Curriculum Vitae

Yannis C. Stamatiou

Personal Info

Name:	Yannis
Surname:	Stamatiou
Parents' names:	Costas and Maria
Born:	17 January 1968 in Volos, Greece
Nationality:	Greek
Marital Status:	Married to Jenny Georgiou-Fotinis Theodosopoulou, with one child
Address:	University of Patras, Rio, Patras, Greece Dept. of Business Administration
Phone:	(+30) 26340 32 476 (home)
email:	stamatiu@ceid.upatras.gr

Education

He graduated from the University of Patras, Department of Computer Engineering and Informatics, with a grade of 8.86/10 (June 1990). In June 1991, he started graduate studies at the same department under a government scholarship, working towards a PhD in Parallel Computation and Parallel Complexity Theory, which he completed in December 1997. In 1999, he received a Certificate of Postgraduate Studies on *Open and Distant Learning Educational Systems* from the Greek Open University with a grade of 9.10/10.

Diploma thesis

His diploma thesis was completed in 1990 under the supervision of Professor Athanasios Tsakalidis and it was titled

"Top-down Rebalancing of Red-Black Trees and their Behaviour in Parallel Processing Environments"

Doctoral thesis

In December 1997 he successfully defended his doctoral thesis that was completed under the supervision of Professor Lefteris Kirousis and it was titled

"Theory and Applications of the Constraint Satisfaction Problem
Distributed Environment-Parallel and Randomized Algorithms-Nonmonotonic Reasoning."

In February 1998 he was officially awarded the PhD degree.

Postdoctoral fellowship

From September 1998 to September 1999 he was a postdoctoral fellow at the Computer Science Department of Carleton University, Ottawa, in Canada. He was jointly supported by the Greek Ministry of National Economy through a NATO scholarship for conducting postdoctoral studies (contract number 106384/ΔOO 1222/2-7-98) and the MITACS project CANCCOM (Complex Adaptive Networks for Computing and Communication). During his stay he conducted research work and taught two courses on Systems Programming using C++.

Invitations for research presentation

- December 1993: Visitor at the university of Karlsruhe, Germany, for a week. He presented his research work on Constraint Satisfaction Problems.
- December 1996: Visitor at Max-Planck-Institute für Informatik, Germany, for 10 days. He presented his research work on the computational complexity of solving in parallel Constraint Satisfaction Problems as well as his work on partiality schemes for enforcing local consistency.
- July 2001: Invited speaker at the *Third Panhellenic Logic Symposium* in Anogia, Crete, for a talk on the *Constraint Satisfaction Problem*, its theoretical aspects and its applications in various scientific disciplines.
- August 2002: Invited speaker at workshop *Random Structures* that was organized at the saac Newton Institute for Mathematical Sciences, Cambridge, with talk's subject the preservation of randomness in algorithms handling ranfom combinatorial sturctures.
- 2002: Invited speaker at the University of Liverpool, Dept. of Computer Science, for a talk on threshold phenomena in Computer Science and Physics.
- Invited speaker at the *1st AIT Annual Workshop on PRactical AspeCts of SEcurity - PRACSE 2006* Athens Information Technology (AIT) center in Athens from 16/6/2006 to 17/6/2006. The titles of the talks were:
  - *AUTHENTICATION PROTOCOLS:* Notions of Authentication, Basic techniques and Typical Attacks.
  - *EVALUATION OF REAL WORLD PROTOCOL STANDARDS:* IPSec, SSH, SSL, Kerberos.

Conference activity

- Program committee member at the *13th International Conference on Cryptology and Network Security (CANS-2014).*
- Program committee member at the 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.

- Program committee member at the *Fourth International Conference on Technical and Legal Aspects of the e-Society 2012 (CYBERLAWS 2013).*

- Program committee member at the *Sixth International Conference on Sensor Technologies and Applications - SENSORCOMM 2012.*

- Program committee member at the *Third International Conference on Technical and Legal Aspects of the e-Society 2012 (CYBERLAWS 2012).*

- Program committee member at the *IEEE Symposium on Wireless Technology & Applications 2012 (ISWTA 2012).*

- Program committee member at the *International Symposium on Foundation of Open Source Intelligence and Security Informatics, 2012 (FOSINT-SI 2012).*

- Program committee member at the *The IADIS e-Commerce 2012 conference.*

- Program committee member at the *European Intelligence and Security Informatics Conference (EISIC 2012).*

- Program committee member at the *7th IEEE International Workshop on Wireless and Sensor Networks Security (IEEE WSNS 2011).*

- Program committee member at the *7th European Conference on Computer Network Defense* (EC2ND 2011).

- Program committee member at the *The 5th International Conference on Information Security and Assurance* (ISA 2011).

- Program committee member at the *7th International Conference on Global Security, Safety & Sustainability (ICGS^{3}11).*

- Program committee member at the *The IADIS e-Commerce 2011 conference.*

- Program committee member at the *Second International Conference on Security-enriched Urban Computing and Smart Grid (SUComS)* 2011.

- Program committee member at the *4th IFIP International Conference on New Technologies, Mobility and Security (NTMS 2011)*, Security Track.

- Program committee member at the *The Sixth IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'10)*

- Program committee member at the *First International Conference on Security-enriched Urban Computing and Smart Grid (SUComS)* 2010.

- Program committee member at the *Webit eGov Summit*, 2010, organized by the eAcademy, eEducation Institute of Bulgaria.

- Program committee member at the *APSIPA (Asia-Pacific Signal and Information Processing Association) Annual Summit and Conference 2010.*

- Program committee member at the *Seventh European Workshop on Public Key Services, Applications and Infrastructures* (EUROPKI 2010).

- Program committee member at the *15th European Symposium on Research in Computer Security* (ESORICS 2010).

- Program committee member at the *The IADIS e-Commerce 2010 conference.*

- Program committee member at the *2nd International Conference on Advanced Science and Technology* (AST 2010).

- Program committee member at the *The 4th International Conference on Information Security and Assurance* (ISA 2010).

- Invited in 2009 as rapporteur in the proposal review process within the 7th EU Framework call for proposals *PHOTONICS.*

- Program committee member at the *International Conference on Information Security and Cryptology (Inscrypt)*, Inscrypt 2009, Inscrypt 2010.

- Program committee member at the *1st International Conference on Sensor Networks Applications, Experimentation and Logistics (SENSAPPEAL 2009).*

- Program committee member at the *2009 International Conference on Security and Cryptography* (SECRYPT 2009).

- Program committee member at the *2009 International Conference on Security Technology (SecTech 2009)*, *2010 International Conference on Security Technology (SecTech 2010).*

- Program committee member at the *4th International Conference on Information Security and Cryptology (Inscrypt 2009).*

- Program committee member at the *Fifth International Conference on Security and Privacy in Communication Networks (SecureComm 2009).*

- Invited twice (2006 and 2007) by the Europoean Union as an expert for reviewing proposals in the field of ICT security.

- Program committee member at the ECAI 2008 Workshop *The Quest for Approximate and Exact Equilibria in Games* (ExCalibur).

- Program committee member at the SECRYPT (International Conference on Security and Cryptography) 2008. SECRYPT is part of ICETE, the *International Joint Conference on e-Business and Telecommunications.*

- Program committee member at the 5th European PKI Workshop (EUROPKI 2008).

- Program committee member at the IADIS Conference on e-Commerce 2007.
- Program committee member at the 6th International Conference on AD-HOC Networks & Wireless (ADHOC-NOW 2006).
- Program committee member at the at Inscrypt (formerly CISC - Conference on Information Security and Cryptology) 2006.
- Program committee member at the 7th International Workshop on Information Security Applications (WISA 2006).
- Program committee member at the 6th International Workshop on Information Security Applications (WISA 2005).
- He is in the Program Committee of the 9th Colloquium on Structural Information and Communication Complexity (SIROCCO 2002).
- Organizing Committee member of the Third Annual European Symposium on Algorithms (ESA '95).
- Organizing Committee member for the 2nd Colloquium on Structural Information and Communication Complexity (SIROCCO '95).

References

- 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.

Book chapters

- E. Konstantinou, P. Nastou, Y. Stamatiou, C. Zaroliagis, Securing Embedded Computing Systems through Elliptic Curve Cryptography, Encyclopedia of Embedded Computing Systems, Mohamed Khalgui, Olfa Mosbahi, Antonio Valentini, (eds), 2012, IGI Global, (to appear).

- P. Nastou, P. Spirakis, and Y.C. Stamatiou, *Prime numbers, discrete logarithms and factorization: Theory and Algorithms*, chapter in the Greek language in a volume titles *Modern Cryptography: Theory and Applications*, edited by Mike Burmester, Stafano Gritzali, Socrates Katsika, and Vasileio Chrysikopoulo, Papasotiriou, 2010.

- P. Kammas, T. Komninos, P. Spirakis, Y.C. Stamatiou, and H. Tsaknakis, *Worm propagation models in Networks: theory and analysis*, In (forthcoming): Pichappan, P. (ed.), Handbook of Research on Threat Management and Information Security: Models for Countering Attacks, Breaches and Intrusions, IGI Global.

- C. Manolopoulos, D. Sofotassios, P. Spirakis, and Y.C. Stamatiou. Privacy protection in eVoting. Invited chapter in the Greek language in a volume titled *Privacy Protection in Information and Communication Technologies: Technical and Legislation issues*, 2009.

- E. Makri and Y.C. Stamatiou, *Deterministic and randomized key pre-distribution schemes for mobile ad-hoc networks: foundations and example constructions*, to appear in a book dedicated to security issues in mobile networks to be published by Nova Science Publishers in 2008.

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

- D. Koukopoulos and Y.C. Stamatiou, *Digital Audio Watermarking Techniques for MP3 Audio Files*, to be included in a book titled "Digital Audio Watermarking Techniques and Technologies: Applications and Benchmarking", to be published by Idea Group in 2007.

- P.E. Nastou and Y.C. Stamatiou, An on chip, CAST-128 based block cipher with dynamically reconfigurable s-boxes generated in parallel. It will appear in 2004 as a chapter in a book dedicated to Embedded Cryptographic Hardware, published by Nova Science Publishers, NY, USA.

- 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: *Business CBSE* (Component-Based Software Engineering), to be published by Kluwer Academic Publishers, 2002

- 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, pages 41–66, 1997.

Textbooks

1. P. Nastou, P. Spirakis, and Y.C. Stamatiou, *Modern cryptography: a leisurely walk*, to be published by CTI-Press, 2003. (In the Greek language.)

2. C. Bouras, L.M. Kirousis, P. Spirakis, and Y.C. Stamatiou, *Introduction to Graphs: Theory, problems and solutions*, published by GUTENBERG Publications in the Greek language, ISBN 960–01–0815–3, 1999. (In the Greek language.)

Notes for international scientific schools

Yannis Stamatiou, *Threshold Phenomena: The Computer Scientist's Point of View*, for a course offered taught by himself in *The LOGIC AND INTERACTION Programme*, 28 January–1 March 2002, that takes place in Marseille, France, coorganized by the *Institut de Mathematiques de Luminy (IML)* and the *Laboratoire d' Informatique Fondamentale de Marseille (LIF).*

Publications in international refereed journals[1]

1. C. Manolopoulos, D. Sofotassios, P. Spirakis, and Y.C. Stamatiou. A Framework for Protecting Voters' Privacy in Electronic Voting Procedures. To appear at *Journal of Cases on Information Technology (JCIT)*, 2013.

2. 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, June 2013.

3. 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.

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

5. 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).

6. 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.

7. E. Konstantinou, A. Kontogiorgis, Y.C. Stamatiou, and C. Zaroliagis, On the Efficient Generation of Prime Order Elliptic Curves, accepted at *Journal of Cryptology*, 2009.

8. 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.

9. C. Manolopoulos, A. Panagiotaki, D. Sofotasios, P. Spirakis, and Y. Stamatiou. The Design, Implementation and Evaluation of an Internet-based eVoting System. *12th Pan-Hellenic Conference on Informatics (PCI 2008)*, 2008.

10. N. Glinos and Y.C. Stamatiou, On the equivalence between random graph models, accepted for publication at *Journal of Discrete Mathematical Science & Cryptography*, TARU publications, 2008.

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

[1] Except the publication with V. Boutsinas and G. Pavlides, he has participated only in publications where coauthors' names are listed in alphabetical order.

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

13. 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.

14. 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.

15. 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*, No. 2, Vol. 7 February 2007.

16. 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*, No. 3, Vol. 10, 313−328, 2007.

17. 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.

18. A. Kaporis, L. Kirousis, and Y.C. Stamatiou, How to prove conditional randomness using the Principle of Deferred Decisions, *Computational Complexity and Statistical Physics*, Oxford University Press, New York, 179−194, 2006.

19. 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.

20. 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.

21. 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.

22. 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.

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

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

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

30. 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.

31. 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.

32. 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.

Publications in refereed conferences

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

2. 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*, Brussels, LNCS, Springer Verlag, expected in 2013.

3. Panayotis E. Nastou, Paul Spirakis, Yannis Stamatiou and Christina Vichou. Agent Agreement Protocols based on Golay Error-Correcting Code. In *Proc. 4th IEEE International Conference on Information, Intelligence, Systems and Applications (IISA2013)*, 2013.

4. Vasiliki Liagkou, George Metakides, Apostolis Pyrgelis, Christoforos Raptopoulos, P. Spirakis, and Yannis 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).

5. P. Kotsopoulos and Y. Stamatiou. *Proc. IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pp. 927–933, 2012.

6. P. E. Nastou, Y. C. Stamatiou and A. Tsiakalos, "The Solution of a Differential Equation Describing the Evolution of a Key Agreement Protocol", *EUROSIAM 2011*, 29–30 of December 2011, Montreux, Switzerland.

7. Panayotis E. Nastou, Yannis C. Stamatiou: A Distributed, Parametric Platform for Constructing Secure SBoxes in Block Cipher Designs. In *Proc. Security Technology - International Conference FGIT-SecTech*, 2011: 155–166.

8. 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, 177–187, 2011.

9. Ioannis Chatzigiannakis, Apostolos Pyrgelis, Paul G. Spirakis, Yannis 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)*: 715–720, 2011.

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

11. 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)*, 2009.

12. P. Kammas, T. Komninos, and Y.C. Stamatiou, Modeling the co-evololution DNS worms and anti-worms in IPv6 networks, in *Proc. The Fifth International Conference on Information Assurance and Security (IAS09)*, 2009.

13. P. Papaioannou, P. Nastou, Y.C. Stamatiou, and Christos Zaroliagis, Secure Elliptic Curve Generation and Key Establishment on a 802.11 WLAN Embedded Device, accepted at the *9th International Symposium on Autonomous Decentralized Systems (ISADS 2009).*

14. V. Papadinas and Y.C. Stamatiou, Geometric approaches for creating low power, low interference connectivity patterns in static, structureless sensor networks, accepted at the *First International Workshop on Autonomous Embedded Systems and Networking (AESN 2009)*, a workshop of ISADS 2009.

15. C. Manolopoulos, P. Nakou, A. Panagiotaki, D. Sofotasios, P. Spirakis, and Y.C. Stamatiou, A step-wise refinement approach for enhancing eVoting acceptance, accepted at *2nd Int. Conf. on Theory and Practice of Electronic Governance (ICEGOV 2008)*, 2008.

16. P. Kammas, T. Komninos, and Y.C. Stamatiou, A queuing theory based model for studying intrusion evolution and elimination in computer network, accepted for presentation at *4th International Conference on Information Assurance and Security (IAS 2008).*

17. 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, accepted for presentation at the *7th International Conference on eGovernment (EGOV 2008).*

18. Y.C. Stamatiou, The theoretical analysis of an agreement protocol using Lambert functions, presented at the 2008 International Workshop on Applied Probability, Invited Session with title *Discrete distributions and asymptotic behaviour.*

19. 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).*

20. 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)*, 366−377, Lecture Notes in Computer Science, Springer-Verlag, 2007.

21. 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.

22. 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), 741−748, IEEE, 2007.

23. 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)*, 343−352, Lecture Notes in Computer Science, Springer Verlag, 2006.

24. 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)*, 2006.

25. 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.

26. 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. ALGOSENSORS 2006*, pp. 130−139, Springer Verlag, 2006.

27. 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.

28. 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.

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

30. 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.*

31. 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)*, pp. 335-349, Springer Verlag, 2005.

32. 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)*, pp. 147-163, Springer Verlag, 2004.

33. 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)*, pp. 309-322, 2003.

34. 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.), 333−348, Springer Verlag, 2002.

35. 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*, 625−636, Springer Verlag, 2002.

36. 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.

37. A.C. Kaporis, L.M. Kirousis, and Y.C. Stamatiou, How to prove 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.

38. 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.

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

40. 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.

41. 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.

42. 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.

43. 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.

44. Y.C. Stamatiou, E. Henriksen, E. Mantzouranis, E.-M. Knudsen, K. Papadaki, M. Psarros, E. Skipenes, N. Stathiakis, K. Stølen, and G. Valvis, Experience and results from applying a model-based risk assessment methodology, in the security analysis of a Tele-cardiology application, presented at the *7th European conference on Electronic Health Records (TEHRE 2002)*, London, UK, 2002.

45. 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, accepted at the *18th Medical Informatics Europe (MIE 2003)*, St. Malo, France, 2003.

46. 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), 7−10, ACM Press, 2001.

47. 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.

    It will be 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.*

48. 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.), 328−338, Springer-Verlag, 2001.

49. 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.), 185−194, 2001. Also, in Electronic Notes in Discrete Mathematics H. Kautz and B. Selman (eds.), Vol. 9, Elsevier Science Publishers, 2001. Also to appear in *Journal of Discrete Mathematics.*

50. 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.), 183−296, Springer-Verlag, 2000.

51. 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.*

52. 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), Hacène Fouchal and Roger Y. Lee (eds.), 189−196, Published by the International Association for Computer and Information Science (ACIS), 2000.

53. 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.

54. 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.

55. 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*, 107−120, Springer-Verlag, 1997. Also, in the *Constraints* journal.

56. 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. *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, 210−224, 1995.

    A short edition of this paper with title *Partial Arc Consistency* appeard in the conference *Over-Constrained Systems* (Cassis, 1995), Michael Jampel (ed.), Vol. 1106 of *Lecture Notes in Computer Science*, Springer-Verlag, 229−236, 1996.

57. 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* (Montréal, 1995), 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.), 41−66, Elsevier Publishers, 1997.

58. 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, 160−163, 1995.

Submitted

1. D. Kalles, A. Papagelis, and Y.C. Stamatiou, Speeding-up and consolidating a heuristic through asymptotic analysis.

2. Y.C. Stamatiou and M. Vamvakari, A statistical/algorithmic framework for modeling fixed odds forecast games.

Publications related to telemedicine applications

1. 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.

2. Y.C. Stamatiou, E. Henriksen, E. Mantzouranis, E.-M. Knudsen, K. Papadaki, M. Psarros, E. Skipenes, N. Stathiakis, K. Stølen, and G. Valvis, Experience and results from applying a model-based risk assessment methodology, in the security analysis of a Tele-cardiology application, presented at the *7th European conference on Electronic Health Records (TEHRE 2002)*, London, UK, 2002.

3. 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, accepted at the *18th Medical Informatics Europe (MIE 2003)*, St. Malo, France, 2003.

Technical reports

1. L.M. Kirousis, E. Kranakis, D. Krizanc, and Y.C. Stamatiou, Approximating the Unsatisfiability Threshold of Random Formulas, *Technical Report* TR-96-27, University of Carleton, 1996.

2. L.M. Kirousis and Y.C. Stamatiou, An Inequality for Reducible, Increasing Properties of Randomly Generated Words, *Technical Report* TR-96.10.34, Computer Technology Institute, 1996.

3. L.M. Kirousis and Y.C. Stamatiou, A purely asynchronous, message-efficient distributed algorithm for achieving arc consistency in networks of relations, *Technical Report*, CTI, 1995.

4. *Implementation and Analysis of Cryptographically Secure Pseudo Random Number Generators for the lottery game KENO of the Greek Government Organization for Lottery Games: final project report on the requirements, the proposed solutions and their cryptographic security.* CTI technical report June 1998. (In the Greek language.) Project team: P. Spirakis, L.M. Kirousis, Y.C. Stamatiou (author of the final report), T. Dimitriou, D. Fotakis, N. Nousis.

Survey-Review articles and presentations

1. P. Spirakis and Y.C. Stamatiou, *New directions in cryptography* (in the Greek language), presentation at the first symposium on *Informatics and Operations Research in the Greek Army Forces*, November 2–3, 1999.

2. P. Spirakis and Y.C. Stamatiou, *Efficient protocols for the detection of mobile eavsdroppers in computer networks* (in the Greek language), presentation at the first symposium on *Informatics and Operations Research in the Greek Army Forces*, November 2–3, 1999. (Talk based on research work of I. Antonopoulou, P. Spirakis, and B. Tampakas.)

Other contributions

He is contributing with Prof. P. Spirakis and Dr. P. Nastou to a monthly column of the greek magazine “Defense and Diplomacy” devoted to cryptography and cryptanalysis.