των εργασιών Σ[27] και Σ[23].)

13. E. Konstantinou, A. Kontogeorgis, Y.C. Stamatiou, and C.D. Zaroliagis: On the Efficient Generation of Prime-Order Elliptic Curves. *Journal of Cryptology* 23(3): 477-503 (2010).

14. E. Makri and Y.C. Stamatiou. An Interactive, Similarity Increasing Algorithm for Random Strings with Applications to Key Agreement in ad hoc Networks. *Studies in Applied Mathematics*. Vol. 121, No. 2, pp. 141-155, 2008.

    (Εκτεταμένη έκδοση της εργασίας Σ[36].)

15. N. Glinos and Y.C. Stamatiou. On the equivalence between random graph models. *Journal of Discrete Mathematical Science & Cryptography*, Vol. 11, No. 4, pp. 405-419, Taylor & Francis Group and TARU publications, 2008.

16. A.C. Kaporis, L.M. Kirousis, Y.C. Stamatiou, M. Vamvakari, and M. Zito, The unsatisfiability threshold revisited, *Discrete Applied Mathematics*, Vol. 155, pp. 1525-1538, Elsevier, 2007.

17. E.C. Laskari, G.C. Meletiou, Y.C. Stamatiou, and M.N. Vrahatis. Cryptography and Cryptanalysis Through Computational Intelligence. Studies in Computational Intelligence (SCI), Vol. 57, Springer-Verlag, pp. 1–49, 2007.

18. E. Konstantinou, Y.C. Stamatiou, and C. Zaroliagis, Efficient generation of secure elliptic curves, *International Journal of Information Security*, 6(1): 47-63, 2007.

    (Εκτεταμένη έκδοση της εργασίας Σ[40].)

19. E.C. Laskari, G.C. Meletiou, Y.C. Stamatiou, D.K. Tasoulis, and M.N. Vrahatis, Assessing the Effectiveness of Artificial Neural Networks on Problems Related to Elliptic Curve Cryptography, Mathematical and Computer Modelling, Volume 46, Issues 1-2, 174-179, Elsevier, 2007.

20. E.C. Laskari, G.C. Meletiou, Y.C. Stamatiou, and M.N. Vrahatis, Applying evolutionary computation methods for the cryptanalysis of Feistel ciphers, *Applied Mathematics and Computation* 184(1): 63-72, Elsevier, 2007.

21. T. Komninos, P. Spirakis, Y.C. Stamatiou, G. Vavitsas. A worm propagation model based on scale free network structures and people's email acquaintance profiles. *IJCSNS - International Journal of Computer Science and Network Security*, Vol. 7 No. 2 pp. 308-315, 2007.

22. S. Antonopoulou, Y.C. Stamatiou, and M. Vamvakari. An asymptotic expansion for the q-binomial series using singularity analysis for generating functions. *Journal of Discrete Mathematical Sciences & Cryptography*, Vol. 10, No. 3, pp. 313-328, 2007.

    (Εκτεταμένη έκδοση της εργασίας Σ[63].)

23. L.M. Kirousis, Y.C. Stamatiou, and M. Zito, The unsatisfiability threshold conjecture: the techniques behind upper bound improvements, *Computational Complexity and Statistical Physics*, Oxford University, pages 159-178, 2006.

    (Εκτεταμένη έκδοση της εργασίας Σ[47].)

24. A. Kaporis, L. Kirousis, and Y.C. Stamatiou, Proving conditional randomness using the Principle of Deferred Decisions, *Computational Complexity and Statistical Physics*, Oxford University Press, New York, 179-194, 2006.

    (Εκτεταμένη έκδοση της εργασίας Σ[48].)

25. E.C. Laskari, G.C. Meletiou, Y.C. Stamatiou and M.N. Vrahatis, Evolutionary computation based cryptanalysis: A first study, *Journal of Nonlinear Analysis: Theory, Methods & Applications*, Volume 63, Issues 5-7, e823-e830, Elsevier, 2005.

26. D. Koukopoulos and Y.C. Stamatiou, A Watermarking Scheme for MP3 Audio Files, International Journal of Signal Processing (IJSP), Vol. 2, No. 3, pp. 206-213, 2005.

27. P.E. Nastou and Y.C. Stamatiou, An on chip, CAST-128 based block cipher with dynamically reconfigurable s-boxes generated in parallel. Volume on *Embedded Cryptographic Hardware: Methodologies & Architectures*, Nova Publishers, 135-152, 2004.

    (Σύμπτυξη και επέκταση των εργασιών Σ[49] και Σ[51].)

28. L.M. Kirousis, E. Kranakis, D. Krizanc, and Y.C. Stamatiou, Locating Information with Uncertainty in Fully Interconnected Networks: The Case of Non-Distributed Memory, *NETWORKS* **42**, Issue 3, 169-180, 2003.

    (Εκτεταμένη έκδοση της εργασίας Σ[60].)

29. Y.C. Stamatiou, Threshold Phenomena: The Computer Scientist's Viewpoint, *EATCS (European Association of Theoretical Computer Science) Bulletin* **80**, 199-234, June 2003.

30. S. Armeni, D. Christodoulakis, I. Kostopoulos, Y.C. Stamatiou, and M. Xenos, Secure information hiding based on computationally intractable problems. *Journal of Discrete Mathematical Sciences & Cryptography* Vol. 6, No. 1, 21-33, April 2003.

    (Εκτεταμένη έκδοση της εργασίας Σ[52].)

31. D. Achlioptas, L.M. Kirousis, E. Kranakis, D. Krizanc, M. S.O. Molloy, and Y.C. Stamatiou, Random Constraint Satisfaction: A More Accurate Picture, *Constraints* **6**, 329-344, 2001.

    (Εκτεταμένη έκδοση της εργασίας Σ[65].)

32. L.M. Kirousis, Y.C. Stamatiou, and M. Vamvakari, Upper Bounds and Asymptotics for the q-binomial Coefficients, *Studies in Applied Mathematics* **107**, 43-62, 2001.

33. A.C. Kaporis, L.M. Kirousis, E. Kranakis, D. Krizanc, Y.C. Stamatiou and E.C. Stavropoulos, Locating Information with Uncertainty in Fully Interconnected Networks with Applications to World Wide Web Information Retrieval, *Computer Journal* **44**, 221-229, 2001.

34. N.D. Dendris, L.M. Kirousis, Y.C. Stamatiou, and D.M. Thilikos, On Parallel Partial Solutions and Approximation Schemes for Local Consistency in Networks of Constraints, *Constraints* **5**, 251-273, 2000.

    (Εκτεταμένη έκδοση της εργασίας Σ[66].)

35. S. Janson, Y.C. Stamatiou, and M. Vamvakari, Bounding the Unsatisfiability Threshold of Random 3-SAT, *Random Structures and Algorithms* **17**, 103-116, 2000.

36. A.C. Kaporis, L.M. Kirousis, and Y.C. Stamatiou, A note on the non-colorability threshold of a random graph, *Electronic Journal of Combinatorics* **7**, #R29, 2000.

37. Y.C. Stamatiou, Phase Transitions in Mathematics and in Physics: Two Faces of the same coin?, *Carleton Journal of Computer Science* **3**, 57-69, 1999.

38. L.M. Kirousis, E. Kranakis, D. Krizanc, and Y.C. Stamatiou, Approximating the Unsatisfiability Threshold of Random Formulas, *Random Structures and Algorithms* **12**, 253-269, 1998.

Ερευνητικές δημοσιεύσεις σε διεθνή συνέδρια με κριτές

1. J. Bothos. A. Zalonis, V. Vlachos, Y. Stamatiou, A. Madhja, S. Thomopoulos, and S. Nikoletseas. Probing Digital Black Markets: A New Approach to Cybersecurity. In Proc. 4th International Conference on Operation Planning, Technological Innovations and Mathematical Applications (OPTIMA), 2017.

2. Vasileios Vlachos, Yannis C. Stamatiou, Adelina Madhja, Sotiris E. Nikoletseas: Privacy Flag: A crowdsourcing platform for reporting and managing privacy and security risks. PCI 2017: 27:1-27:4

3. Madhja , S.E. Nikoletseas, Y.C. Stamatiou, D. Tsolovos and V. Vlachos, "Crowd Sourcing Based Privacy Threat Analysis and Alerting", In 3rd International Conference on Cryptography, Cyber Security and Information Warface (CryCybIW), Hellenic Military Academy, 26-27 May 2016

4. A.D. Avgerou, P. Nastou, and Y.C. Stamatiou. Innovative Applications and Services Based on Privacy Enhanced Distributed Computations on IoT Devices. *18th IEEE Conference on Business Informatics (CBI 2016)*, 29 Aug. - Sept., 2016.

5. C. Makris, K. Patikas, and Y.C. Stamatiou. Increasing trust towards eCommerce: Privacy Enhancing Technologies against Price Discrimination. In *Proc. 13th International Conference on Web Information Systems and Technologies (WEBIST 2016)*, 2016.

6. A.D. Avgerou, P. Nastou, D. Nastouli, P. Pardalos and Y.C. Stamatiou. Adopting an ABCs Authentication Framework for Collective Intelligent eBusiness Models in Smart Cities. In *Proc. 8th International Conference on Security Technology (SecTech 2015)*, 2015.

7. K. Ispoglou, C. Makris, Y.C. Stamatiou, E.C. Stavropoulos, A.K. Tsakalidis, V. Iosifidis. Partial Order Preserving Encryption Search Trees. In *Proc. 26th International Conference on Database and Expert Systems Applications (DEXA 2015)*, pp. 49-56, Lecture Notes in Computer Science, Springer, 2015.

8. C. Makris, Y. Plegas, Y.C. Stamatiou, E.C. Stavropoulos, and A.K. Tsakalidis. Reducing Redundant Information in Search Results Employing Approximation Algorithms. In *Proc. 26th International Conference on Database and Expert Systems Applications (DEXA 2014)*, pp. 240-247, Lecture Notes in Computer Science, Springer, 2014.

9. Z. Benenson, A. Girard, I. Krontiris, V. Liagkou, K. Rannenberg, and Y. Stamatiou. User Acceptance of Privacy-ABCs: An Exploratory Study. In *Proc. 2nd International Conference on Human Aspects of Information Security, Privacy, and Trust*, pp. 375-386, Springer, 2014.

10. P. Spirakis and Y.C. Stamatiou. A user-centric, privacy respecting perspective for studying and managing the "Digital-Self". In *Proc. 9th International IFIP Summer School on Privacy and Identity Management for the Future Internet in the Age of Globalisation*. Springer, 2014.

11. Y.C. Stamatiou. Privacy Attribute Based Credentials (Privacy-ABCs): advancing privacy-preserving e-participation in the education sector. *Proceedings of the 8th International IFIP Summer School on Privacy and Identity Management for Emerging Services and Technologies*, pp. 64-76, Springer Verlag, 2014,

12. Z. Benenson, I. Krontiris, V. Liagkou, K. Rannenberg, A. Schopf, D. Schroder, and Y. Stamatiou. Understanding and Using Anonymous Credentials. *9th Symposium on Usable Privacy and Security (SOUPS 2013)*. Electronic proceedings.

13. P. Spirakis and Y, Stamatiou. Attribute Based Credentials towards refined public consultation results and effective eGovernance. In *Proc. Cyber Security Privacy EU FORUM and Trust in the Digital World 2013 collection of research papers*, pp. 115 - 126, LNCS, Springer Verlag, 2013.

14. Panayotis E. Nastou, Paul Spirakis, Yannis Stamatiou and Christina Vichou. On the Design of Agent Agreement Protocol using Linear Error-Correcting Codes. In *Proc. 4th IEEE International Conference on Information, Intelligence, Systems and Applications (IISA 2013)*. IEEE, pp. 1-6, 2013.

15. V. Liagkou, G. Metakides, A. Pyrgelis, C. Raptopoulos, P. Spirakis, and Y. Stamatiou. Privacy preserving course evaluations in Greek higher education institutes: an e-Participation case study with the empowerment of Attribute Based Credentials. *Annual Privacy Forum 2012*. Electronic proceedings.

16. P. Kotsopoulos and Y. Stamatiou. Uncovering Mobile Phone Users' Malicious Activities Using Open Source Tools. In *Proc. IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*. IEEE, pp. 927-933, 2012.

17. P. E. Nastou, Y. C. Stamatiou and A. Tsiakalos. The Solution of a Differential Equation Describing the Evolution of a Key Agreement Protocol. In *Proc. 16th EUROPMENT International Conference on Applied Mathematics (EUROSIAM 2011)*. Electronic proceedings by the European Society for Applied Sciences and Development (EURORMENT), 2011.

18. P.E. Nastou and Y.C. Stamatiou. A Distributed, Parametric Platform for Constructing Secure SBoxes in Block Cipher Designs. In *Proc. Security Technology - International Conference (SecTech), Communications in Computer and Information Science Volume 259*, Springer-Verlag, pp. 155-166, 2011.

19. G. C. Meletiou, Y.C. Stamatiou, and A. Tsiakalos. Lower Bounds for Interpolating Polynomials for Square Roots of the Elliptic Curve Discrete Logarithm. 5th International Conference on Information Security and Assurance (ISA 2011). LNCS, Springer Verlag, pp. 177-187, 2011.

20. I. Chatzigiannakis, A. Pyrgelis, P.G. Spirakis, and Y.C. Stamatiou. Elliptic Curve Based Zero Knowledge Proofs and their Applicability on Resource Constrained Devices. In *Proc. EEE 8th International Conference on Mobile Adhoc and Sensor Systems, MASS 2011, Workshop: Wireless and Sensor Network Security Workshop (WSNS 2011)*. IEEE, pp. 715-720, 2011.

21. P. Spirakis and Y.C. Stamatiou, *Kolmogorov complexity arguments in propositional logic*, in *Proc. 7th Panhellenic Logic Symposium (PLS7) (with international participation)*, 2009. Electronic proceedings.

22. V. Liagkou, P. Spirakis, and Y.C. Stamatiou. Can formalism alone provide an answer to the quest of a viable definition of trust in the WWW society? In *Proc. 3rd International Conference on e-Democracy (e-Democracy 2009)*. Springer-Verlag, pp. 199-208, 2009.

23. P. Kammas, T. Komninos, and Y.C. Stamatiou. Modeling the co-evololution DNS worms and anti-worms in IPv6 networks. In *Proc. 5th International Conference on Information Assurance and Security (IAS 09)*, IEEE, pp. 171 - 174, 2009.

24. P. Papaioannou, P. Nastou, Y.C. Stamatiou, and C. Zaroliagis, Secure Elliptic Curve Generation and Key Establishment on a 802.11 WLAN Embedded Device. In Proc. *9th International Symposium on Autonomous Decentralized Systems (ISADS 2009)*, IEEE, pp. 41-48, 2009.

25. V. Papadinas and Y.C. Stamatiou, Geometric approaches for creating low power, low interference connectivity patterns in static, structureless sensor networks. In *Proc. First International Workshop on Autonomous Embedded Systems and Networking (AESN 2009)*, a workshop of ISADS (International Symposium on Autonomous Decentralized Systems), IEEE, pp. 237-242, 2009.

26. C. Manolopoulos, P. Nakou, A. Panagiotaki, D. Sofotasios, P. Spirakis, and Y.C. Stamatiou. A step-wise refinement approach for enhancing eVoting acceptance. In *Proc. 2nd Int. Conf. on Theory and Practice of Electronic Governance (ICEGOV 2008)*, ACM, pp. 275-280, 2008.

27. P. Kammas, T. Komninos, and Y.C. Stamatiou. A queuing theory based model for studying intrusion evolution and elimination in computer networks, In *Proc. 4th International Conference on Information Assurance and Security (IAS 2008)*, IEEE, pp. 167 - 171, 2008.

28. C. Manolopoulos, A. Panagiotaki, D. Sofotasios, and Y.C. Stamatiou, Experience and Benefits from the application of a Formal Risk Assessment Framework in the Evoting domain. *In Proc. 7th International Conference on eGovernment (EGOV 2008)*, pp. 205-211, Trauner-Verlag, 2008.

29. Y.C. Stamatiou, The theoretical analysis of an agreement protocol using Lambert functions, presented at the 2008 International Workshop on Applied Probability. Acceptet for presentation at the Invited Session with title *Discrete distributions and asymptotic behaviour*, International Workshop on Applied Probability (IWAP 2008). Electronic proceedings, 2008.

30. N. Glinos, Y.C. Stamatiou, and M. Vavakari, A statistical/algorithmic framework for modeling fixed odds games, accepted for presentation at the *17th IASTED International Conference on Applied Simulation and Modelling (ASM 2008)*, IASTED publications, pp. 59-64, 2008.

31. A. Antoniou, C. Korakas, C. Manolopoulos, A. Panagiotaki, D. Sofotassios, G. Spirakis, Y.C. Stamatiou. A Trust-Centered Approach for Building E-Voting Systems. in *Proc. 6th International Conference on eGovernment (EGOV 2007)*, Lecture Notes in Computer Science, Springer-Verlag, pp. 366-377, 2007.

32. V. Liagkou, E. Makri, P. Spirakis, and Y.C. Stamatiou, The Digital Territory as a complex system of interacting agents, emergent properties and technologies, presented as a short paper at the European Conference on Complex Systems ECCS 2007. Electronic proceedings, 2007.

33. V. Liagkou, E. Makri, P. Spirakis, and Y.C. Stamatiou. Trust in global computing systems as a limit property emerging from short range random interactions. In *Proc. Second International Conference on Availability, Reliability and Security (ARES 2007, The International Dependability Conference)*, IEEE, pp. 741-748, 2007.

34. T. Komninos, Y. C. Stamatiou, and G. Vavitsas. A Worm Propagation Model Based on People's Email Acquaintance Profiles. In *Proc. 2nd international Workshop on Internet & Network Economics (WINE 2006)*. Lecture Notes in Computer Science, Springer Verlag, pp. 343-352, 2006.

35. E. Makri and Y.C. Stamatiou, Deterministic Key Pre-distribution Schemes for Mobile Ad-Hoc Networks based on Set Systems with Limited Intersection Sizes. In *Proc. 2nd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'06)* in the context of the IEEE 3rd International Conference on Mobile Adhoc and Sensor Systems (MASS 2006). IEEE, pp. 833-838, 2006.

36. E. Makri and Y.C. Stamatiou, Distributively Increasing the Percentage of Similarities Between Strings with Applications to Key Agreement, in *Proc. 5th International Conference on AD-HOC Networks & Wireless (ADHOC-NOW 2006)*, pp. 211-223, Springer Verlag, 2006.

37. V. Liagkou, E. Makri, P. Spirakis, and Y.C. Stamatiou. The threshold behaviour of the fixed radius random graph model and applications to the key management problem of sensor networks. In *Proc. 2nd International Workshop on Algorithmic Aspects of Wireless Sensor Networks (ALGOSENSORS 2006)*, pp. 130-139, Springer Verlag, 2006.

38. E. Konstantinou, V. Liagkou, P.G. Spirakis, Y.C. Stamatiou, M. Yung, Trust Engineering: From Requirements to System Design and Maintenance - A Working National Lottery System Experience, in *Proc. 8th International Security Conference (ISC 2005)*, pp. 44-58, Springer-Verlag, 2005.

39. Dimitrios Koukopoulos and Yannis C. Stamatiou. An Efficient Watermarking Method for MP3 Audio Files. In *Proc. International Enformatica Conference (IEC 2005)*, pp. 154-159, 2005.

40. E. Konstantinou, A. Kontogeorgis, Y.C. Stamatiou, and C. Zaroliagis. Generating Prime Order Elliptic Curves Difficulties and Efficiency Considerations. In *Proc. 7th International Conference on Information Security & Cryptography (ICISC 2004)*. Springer-Verlag, pp. 261-278, 2005.

41. T. Komninos, P. Spirakis, Y.C. Stamatiou, E. Valeontis, H. Yannakopoulos, A Software Tool for Distributed Intrusion Detection in Computer Networks, *best poster award at Twenty-Third Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing PODC 2004*.

42. E. Konstantinou, Y.C. Stamatiou, and C. Zaroliagis, On the Use of Weber Polynomials in Elliptic Curve Cryptography, In *Proc. Public Key Infrastructure: First European PKI Workshop, Research and Applications (EURO-PKI 2004)*. Springer Verlag, pp. 335-349, 2005.

43. E. Konstantinou, V. Liagkou, P. Spirakis, Y.C. Stamatiou, and M. Yung. Electronic National Lotteries. In *Proc. 8th International Conference on Financial Cryptography (FC 2004)*. Springer Verlag, pp. 147-163, 2004.

44. E. Konstantinou, Y.C. Stamatiou, and C. Zaroliagis. On the construction of prime order Elliptic Curves. In *Proc. 4th International Conference on Cryptology in India (INDOCRYPT 2003)*, Springer Verlag, pp. 309-322, 2003.

45. E. Konstantinou, Y.C. Stamatiou, and C. Zaroliagis. On the efficient generation of Elliptic Curves over Prime Fields. In *Proc. 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002)*, B.S. Kaliski Jr., C.K. Koç, C. Paar (eds.). Springer Verlag, pp. 333-348, 2002.

46. E. Konstantinou, Y.C. Stamatiou, and C. Zaroliagis. A software library for Elliptic Curve cryptography. In *Proc. 10th European Symposium on Algorithms (ESA 2002), Engineering and Applications track*. Springer Verlag, pp. 625-636, 2002.

47. L.M. Kirousis, Y.C. Stamatiou, and M. Zito, The unsatisfiability threshold conjecture: the techniques behind upper bound improvements. Presented at the *Phase Transitions and Algorithmic Complexity* Workshop that was organized from June 3 to June 5 2002 by the Institute for Pure and Applied Mathematics, University of California, Los Angeles.

48. A.C. Kaporis, L.M. Kirousis, and Y.C. Stamatiou, Proving conditional randomness using the Principle of Deferred Decisions. Presented at the *Phase Transitions and Algorithmic Complexity* workshop that was organized from June 3 to June 5 2002 by the Institute for Pure and Applied Mathematics, University of California, Los Angeles.

49. P. Nastou and Y.C. Stamatiou, Enhancing the security of block ciphers with the aid of parallel substitution box construction. Accepted at *First International Workshop on Assurance in Distributed Systems and Networks (ADSN)*, pp. 29-34, IEEE Computer Society, 2002.

50. D. Koukopoulos and Y.C. Stamatiou, A Real-Time Compressed-Domain Watermarking Scheme for Mpeg Audio Layer 3. *Watermarking 2002*, March 2002.

51. P. Nastou and Y.C. Stamatiou, Dynamically modifiable ciphers using a reconfigurable CAST-128 based algorithm on ATMEL's FP*SLIC* reconfigurable FPGA architecture. Presented at the *9th Reconfigurable Architectures Workshop (RAW 2002)*, April 2002. The proceedings will be published by IEEE Computer Society Press. Also, Technical Report TR-01100901, ATMEL HELLAS SA.

52. S. Armeni, D. Christodoulakis, I. Kostopoulos, Y.C. Stamatiou, and M. Xenos, Proving copyright ownership using hard instances of combinatorial intractable problems. In *Proc. 8th Panhellenic Conference in Informatics* (Nicosia, 2002), Y. Manolopoulos and S. Evripidou (eds.), 137-145, Livanis Publications, 2002. Also in *Proc. Advances in Informatics*, Vol. 2563, pp. 262-278, Springer Verlag, 2003.

53. P. Spirakis and Y.C. Stamatiou, *How to prove the possession of a secret without revealing it with applications to person identification*, in *Proc. 1st e-Democracy conference with international participation - Electronic Democracy: Information Society and Citizen's rights*, 2003.

54. Y.C. Stamatiou, E. Henriksen, M.S. Lund, E. Mantzouranis, M. Psarros, E. Skipenes, N. Stathiakis, and K. Stølen, Experiences from using model-based risk assessment to evaluate the security of a telemedicine application, presented at *Telemedicine in Care Delivery (TICD)*, Pisa, Italy, 2002.

55. Y.C. Stamatiou, E. Skipenes, E. Henriksen, N. Stathiakis, A. Sikianakis, E. Charalambous, N. Antonakis, K. Stølen, F. den Braber, M.S. Lundf, K. Papadaki , G. Valvis. The CORAS approach for model-based risk management applied to a telemedicine service. In *Proc. 18th Medical Informatics Europe (MIE 2003)*, St. Malo, France, IOS Press, 206-211, 2003.

56. D. Koukopoulos and Y.C. Stamatiou, A compressed domain watermarking algorithm for Mpeg Layer 3. In *Proc. Multimedia and Security Workshop at ACM Multimedia 2001* (Ottawa, 2001), pp. 7-10, ACM Press, 2001.

57. L.M. Kirousis, Y.C. Stamatiou, and M. Zito, Upper bounds on the satisfiability threshold: A review of the rigorous results. Presented at the *Workshop on Computational Complexity and Statistical Physics*, Santa Fe Institute, 4-6, September 2001.

    Included in a special volume dedicated to threshold phenomena in combinatorics and physics, to be published by the Sante Fe Institute (SFI) publications. The title was changed to *The unsatisfiability threshold conjecture: the techniques behind upper bound improvements*.

58. A.C. Kaporis, L.M. Kirousis, Y.C. Stamatiou, M. Vamvakari, and M. Zito, Coupon Collectors, q-Binomial Coefficients and the Unsatisfiability Threshold. In *Proc. 7th Italian Conference on Theoretical Computer Science (ICTCS 2001)* (Torino 2001), A. Restivo, S. Ronchi della Rocca, and L. Roversi (eds.), pp. 328-338, Springer-Verlag, 2001.

    Είναι μία ανανεωμένη έκδοση της εργασίας με τίτλο *The unsatisfiability threshold revisited*, των ίδιων συγγραφέων, που παρουσιάστηκε στο SAT 2001.

59. A.C. Kaporis, L.M. Kirousis, Y.C. Stamatiou, M. Vamvakari, and M. Zito, The unsatisfiability threshold revisited. It appeared in: *Working Notes of Workshop on Theory and Applications of Satisfiability Testing (SAT 2001), Boston, Massachusetts*, H. Kautz and B. Selman (eds.), pp. 185-194, 2001. Also, in Electronic Notes in Discrete Mathematics H. Kautz and B. Selman (eds.), Vol. 9, Elsevier Science Publishers, 2001. Also in *Journal of Discrete Mathematics*.

60. L.M. Kirousis, E. Kranakis, D. Krizanc, and Y.C. Stamatiou, Locating Information with Uncertainty in Fully Interconnected Networks. In *Proc. 14th International Symposium on Distributed Computing (DISC 2000)*, Vol. 1914 of *Lecture Notes in Computer Science* (Toledo, 2000), M. Herlihy (ed.), pp/ 183-296, Springer-Verlag, 2000.

61. S. Armeni, D. Christodoulakis, I. Kostopoulos, Y.C. Stamatiou, and M. Xenos, A Transparent Watermarking Method for Color Images, *Proceedings of the IEEE first Balkan Conference on Signal Processing, Communications, Circuits and Systems, Istanbul, Turkey, 2000*.

62. P. Bose, R. Dagher, E. Kranakis, D. Krizanc, and Y. C. Stamatiou, Experimental comparison between Location Update and Caching protocols for user tracking in Wireless Networks. In *Proc. 1st International Conference on Software Engineering Applied to Networking & Parallel/Distributed Computing (SNPD 2000)* (Reims, 2000), Hacene Fouchal and Roger Y. Lee (eds.), pp. 189-196, Published by the International Association for Computer and Information Science (ACIS), 2000.

63. Y.C. Stamatiou and M. Vamvakari, An asymptotic expansion for the q-hypergeometric series using singularity analysis for generating functions. Presented at the *Fifth International Symposium on Orthogonal Polynomials, Special Functions and their Applications (OPSFA 1999)* (Patras, 1999), *Book of abstracts*, 84-85, Department of Mathematics, University of Patras, 1999.

64. Y.C. Stamatiou and D.M. Thilikos, Monotonicity and Inert Fugitive Search Games. Presented at the *6th Twente Workshop on Graphs and Combinatorial Optimization* and it appears in *Electronic Notes in Discrete Mathematics*, H.J. Broersma, U. Faigle, C. Hoede and J.L. Hurink (eds.), Vol. 3, Elsevier Science Publishers, 2000.

65. D. Achlioptas, L.M. Kirousis, E. Kranakis, D. Krizanc, M. S.O. Molloy, and Y.C. Stamatiou, Random Constraint Satisfaction: A More Accurate Picture, In *Proc. Third International Conference on Principles and Practice of Constraint Programming (CP 97)* (Schloss Hagenberg, 1997), Vol. 1330 of *Lecture Notes in Computer Science*, pp. 107-120, Springer-Verlag, 1997. Also, in the *Constraints* journal.

66. N.D. Dendris, L.M. Kirousis, Y.C. Stamatiou, and D.M. Thilikos, Partiality and Approximation Schemes for Local Consistency in Networks of Constraints, also in the *Constraints* journal. Επίσης *Proc. of the 15th Conference on the Foundations of Software Technology and Theoretical Computer Science (FST & TCS)* (Bangalore, 1995), P.S. Thiagarajan (ed.), Vol. 1026 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 210-224, 1995.

    Μία συντομευμένη έκδοση της εργασίας αυτής με τίτλο *Partial Arc Consistency* εμφανίστηκε στο συνέδριο *Over-Constrained Systems* (Cassis, 1995), Michael Jampel (ed.), Vol. 1106 of *Lecture Notes in Computer Science*, Springer-Verlag, 229-236, 1996.

67. B.B. Boutsinas, Y.C. Stamatiou, and G. Pavlides, Parallel Reasoning using Weighted Inheritance Networks, *Working Notes, Third International Workshop on Parallel Processing for Artificial Intelligence* (Montreal, 1995), pp. 29-39, 1995.

An expanded version of this work with title *Massively Parallel Support for Nonmonotonic Reasoning*, also appeared in a book dedicated to the application of parallel processing techniques in Artificial Intelligence: *Parallel Processing for AI 3*, James Geller, Hiroaki Kitano and Christian Suttner (eds.), pp. 41-66, Elsevier Publishers, 1997.

68. B.B. Boutsinas and Y.C. Stamatiou, A knowledge-based approach for recognizing polyhedral scenes. In *Proc. 13th IASTED International Conference on Applied Informatics* (Austria 1995), M.H. Hamza (ed.), IASTED publications, pp. 160-163, 1995.

Εργασίες επισκόπησης και παρουσιάσεις

1. Π. Σπυράκης και Γ.Κ. Σταματίου, *Νέες κατευθύνσεις στην Κρυπτογραφία*, παρουσίαση στο Πρώτο Συμπόσιο Πληροφορικής και Επιχειρησιακής Έρευνας των Ελληνικών Ενόπλων Δυνάμεων, Πολεμικό Μουσείο, Αθήνα, 2-3 Νοεμβρίου, 1999.

2. Π. Σπυράκης και Γ.Κ. Σταματίου, *Αποδοτικά πρωτόκολλα για την ανίχνευση κινούμενων ωτακουστών σε δίκτυα υπολογιστών*, παρουσίαση στο Πρώτο Συμπόσιο Πληροφορικής και Επιχειρησιακής Έρευνας των Ελληνικών Ενόπλων Δυνάμεων, Πολεμικό Μουσείο, Αθήνα, 2-3 Νοεμβρίου, 1999. (Ομιλία στηριγμένη σε ερευνητική εργασία των Η. Αντωνοπούλου, Π. Σπυράκη, και Β. Ταμπακά.)

Άλλες συγγραφικές δραστηριότητες

Κρατά με τον Καθηγητή κ. Σπυράκη και τον Δρ. Παναγιώτη Νάστου μία μόνιμη στήλη στο περιοδικό <<Άμυνα και Διπλωματία>> αφιερωμένη σε θέματα κρυπτογραφίας και κρυπτανάλυσης.