CURRICULUM VITAE

Personal Data

Name: Constantinescu Nicolae

Birthday: 21.11.1973

Place : Craiova city

Adresse : Bucharest, Bd. Octavia Goga, nr. 14

Nationality: Romanian

Phone: +40745308324

E-mail:
nikyc@inf.ucv.ro;
nikyc@central.ucv.ro,
nicolae.constantinescu@securitateainformatiei.ro

URL: `http://inf.ucv.ro/~nikyc`

Education

2006 - Ph.D. in Mathematics, title: Optimization of Parallel Algorithms and cryptographic applications, University of Bucharest, Romania, scientific supervisors: Prof. dr. Ion Vaduva; reviewers committee : Academician Prof. Dr. M. Iosifescu; Academician Prof. Dr. I. Tomescu; Prof. Dr. R. Trandafir

1998 - Master in Informatics, speciality Artificial Intelligence - University of Craiova, Romania

1997 - Faculty of Mathematics and Informatics, section of Informatics - University of Craiova, Romania

Upgrade courses

Three months stage in University of Makedonia, Greece. In this place I come in on study for mathematical models used in Sun network communication security, the results of research was published in security issues from USA and Greece

Aptitude for domains

numerically analysis of pseudorandom numerical generators

nonlinear analysis systems for secret key discovery in long encrypted data - cryptanalysis

One-way functions. Elliptic curves. DLP. ECDLP

Authentication protocols

Information Security

Programming Languages

Affiliations

American Mathematical Society, since 2002

Societies of Mathematics Sciences from Romania, since 2002

Romanian Probability and Statistics Society, since 2002

Society for Computing Technology, since 2009

Reviewer

Mathematical Reviews

Zentralblatt

Reviewer/Decisional

Elsevier, Computer&Security

Elsevier, Mathematical and Computer Modelling

Springer, Soft Computing

Taylor&Francis, International Journal of Computer Mathematics

SCT, Journal of Knowledge, Communications and Computing Technologies, Ed. In Chief

International Journal Of Network Security

Annals of the University of Craiova

Languages

English - advanced (read, write, spoken)

Russian - medium (read, write, spoken)

French - beginner (read, write, spoken)

Professional Activity

From 2011 : Assoc. Prof in University of Craiova, Faculty of Mathematics and Informatics, Department of Informatics

From 2007 - to 2011 : Lecturer in University of Craiova, Faculty of Mathematics and Informatics, section of Informatics

From 2001 - to 2007: As. Prof. in University of Craiova, Faculty of Mathematics and Informatics, section of Informatics

From 1999 - to 2001: research in mathematics Advanced Institute of Technology, Bucharest. In this place I come in on study for mathematical models used in protection of the communication.

Invited Speakers

Feb. 2009, University of Macedonia, Thessaloniki, Greece, Research Project: "Cryptography, at the Computational System & Software Engineering"

Sept. 2007, Limoges University, France, Research Project: Protection de l'Information, Codage, Cryptographie

Research Projects

I Function in the project: Director

- **National Projects**

  1. Grant no.316/2007, (Director) Project: Elliptic Curves Non-Supersingular Study and Intractability of their isomorphic class. Director Lecturer Dr. N. Constantinescu.
     Period: 2007-2009;
     Research Objectives:
     - NonSupersingular eliptic curves generated space study
     - Construction of an Interface between mathematical model and Implementation model
     - Cryptographical algorithms for constructed model

- **International Projects**

  1. CNRS Resercher (Director), 6 months, Paris-Orsay University. Project: Hiden Information Analyses.
     Period: 2007-2008;
     Research Objectives:
     - Hiden Information Analysis. Image Analysis
     - Algorithms Optimization for Hiden Information Search

II Function in the project: Member

1. CNCSIS IDEI PCE, 47/2011 Period: 2011-2014 Research Objectives:

2. CNMP, ATHOS (Biometrically Signature Authomatic Authentication Service). Director: Phd. Bogdan Warinschi.
   `http://rd.softwin.ro/index.php?option=com_content&view=article&id=60&Itemid=76&lang=ro`
   Period: 2010-2013;
   Research Objectives:
   - mathematical model, architecture and solution for SaaS and SoA
   - implementation of the cryptographycally functions developed in SISEB

- delivery the cryptograpycally library which begin a developer/client solution to authenticate parts of the communication

3. CNMP Research Contract no. 2660/2007, Partnership Section, (Member) Project: SISEB (Biometric Signature Secured e-Banking System). Director: Phd. Adrian Dinescu.
   `http://rd.softwin.ro/index.php?option=com_content&view=article&id=30&Itemid=31&lang=ro`
   Period: 2007-2010;
   Research Objectives:
   - Establish the Secured Bank Acces Procedure, based on a Biometric Authentication
   - Cryptographycally Algorithm Analyse and Optimisation
   - Application Development
4. AMCSIT Research Contract no. 1166/2007, Inovation Section, (Member) Project: BIOACS (Biometrically System for Acquisition and Authetication of Dynamically Signature). Director: Phd. Adrian Dinescu.
   `http://rd.softwin.ro/index.php?option=com_content&view=article&id=39&Itemid=51&lang=ro`
   Period: 2007-2010;
   Research Objectives:
   - biometrical data acquisition analyses
   - optimization and implementation of cryptographical algorithms
   - optimization and implementation of SRA-authentication algorithms
5. Grant no.976/2002, Project: Processing Incomplete Knowledge in Web Extraction. Director Prof.Dr. I. Iancu.
   Period: 2002-2003;
   Research Objectives:
   - To obtain new operators for managing uncertainty in inferential processes
   - To develop of a general representation language for web engines search criteria
   - To obtain optimal algorithms
   - To extend the resolution reasoning in order to support distributed knowledge

- A knowledge base model and query language for such knowledge

Publications

Theses

- Semantic Programs Computing, Faculty Degree Thesis, Faculty of Mathematics and Informatics, University of Craiova, Craiova June 1997, 56 pp.
- Parallel Computing in Artificial Intelligence, Faculty of Mathematics and Informatics, University of Craiova, Dissertation Thesis, Craiova June 1998, 52 pp.
- Optimization of Parallel Algorithms and cryptographic applications, University of Bucharest, Phd. Thesis, Bucharest 30 June 2006, 167 pp.

Articles

- **ISI Indexed**

1. Emil Simion and Nicolae Constantinescu, Complexity Computations in Code Cracking Problems, Concurrent Engineering in Electronic Packaging, IEEE Communication, Conference Date: may 05-09, 2001, pp. 225-232, ISSE 2001.
2. George Stephanides and Nicolae Constantinescu, Identification of parts in identity-based encryption, Advandces in Learning, Commerce and Society, K. Morgan Editor, University of Bergen, Norway and J.M. Spector, Syracuse University, USA, Vol. 30, pp. 177-181, 2004.
3. Nicolae Constantinescu and George Stephanides, The GN-authenticated key agreement, Journal of Applied Mathematics and Computation, Elsevier, London, Vol. 170, No. 1, pp. 531-544, 2005.
4. Nicolae Constantinescu, George Stephanides, Mirel Cosulschi and Mihai Gabroveanu, RSA-Padding Signatures with Attack Studies, International Conference on Web Information Systems and Technologies: Internet Technology/Web Interface and Applications, INSTICC Press Setubal, Portugal Jose A. Moinhos Cordeiro and Vitor Pedrosa and Bruno Encarnacao and Joaquim Filipe (ed.), ISBN 978-972-8865-46-7, pp. 97-100, 2006.

5. Mirel Cosulschi, Adrian Giurca, Bogdan Udrescu, Nicolae Constantinescu and Mihai Gabroveanu, HTML Pattern Generator-Automatic Data Extraction from Web Pages. International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, sept. 26-29 2006, IEEE Computer Society, ISBN 978-0-7695-2740-6, pp. 75-78, 2007.
6. Mihai Gabroveanu, Ion Iancu, Mirel Cosulschi and Nicolae Constantinescu, Towards Using Grid Services for Mining Fuzzy Association Rules, IEEE Computer Society Ninth International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, IEEE Computer Society, ISBN 978-0-7695-3078-9, pp. 507-513, 2007.
7. Ion Iancu, Mihai Gabroveanu, Mirel Cosulschi and Nicolae Constantinescu, Implication-Based Support Measures for Fuzzy Association Rules, IEEE Computer Society Ninth International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, IEEE Computer Society, ISBN 978-0-7695-3078-9, pp. 144-150, 2007.
8. Mirel Cosulschi, Mihai Gabroveanu and Nicolae Constantinescu, Usage of advanced data structure for improving efficiency for large (n, m) permutations inspired from the Josephus problem, Romanian Journal of Information Science and Technology, Romanian Academy, Vol. 12, No. 1, pp. 13-24, 2009.
9. Nicolae Constantinescu and Costin Boldea, High-Level Secured Signature Scheme, Mathematical Methods and Applied Computing, Vol. 1, pp. 115-118, 2009.
10. Mirel Cosulschi, Mihai Gabroveanu and Nicolae Constantinescu, Web Services for Search Integration, IDC - Intelligent Distributed Computing III, Vol. 237, pp. 63-73, Published: 2009 Conference Title: 3rd International Symposium on Intelligent and Distributed Computing (IDC 2009) Conference Date: oct. 13-14, Springer Verlag, Germany, 2009, ISBN 978-3-642-03213-4.
11. Nicolae Constantinescu and Costin Boldea, Two-Dimensional (2D) Cellular Automata for the Vernam Cipher Algorithm in Secret Key Cryptography, Annals of DAAAM, 2009, Vol. 20, pp. 881-882, Vienna, Austria.
12. Nicolae Constantinescu, Costin Boldea and Cristea Boboila, Elliptic Curves Cryptosystems for ECommerce Applications, Conference on Recent Advances in Mathematics and Computers in Busi-

ness, Economics, Biology & Chemistry, ISSN: 1790-2769, ISBN: 978-960-474-194-6, pp. 216-221, 2010.

13. Cristea Boboila, Nicolae Constantinescu and Costin-Radu Boldea, Preserving Consistency and Security of Data in E-business Applications, Conference on Recent Advances in Mathematics and Computers in Business, Economics, Biology & Chemistry, ISSN: 1790-2769, ISBN: 978-960-474-194-6, pp. 211-215, 2010.
14. Mihai Gabroveanu, Mirel Cosulschi and Nicolae Constantinescu, WebKM - Online Data Mining System, Intelligent Distributed Computing IV, Vol. 315, pp. 41-46, Springer-Verlag, 2010.
15. Nicolae Constantinescu and Cristea Boboila, Tripartite Authentication for an E-commerce System, Applied Economics, Business & Development, Tunisia, ISSN: 1790-5109, ISBN: 978-960-474-184-7, pp. 208-213, 2010.
16. Cristea Boboila and Nicolae Constantinescu, CELICA: A Multi-Agent Communication System for Electronic Commerce, Applied Economics, Business & Development, ISSN: 1790-5117, ISBN: 978-960-474-178-6, pp. 23-28, 2010.
17. Ion Iancu, Nicolae Constantinescu and Mihaela Colhon, Fingerprints Identification using a Fuzzy Logic System, International Journal of Computers, Communications & Control, Vol. V , No. 4, pp. 525-531, 2010.
18. Nicolae Constantinescu and Ion Iancu, Fuzzy Identity Authentication, International Conference on Computers, ISSN: 1792-4251, ISBN: 978-960-474-201-1, pp. 168-173, 2010.
19. Dorel Savulea, Nicolae Constantinescu, Authentication Hierarchy in Distributed Deductive Databases, International Conference on Computers, ISSN: 1792-4251, ISBN: 978-960-474-201-1, pp. 238-243, 2010.
20. Nicolae Constantinescu, Security System Vulnerabilities, Proceedings of the Romanian Academy Series A-Mathematics Physics Technical Sciences Information Science, Vol. 13, No. 2, pp. 175-179, 2012.
21. Ion Iancu, Nicolae Constantinescu, Intuitionistic fuzzy system for fingerprints authentication, Applied Soft Computing, Vol. 13, No. 4, pp. 2136-2142, 2013,

- **International Indexed Databases**

1. Vasile Preda, Emil Simion and Nicolae Constantinescu, Reliability Analysis of the Stress-Strength, Proc. of the 6th International symposium for design and technology of electronic packages, SYTME 2000, sept. 21-24, pp. 29-32.
2. Emil Simion, Nicolae Constantinescu and Mircea Barboi, Bayesian Estimators in Cryptography, IEEE Communications 2000 and Military Technical Academy, dec. 7-9 2000, Bucharest, pp. 385-388.
3. Emil Simion and Nicolae Constantinescu, Linear Complexity Computations of Cryptographic Systems, International Conference of Telecommunications, IEEE Communication, Bucharest, Vol. 1, 4-7 June 2001, pp. 85-89.
4. Mirel Cosulschi and Nicolae Constantinescu, Optimum Search Method of Information, The Annals of the University of Craiova - Mathematics and Computer Science series, Vol. XXVIII, 2001.
5. Nicolae Constantinescu and Mirel Cosulschi, GA Based Parallel Clusters, The Annals of the University of Craiova - Mathematics and Computer Science series, Vol. XXIX, pp. 180-185, 2002.
6. Nicolae Constantinescu, Elliptic curves-based algorithms in cryptography, Annals of University of Bucharest, Vol. XXXI, No. 1, pp. 149-159, 2004.
7. Nicolae Constantinescu and George Stephanides, Identity-Based Encryption, International Conference on Data Security, Grecee 2004, published by WIT Press in Research Notes in Data Security.
8. Nicolae Constantinescu and George Stephanides, Secure Key-Exchange, Research Notes in Data Security, pp. 162-167, Greece, 2003.
9. Nicolae Constantinescu, The agreement of the common key, The Annals of the University of Craiova - Mathematics and Computer Science series, Vol. XXX, No. 2, pp. 59-65, 2003.
10. Mirel Cosulschi, Nicolae Constantinescu and Mihai Gabroveanu, Classification and comparison of information structures from a web page, The Annals of the University of Craiova, Vol. XXXI, pp. 109-121, 2004.
11. Mihai Gabroveanu, Nicolae Constantinescu, George Stephanides and Mirel Cosulschi, A distributed algorithm for mining fuzzy association rules, Proceedings of International Conference on Web

Information Systems and Technologies, Miami, USA, Vol. 5, pp. 206-209, 2005.

12. Mihai Gabroveanu, Mirel Cosulschi and Nicolae Constantinescu. A new approach to mining fuzzy association rules from distributed databases. Annals of the University of Bucharest, Mathematics and Computer Science Series, Vol. LIV, pp. 3-16, 2005.
13. Mirel Cosulschi, Bogdan Udrescu, Nicolae Constantinescu, Mihai Gabroveanu and Adrian Giurca, Experiences Regarding Automatic Data Extraction From Web Pages. Proceedings of IADIS International Conference on WWW/Internet. Murcia, Spain, ISBN 972-8924-19-4, pp. 281-288, 2005.
14. George Stephanides, Mirel Cosulschi, Mihai Gabroveanu and Nicolae Constantinescu. AHPA-Calculating Hub and Authority for Information Retrieval. 22nd International Conference on Data Engineering Workshops, ICDE 2006. IEEE Computer Society Atlanta, GA, USA , ISBN 0-7695-2571-7, pp. 36-42.
15. Nicolae Constantinescu, Non Singular Elliptic Curves - From Theory to Application. Algorithm attacks discussions, Mathematica Journal, Babes-Bolyai University, Tome 50(73), No. 2 (2008), pp. 177-186.
16. Nicolae Constantinescu, Linear Feedback Shift Register Optimizations, Annals of the University of Craiova, Mathematics and Computer Science Series, Vol. XXXVI, No. 1, 2009, pp. 49-54.
17. Nicolae Constantinescu, Combining Linear Feedback Shift Registers, Annals of the University of Craiova, Mathematics and Computer Science Series, Vol. XXXVI, No. 2, pp. 42-46, 2009.
18. Nicolae Constantinescu, Elliptic curve cryptosystems and scalar multiplication, Annals of the University of Craiova, Mathematics and Computer Science Series, Vol. XXXVII, No. 1, pp. 27-34, 2010.
19. Nicolae Constantinescu, Authentication hierarchy based on blind signature, Journal of Knowledge Communication and Computing Technologies, Vol. 1, No. 1, pp. 77-84, 2010.
20. Nicolae Constantinescu, Authentication Protocol Based on Elliptic Curve Cryptography, Annals of the University of Craiova, Mathematics and Computer Science Series, Vol. XXXVII, No. 2, pp. 83-91, 2010.

21. Dorel Savulea, Nicolae Constantinescu, Statistical Correlation Study, Annals of the University of Craiova, Mathematics and Computer Science Series, Vol. XXXVII, No. 3, pp. 35-51, 2010.
22. Alin Golumbeanu, Nicolae Constantinescu, Digital Declaration implementation study, Journal of Knowledge Communication and Computing Technologies, Vol. 2, No. 2, pp. 35-47, 2010.
23. Nicolae Constantinescu, Claudiu-Ionut Popirlan, Authentication model based on Multi-Agent System, Annals of the University of Craiova, Mathematics and Computer Science Series, Vol. XXXVIII, No. 2, pp. 59-68, 2011.
24. Dorel Savulea, Nicolae Constantinescu, Statistical Analysis of the Demographic Ageing Process in the EU Member States, Former Communist Countries, International Journal of Advanced Computer Science and Applications, Vol. 3, No. 12, pp. 13-24, 2012.

- **International Conferences**

1. Mihai Gabroveanu, Mirel Cosulschi, Nicolae Constantinescu and Adrian Giurca, Mining Association Rules on Knowledge Grid Network, The First East European Conference on Health Care Modeling and Computation (HCMC 2005), Craiova, Romania.

- **National Conferences**

1. Emil Simion and Nicolae Constantinescu, Principles in Cryptanalysis of Stream Ciphers. Annual Proc. of SSMR, may 25-28 Constanta 1999, 6 pp.
2. Emil Simion, Nicolae Constantinescu and Dan Pop, Bayesian Cryptographic Analyze, XXVII session of Advanced Institute of Technology, 1999, 8 pp.
3. Emil Simion and Nicolae Constantinescu, Checking and Testing Random Games Tables, The Annual Meeting of the Mathematical Statistical Center of the Romanian Academy, Bucharest feb. 23 2001.
4. Nicolae Constantinescu and Emil Simion, Pseudoaleator uniform generator; Variant of LFSR structures, 5-th Conference of Statistics and Probability Society, University of Bucharest and Romanian Academy, Bucharest, feb. 22-23 2002, 5 pp.
5. Mihai Gabroveanu, Mirel Cosulschi and Nicolae Constantinescu, Some remarks regarding optimization of mining fuzzy association

rules, 8-th Conference of Romania Probability and Statistics Society, University of Bucharest, Faculty of Mathematics and Informatics, apr. 22-23 2005.

- **Other**

  1. Nicolae Constantinescu, Authentication ranks with identities based on elliptic curves, Annals of the University of Craiova, Mathematics and Computer Science Series, Vol. XXXIV, pp. 94-99, 2007.
  2. Mihai Dupac and Nicolae Constantinescu, 3D Steganography Models, Annals of the University of Craiova, Mathematics and Computer Science Series, Vol. XXXV, pp. 97-102, 2008.

Books

1. Cristian Kevorchian, Nicolae Constantinescu, Programare Logica. O Abordare Pragmatica, Craiova, Sitech, 2005, 220 pag.
2. N. Constantinescu, Bazele Programarii Procedurale, Ed. Universitaria Craiova 2009, 172 pag.
3. Nicolae Constantinescu, Criptografie, Ed. Academiei 2009, 530 pag.
4. Nicolae Constantinescu, Programare Procedurala, Ed. II-a, Adugit i revizuit, Ed. Universitaria Craiova 2012, 365 pag.

Elaborated Studies in Advanced Institute of Technology

Algorithmic studies for security protocols in Internet, Technical Report, Advanced Technologies Institute, 1999

Artificial Intelligence Algorithms to generate particular dictionary, Technical Report, Advanced Technologies Institute, 1999

Optimizations of parallel algorithms used in cryptographic analysis, Technical Report, Advanced Technologies Institute, 1999

President/Organizer/Editor of International Conference and Summer Schools

1. Summer School *Teoria Codurilor*, University of Bucharest, Member in the Organization Committee, 2008.

2. Franco-Romain International Conference in Aplied Mathematics, 2009, Member in Organization Committee, Chairman of the Cryptography section.

3. ICCCI 2013, 5th International Conference on Computational Collective Intellligence Technologies and Applications, Local Organizing Committee.

Citations

1. Jahresforschungsbericht 2006 / 2007 Drittmittelforschungsprojekte Publikationen Abgeschlossene Promotionen und Habilitationen, Brandenburgische Technische Universitt Cottbus (cited paper HTML Pattern Generator: Automatic Data Extraction from Web Pages)

2. W. Gatterbauer, P. Bohunsky, M. Herzog, B. Krupl, and B. Pollak - Towards Domain Independent Information Extraction from Web Tables, WWW 2007 (cited paper Classification and comparison of information structures from a web page) (http://portal.acm.org/citation.cfm?id=1242583)

3. Wolfgang Gatterbauer, Paul Bohunsky, Marcus Herzog, Bernhard Krupl, and Bernhard Pollak, Towards DomainIndependent Information Extraction from Web Tables, WWW 2007 / Track: Data Mining Session: Identifying Structure in Web Pages, (cited paper Classification and comparison of information structures from a web page)

4. M. Ben Saad, S. Ganarski, Z. Pehlivan - A Novel Web Archiving Approach based on Visual Pages Analysis, 9th International Web Archiving Workshop, 2009 (cited paper Classification and comparison of information structures from a web page)

5. Mikel Sorli and Dragan Stokic, Book: Innovating in Product/Process Development. Gaining Pace in New Product Development, Springer, ISBN 978-1-84882-544-4 (Print) 978-1-84882-545-1 (Online), DOI 10.1007/978-1-84882-545-1, 2009, capitolul Future Trends, pp 219-254: (cited paper Pattern Generator - Automatic Data Extraction from Web Pages, Synasc 2006)

6. Milos Kudelka, Yasufumi Takama, Vaclav Snasel, Karel Klos and Jaroslav Pokorny -Visual similarity of web pages, Ch 13, in Advances in Intelligent Web Mastering - 2, Proceedings of the 6th Atlantic Web Intelligence Conference - AWIC'2009; Series: Advances in Intelligent and Soft Computing, Vol. 67, Snel, V.; Szczepaniak, P.S.; Abraham, A.; Kacprzyk, J. (Eds.), 2010, ISBN: 978-3-642-10686-6. (cited paper Classification and comparison of information structures from a web page)

7. Wolfgang Gatterbauer, Bernhard Kruepl, Paul Bohunsky, Marcus Herzog - Information Extraction Using Spatial Reasoning On The CSS2

Visual Box Model. (US Patent Application 20080294679, WASHINGTON, DC) (patent for the LIXTO SOFTWARE GMBH Company). (cited paper: Classification and comparison of information structures from a web page)

8. M. Ben Saad, S. Ganarski, Z. Pehlivan - Vi-DIFF: Understanding Web Pages Changes, Proceedings of 21st International Conference DEXA 2010, Bilbao, Spain, August 2010, Springer, LNCS, Volume 6261, DOI: 10.1007/978-3-642-15364-8-1, 2010, ISBN: 978-3-642-15363-1, pp. 1-15.(cited paper Classification and comparison of information structures from a web page)

9. Vclav Snel, Milo Kude(lka, Zdene(k Hork: Web Content Mining Using MicroGenres (chapter 4), Advanced Techniques in Web Intelligence (Juan D. Velsquez and Lakhmi C. Jain eds.), Studies in Computational Intelligence, Springer, Volume. 311/2010, ISBN: 978-3-642-14460-8, DOI: 10.1007/978-3-642-14461-5-4, 2010, pp. 79-112.(cited paper Classification and comparison of information structures from a web page)

10. Myriam Ben Saad, Stphane Ganarski - Using visual pages analysis for optimizing web archiving, EDBT '10: Proceedings of the 2010 EDBT/ICDT Workshops, Lausanne, Switzerland, ACM International Conference Proceeding Series, Vol. 426, ISBN: 978-1-60558-990-9, 2010, pp. 1-7. (ACM Portal)(cited paper Classification and comparison of information structures from a web page)