Curriculum Vitæ et Studiorum

Stelvio Cimato

June 2023

Personal Data:

Name: Stelvio Cimato

Work Address: Dipartimento di Informatica
Università degli Studi di Milano
Via Celoria, 18
20135 MIlano (MI)

Telephone: +39 02-503 16258

E-mail: stelvio.cimato@unimi.it

URL: http:/homes.di.unimi.it/cimato

Position:

Since April 2016, associate professor at the Dipartimento di Informatica of the Università degli studi di Milano.

Education:

January 2005- March 2016 assistant professor at the Dipartimento di Informatica of the Università degli studi di Milano.

September 1999- December 2004 research fellow at the Dipartimento di Informaticae Applicazioni of the Università degli studi di Salerno

February 99 Ph.D in Computer Science at Università degli Studi di Bologna consortied with Università degli Studi di Padova e Venezia.

June 94 Laurea degree in Scienze dell'Informazione at l'Università degli Studi di Salerno, 110/110 cum laude.

1 Professional experience

January 2005- March 2016 assistant professor at the Dipartimento di Informatica of the Università degli studi di Milano.

June 1999 - December 2004 Research fellow at Dipartimento di Informatica ed Applicazioni dell'Università di Salerno

1994-1999 PhD: Dottorato di Ricerca in Informatica (X ciclo), at the Dipartimento di Scienze dell'Informazione dell'Università di Bologna consortied with Università di Padova e Venezia. 22 Febbraio 1999 defends his thesis *"A Methodology for the Specification of Java Components and Architectures*", supervisor Prof. Paolo Ciancarini.

2 Research interests and projects

Stelvio Cimatos research interests are in the main area of data security and cryptography. In particular, he is interested in Visual Cryptography, Web Services Security, Biometric authentication, protocols and web application. His work is reported in peer-reviewed articles in international journals, conference proceedings, and book chapters. He has participated in several projects involving different aspects of data security and information protection.

2.1 International Projects

- Erasmus+ Erasmus Mundus Design Measures (ERASMUS-EDU-2022-EMJM-DESIGN) CALL ID: ERAS MUS-EDU-2022-PEX-EMJM-MOB - Master in Intelligent Systems for a Sustainable Digital Transformation of the Society MINDS. Role: (co-)Resp. for UNIMI

- TENACIOUS: Trustworthy sEmaNtic Aware marketplaCe for Interoperable clOUd Services, selected for the first phase of the European project funded by the European Commission under the European Unions Horizon 2020 Research and Innovation Programme (Call topic ICT-54) and part of the European Commissions Next Generation Internet (NGI) initiative. Role: co-leader together with E. Bellini, B. Di Martino, A. Esposito, and E. Damiani

- European Project H2020 Threat Arrest - Cyber Security Threats and Threat Actors Training - Assurance Driven Multi-Layer, end-to-end Simulation and Training Grant Number 786890 (2018-21), Resp. UNIMI: prof. Ernesto Damiani, (36 months), Role: WP Leader

- European Project Erasmus+ FIT EUROPE (Future IT leaders for a multicultural, digital Europe) 9/2019-8/2022 Rfrence : 2019-1-FR01-KA203-063041. Resp. UNIMI: prof. Ernesto Damiani, (36 mesi), Role: WP Leader

- European Project H2020-MSCA-RISE-2019 AERAS (A CybEr range tRaining platform for medicAl organisations and systems Security). Resp. UNIMI: prof. Ernesto Damiani, Role: Participant

- COST Action CA17124 - Digital forensics: evidence analysis via intelligent systems and practices, Proposal Reference OC-2017-1-22305, Role: Secondary proposer for Univ. degli studi di MIlano. Chair Jesus Medina Moreno Universita' di Cadice, vice Chair prof. Stefania Costantini - Univ. dell'Aquila -Start action 10/09/2018 End of Action - 09/09/2022

- European Project H2020 TOREADOR - TrustwOrthy model-awaRE Analytics Data platfORm Grant Number 688797 (2015-18), Resp. UNIMI: prof. Ernesto Damiani, (36 months), Role: Participant
- European Project FP7: PRACTICE (PRivAcy-preserving CompuTation In The Cloud) FP7- 609611 (2013-16), Responsabile scientifico UNIMI: prof. Ernesto Damiani, (36 months), Role: WP Leader
- European Project FP7: CUMULUS - Certification infrastrUcture for MUlti-Layer cloUd Services FP7-318580 (2012-2015), Responsabile scientifico UNIMI: prof. Ernesto Damiani, (36 months), Role: Participant
- European Project FP7: ASSERT4SOA (Advanced Security Service cERTificate for SOA) FP7-257351 (2010-2013), Responsabile scientifico UNIMI: prof. Ernesto Damiani, (36 months) Role: Participant
- European Project FP7: SECURESCM (SECURE Supply Chain Management) FP7- 213531 (2008-2011) , Responsabile scientifico UNIMI: prof. Ernesto Damiani, (36 months), Role: WP Leader

2.2 National Projects

- PRIN 2010 GenData 2020 (Data-Centric Genomic Computing) (PRIN 2010) Responsible Prof. S. Ceri, Unità di ricerca di Milano, resp. prof. P. Samarati (36 mesi)
- PRIN 2008: PEPPER: Privacy E Protezione di dati PERsonali, Responsible Prof. S. Paraboschi, Unità di ricerca di Milano, scientific resp. Prof. P. Samarati. (24 mesi)
- PRIN 2006: Basi di dati crittografate, Responsible Prof. S. Paraboschi, Unità di ricerca di Milano, scientific resp. Prof. P. Samarati. (24 mesi)
- Progetto MIUR Co-financed *Metodi Formali per la Sicurezza e il Tempo (MEFISTO)*, 2002-2003.
- Progetto *Pubblicità Online: Nuove Misure per Nuovi Media. Auditing e Accounting Sicuro sul Web*, programme CNR-Agenzia 2000.

2.3 Local Projects

Coordinator

- Coordinator and Responsible for the project *Protocolli di Autenticazione per Smartcard e Applicazioni a Mobile Commerce*, financed by Università di Salerno, - Anno 2001.
- Coordinator and Responsible for the project *Nuove Tendenze nel Commercio Elettronico e Pubblicità Online: gli E-Coupon*, financed by Università di Salerno - Anno 2000.

3 Professional Activities

3.1 Editorial Board of Journals

- Since July 2019 member of the editorial board for *Future Internet*, MDPI
- Since June 2018 member of the editorial board for *Cryptography*, MDPI

- Since March 2018 member of the editorial board for *Security and Communication Networks* , Hindawi
- From January 2017 to Decembre 2020 member of the editorial board for *Electronic Commerce Research and Applications*, Elsevie
- From January 2008 to December 2012 member of the editorial board for *Recent Patents on Computer Science*, Bentham Science Publishers
- Member of the IEB for Special Issue of Information Systems Frontiers on Intelligent Systems and Smart Homes, pubblicato da Springer (2007)

3.2 Organization of International Conferences

- Program Chair *ICSEB 2022, 6th International Conference on Software and e-Business*, Shenzhen, China - December 09-11, 2022
- Program Chair *ICSEB 2021, 5th International Conference on Software and e-Business* , virtual — December 3-5, 2021
- Program Chair *ICSEB 2020, 4th International Conference on Software and e-Business* , virtual — December 18-20, 2020
- Technical Committee Chair *ICSEB 2019, 3rd International Conference on Software and e-Business* , Tokyo, Japan — December 9-11, 2019
- Program Chair *COMPSAC 2019: The 43nrd IEEE Computer Society International Conference on Computers, Software & Applications* Milwaukee, USA - July 15-19, 2019
- Program Chair *COMPSAC 2018: The 42nd IEEE Computer Society International Conference on Computers, Software & Applications* Tokyo, Japan - July 23-27, 2018
- Workshop Co-Chair *COMPSAC 2017: The 41th IEEE Computer Society International Conference on Computers, Software & Applications* Turin, Italy - July 3-8, 2017
- Organizzatore del workshop *Advances in Permutation Based Cryptograhy*, October 10, Milan, Italy, 2018.
- Workshop Co-Chair *COMPSAC 2016: The 40th IEEE Computer Society International Conference on Computers, Software & Applications* Atlanta, Georgia, USA - June 10-14, 2016
- Fast Abstract Co-Chair *COMPSAC 2015: The 39th IEEE Computer Society International Conference on Computers, Software & Applications* Taichung, Taiwan - July 1-5, 2015
- Program Chair del Workshop *14th IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2022)* in conjunction with COMPSAC 2022, virtual - June 27,July 1 2022
- Program Chair del Workshop *13th IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2021)* in conjunction with COMPSAC 2021, virtual - July 12-16, 2021
- Program Chair del Workshop *12th IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2020)* in conjunction with COMPSAC 2020, Madrid, Spain - July 13-17, 2020

- Program Chair del Workshop *11th IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2019)* in conjunction with COMPSAC 2019, Turin, Italy - July 15-19, 2019
- Program Chair del Workshop *10th IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2018)* in conjunction with COMPSAC 2018, Tokyo, Japan - July 23-27, 2018
- Program Chair del Workshop *9th IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2017)* in conjunction with COMPSAC 2017, Turin, Italy - July 3-8, 2017
- Program Chair del Workshop *8th IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2016)* in conjunction with COMPSAC 2016,Atlanta, Georgia, USA - June 10-14, 2016
- Program Chair del Workshop *7th IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2015)* in conjunction with COMPSAC 2015,Taichung, Taiwan - July 1-5, 2015
- Organizzatore del 12th workshop del collegio di dottorato MDPS in "Multimedia, Distributed and Pervasive Systems" June 23-27, Crema, Italy, 2014.
- Program Chair del Workshop *6th IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2014)* in conjunction with COMPSAC 2014,Västeras, Sweden
- Program Chair del Workshop *5th IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2013)* in conjunction with COMPSAC 2013, Kyoto, Japan
- Program Chair and organizer of the *4th IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2012)* in conjunction with COMPSAC 2012, Izmir, Turkey
- Program Chair and organizer of the *3rd IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2011)* in conjunction with COMPSAC 2011, Munich, Germany
- Program Chair and organizer of the *2nd IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2010)* in conjunction with COMPSAC 2010, Seoul, Korea
- Program Chair and organizer of the *1st IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2009)* in conjunction with COMPSAC 2009, Seattle, USA
- General Chair of *4th Conference on Security in Communication Networks (SCN'04)*, Amalfi, Italia, Settembre 2004.
- Publication Chair of *23rd International Information Security Conference (SEC 2008)* Milano, Italia, Settembre 2008.
- Organizer of the *17th International Conference on Distributed Computing (DISC'03)*, Sorrento, Italia, Ottobre 2003.
- Organizer of the *3rd Security in Communication Network (SCN'02)*, Amalfi, Italia, Settembre 2002.

3.3 Program Committee Member

- SEKE -International Conference on Software Engineering and Knowledge Engineering (2011-2020)
- ICME - IEEE International Conference on Multimedia and Expo (2011-2020)
- IMMM -International Conference on Advances in Information Mining and Management (2011-2018)
- ICISSP - International Conference on Information Systems Security and Privacy (2015-2020)
- ICCSIT - 1st International Conference on Computer Science and Information Technology (2018-19)
- ICISA - iCatse Conference on Information Science and Applications (2016-2019)
- PSBD - 4th International Workshop on Privacy and Security of Big Data (2017)
- KES - International Conference on Knowledge-Based and Intelligent Information and Engineering Systems (2017-19)
- ISIC - International Conference on Information Security and Intelligent Computing at Shennongjia, Hubei (2017)
- SIN - International Conference on Security of Information and Networks (2015-2016)
- SAPSE - IEEE International Workshop on Security Aspects of Process and Services Engineering in conjunction with COMPSAC IEEE conference (2009-2020)
- ESAS - IEEE International Workshop on E-Health Systems and Semantic Web (2016-2018)
- SFCS - IEEE International Workshop on Security and Forensics in Communication Systems in conjunction with AsiaCCS (2012-2015)
- ICB, International Conference on Biometrics (2015)
- WPS, 5th FTRA International Workshop on Web and Pervasive Security, Jeju, Korea (2012)
- SETOP, 5th SETOP International Workshop on Autonomous and Spontaneous Security, Pisa, Italy (2012)
- NPC, 9th IFIP International Conference on Network and Parallel Computing, Gwangju, Korea (2012)
- ISPEC, International Conference on Information Security Practice and Experience (2014)
- POLICE, International Workshop on Security Policies in Cloud Environment (2013- 14)
- CIS, International Conference on Computational Intelligence and Security (2005-2015)

- NSS, IFIP International Workshop on Network and System Security (2007-2011)
- IDEAL, International Conference on Intelligent Data Engineering and Automated Learning, (2010-2014)
- ICSNC, International Conference on Systems and Networks Communications, (2008-2015)
- ISSA, Annual Information Security South Africa Conference (2005-2012)
- SECURWARE, International Conference on Emerging Security Information, Systems and Technologies,(2011-2014)
- SESYS, Security Systems track of the International Conference on Systems and Networks Communications (2006-2007)
- SECRYPT 2009, International Conference on Security and Cryptography, Milan, Italy, (2009)
- BPS 2009, 1st International Workshop on Business Processes Security, in conjunction with DEXA 2009, Linz, Austria, (2009)
- ICICS 2007, Ninth International Conference on Information and Communications Security, Zhengzhou, Henan, China, (2007)
- IS, International Symposium on Information Security,(2006-2007)
- WISH, International Workshop on Intelligent Systems and Smart Home, (2007-2008)
- ASIACCS'07, ACM Symposium on Information, Computer and Communications Security, Singapore, March 2007.

3.4 Invited Talks

- Keynote speaker *Secure Data Sharing and Mining on the Cloud*, 2nd International Conference on Security with Intelligent Computing and Big-data Services (SICBS 2018), Guilin, China, December 14-16, 2018.
- *Tutorial on Visual Cryptography*, 8th IEEE International Workshop on Information Forensics and Security (WIFS) 2016, Abu Dhabi, UAE, December 4-7, 2016.
- *Panel on Big data security: issues and challenges.*, SIN '16 9th International Conference on Security of Information and Networks. Newark, NJ, USA, July 20 - 22, 2016.
- *Data Analysis with Privacy Constraints*, CRiSIS 2011. 6th International Conference on. Risks and Security of Internet and Systems, Timisoara, Romania, 26-28 September 2011
- *RFID Security in Business Applications*, Workshop on RFID Security, Akademia Ekonomiczna, Wroclaw, Poland, March 2008
- *Cryptographic Protocols for Internet Services.*
  3rd International School on Foundations of Security Analysis and Design (FOSAD 2002), Bertinoro (FC), Italia, Settembre 2002.

- *A Methodology for the Specification of Java Components and Architectures*, System Integration, Dagstuhl Seminar 99111, Dagstuhl, Germania, Marzo 1999.
- *Formal Specification of Component-Based Java Applications.* iNRIA-IRISA, University of Rennes, Francia, Ottobre 1998.

3.5 Reviewer Activity

Reviewer for international journals

- Theoretical Computer Science
- IEEE Transaction on Information Theory
- IEEE Transaction on Knowledge and Data Engineering
- IEEE Transaction on Information Forensics and Security
- IEEE Transaction on Parallel and Distributed Systems
- IEEE Transaction on Image Processing
- IEEE Transactions on Circuits and Systems for Video Technology
- IEEE Transaction on Multimedia
- IEEE Internet Computing
- ACM Transaction on Web
- IEEE Computers
- Electronic Commerce Research and Applications,
- Computer Networks, Elsevier
- Transactions on Data Hiding and Multimedia Security, Springer
- Computers & Security
- MultimediaTools and Applications, Elsevier
- Multimedia Systems Springer
- Journal of Systems and Software, Elsevier
- Journal of Computer Security, IOS Press
- Journal of Visual Communication and Image Representation
- Design, Codes and Cryptography, Kluwer
- Imaging Science Journal, Maney Publishing on behalf of the Royal Photographic Society
- Eurasip Journal on Information Security
- Journal of Computer and Science Technology, Springer
- Image and Vision Computing, Elsevier
- Information Sciences, Elsevier

- Security and Communication Networks, Springer
- Optical Engineering, SPIE
- Signal Image and Video Processing
- Telecommunication Systems, Springer

4 Service and Teaching Activities

He has held the following courses for the Laurea Degree in Computer Science Università' degli Studi di Milano.

- "Systems and Network Security" (12 cfu – 96 h) [2016-present]
- "Cryptography" (6 cfu – 48 h) [2005-present]
- "Cryptography" (6 cfu – 48 h) ONLINE edition [2005-present]
- "Laboratory of Applied Cryptography)" (6 cfu – 48 ore) [2005–2008]

4.1 Activities for Doctoral School

He has been: - Supervisor of 2 PhD students - Co-supervisor of 3 PhD students - Holder of teaching positions in the context of the Research Doctorate in Computer Science of the University of Milan. - Member of the commission of 2 final national and international doctorate exams (PhD) - Alternate member of the commission of 3 final doctoral exams

- Since 2011 to 2018 he has been member of the Teaching College for the Doctorate School in Informatics of the Università degli Studi Milano
- He has been supervisor for the thesis in Informatica of the following students:
  - XXXIV Course, student Maria Chiara Molteni, titled "On the security of cryptographic circuits: protection against probing attacks and performance improvement of garbled circuits"
  - XXIX course, Silvia Mella, titled "Analysis of cryptographic algorithms against theoretical and implementation attacks"
- He has been co-supervisor of the following students:
  - XXIII Course, student Francesco Pagano, titled "A Distributed Approach to Privacy on the Cloud"
  - XXV Course, Student Maryam Sepehri, titled "Privacy-preserving Query Processing over Outsourced Encrypted Data and Multi-Party Computation"
  - XXX Course, student Maryam Ehsanpour, titled "Toward Lower Communication in Garbled Circuit Evaluation"

5 Publications

5.1 Edited books and Special issues

[1] Shi Dong, Stelvio Cimato, Joarder Kamruzzaman, and Yongsheng Hao Special issue "Real-Time Image Steganography and Steganalysis" in Journal of Electronic Imaging - SPIE, 2022

[2] J.C.N. Yang, S. Cimato, Lizhi Xiong Special issue "Information Theory and Its Applications in Multimedia Security and Processing", in Entropy - MDPI, 2022

[3] Yimin Yang, James C.N. Yang, Cheonshik Kim, Stelvio Cimato, Gaurav Bhatnagar, Special issue "Computational Intelligence Techniques for Information Security and Forensics in IoT Environments" in Wireless Communications and Mobile Computing, Wiley - Hindawi

[4] Zhili Zhou, Ching-Nung Yang, Cheonshik Kim, Stelvio Cimato: Special issue "Deep learning for real-time information hiding and forensics" Journal of Real-Time Image Processing, Volume 17, Number 1, February 2020, Springer,

[5] James Ching-Nung Yang, Cheonshik Kim, Stelvio Cimato: Special issue "Computing Methods in Steganography and Multimedia Security" Mathematics, July 2020, MDPI

[6] S. Cimato, C.N. Yang *Visual Cryptography and Secret Image Sharing*, CRC Press, USA, 2011.

5.2 Edited Proceedings

[7] Vladimir Getov, Jean-Luc Gaudiot, Nariyoshi Yamai, Stelvio Cimato, J. Morris Chang, Yuuichi Teranishi, Ji-Jiang Yang, Hong Va Leong, Hossain Shahriar, Michiharu Takemoto, Dave Towey, Hiroki Takakura, Atilla Eli, Susumu Takeuchi, Satish Puri: 43rd IEEE Annual Computer Software and Applications Conference, COMPSAC 2019, Milwaukee, WI, USA, July 15-19, 2019, Volume 1. IEEE 2019, ISBN 978-1-7281-2607-4

[8] S. Reisman, S. I. Ahamed, C. Demartini, T. M. Conte, L. Liu, W. R. Claycomb, M. Nakamura, E. Tovar, S. Cimato, C. Lung, H. Takakura, J. Yang, T. Akiyama, Z. Zhang, K. Hasan, 2018 IEEE 42nd Annual Computer Software and Applications Conference, COMPSAC 2018, Tokyo, Japan, 23-27 July 2018, Volume 1, IEEE Computer Society, 2018.

[9] S. Reisman, S. I. Ahamed, C. Demartini, T. M. Conte, L. Liu, W. R. Claycomb, M. Nakamura, E. Tovar, S. Cimato, C. Lung, H. Takakura, J. Yang, T. Akiyama, Z. Zhang, K. Hasan, 41st IEEE Annual Computer Software and Applications Conference, COMPSAC 2017, Turin, Italy, July 4-8, 2017. Volume 1, IEEE Computer Society, 2017.

[10] S. Reisman, S. I. Ahamed, C. Demartini, T. M. Conte, L. Liu, W. R. Claycomb, M. Nakamura, E. Tovar, S. Cimato, C. Lung, H. Takakura, J. Yang, T. Akiyama, Z. Zhang, K. Hasan, 41st IEEE Annual Computer Software and Applications Conference, COMPSAC 2017, Turin, Italy, July 4-8, 2017. Volume 2, IEEE Computer Society, 2017.

[11] S. Jajodia, P. Samarati e S. Cimato, editors *Proceedings of the 23rd International Information Security Conference (SEC 2008)*, IFIP Series, Springer Verlag.

[12] C. Blundo e S. Cimato, editors *Security in Communication Networks, Fourth International Conference, (SCN 2004)*, Vol. 3352 di Lecture Notes in Computer Science, Springer Verlag, New York, USA, 2005.

[13] S. Cimato, C. Galdi e P. Persiano, editors *Security in Communication Networks, Third International Conference, (SCN 2002)*, Vol. 2576 di Lecture Notes in Computer Science, Springer Verlag, New York, USA, 2003.

5.3 International Journals

[14] C. Blundo, S. Cimato and L. Siniscalchi, "Role Mining Heuristics for Permission-Role-Usage Cardinality Constraints", Comput. J., vol. 65, no. 6, 2022, pp. 13861411.

[15] A. Bernasconi, S. Cimato, V. Ciriani, M. Molteni, "Multiplicative Complexity of XOR Based Regular Functions", IEEE Transactions on Computers, 2022.

[16] C. Blundo, S. Cimato and L. Siniscalchi, "Heuristics for constrained role mining in the post-processing framework", J. Ambient Intell. Humaniz. Comput., vol. -, no. -, 2022, pp. .

[17] S. Cimato, G. Gianini, M. Sepehri, R. Asal, E. Damiani, "A cryptographic cloud-based approach for the mitigation of the airline cargo cancellation problem", Journal of Information Security and Applications, vol. 51, 2020, pp. 1-21.

[18] C. Blundo, S. Cimato and L. Siniscalchi, "Managing Constraints in Role Based Access Control", IEEE Access, vol. 8, 2020, pp. 140497140511. [bibtex] [pdf] [doi]

[19] E. Damiani, V. Bellandi, S. Cimato, G. Gianini and A. Zilli, "Towards Economics-Aware Risk Assessment on the cloud", *IEEE Security and Privacy*, vol. 13, no. 6, pp. 30-37, IEEE Computer Society, New York, USA, 2015. ISSN 1540-7993

[20] M. Sepehri, S. Cimato and E. Damiani, "Privacy-Preserving Query Processing by Multi-Party Computation", *The Computer Journal*, vol. 58(10), pp. 2195-2212, Oxford University Press, Oxford, UK, 2015. ISSN: 0010-4620

[21] M. Hadavi, R. Jalili, E. Damiani, and S. Cimato, "Security and searchability in secret sharing-based data outsourcing", *International Journal of Information Security*, vol. 14 (6), pp. 513-529, 2015. ISSN:1615-5262

[22] E. Damiani, S. Cimato and G. Gianini,"A risk model for cloud processes", *The ISecure International Journal on Information Security*, vol.6(2), pp. 99-123, ISC, 2014. ISSN: 2008-2045

[23] S. Cimato, James C.N. Yang, and Chih-Cheng Wu, "Visual Cryptography Based Watermarking" in *Transactions on Data Hiding and Multimedia Security*, vol 8363, pp. 91-109, Springer, USA, 2014. ISBN: 978-3-642-55045-4

[24] S. Abbasi, S. Cimato and E. Damiani, "Clustering Models in Secure Clustered Multiparty Computation" in *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol 4:2, pp. 63-76, ISYOU, June 2013. ISSN: 2093-5374

[25] F. Kerschbaum, A. Schropfer, A. Zilli, R. Pibernik, O. Catrina, S. de Hoogh, B. Schoenmakers, S. Cimato and E. Damiani *Secure Collaborative Supply-Chain Management* in IEEE Computer, vol 9, 38-43, IEEE, September 2011.

[26] C. Blundo, S. Cimato, S. De Capitani di Vimercati, A. De Santis, S. Foresti, S. Paraboschi, and P. Samarati *Managing Key Hierarchies for Access Control Enforcement: Heuristic Approaches* in Computers & Security, vol 29(5), pp 533-547, Elsevier, July2010

[27] S. Cimato, R. Sassi e F. Scotti *Biometrics and Privacy* Recent Patents on Computer Science Volume 1 (2):98-109, Bentham Publisher, USA, 2008

[28] S. Cimato, R. De Prisco e A. De Santis, *"Colored visual cryptography without color darkening"* in Theoretical Computer Science 374 (1–3): 261-276, Elsevier, Essex, UK, 2007.

[29] C. Blundo, S. Cimato e A. De Santis, *"Visual Cryptography Schemes with Optimal Pixel Expansion"* in Theoretical Computer Science 369: 169-182, Elsevier, Essex, UK, 2006.

[30] S. Cimato, R. De Prisco e A. De Santis, *Probabilistic Visual Cryptography Schemes* The Computer Journal, 49: 97-107, Oxford University Press, Oxford, UK, 2006.

[31] S. Cimato, A. Cresti e P. D'Arco, *"A Unified Model for Unconditionally Secure Key Distribution"*, Journal of Computer Security, 14(1), pp. 45-64, IOS Press, Amsterdam, The Netherlands, 2006.

[32] S. Cimato, A. De Santis e U. Ferraro *"Overcoming the Obfuscation of Java Programs by Identifiers Renaming"*, in Journal of Systems and Software, Vol. 78, Issue 1, pp 60-72, Elsevier, New York, USA, 2005.

[33] S. Cimato, R. De Prisco e A. De Santis, *"Optimal Colored Threshold Visual Cryptography Schemes"*, in Designs, Codes and Cryptography, Vol 35, N. 3, pp. 311-335, Kluwer Academic Publishers, Norwell, USA, 2005.

[34] S. Cimato, A. De Santis, A. L. Ferrara, and B. Masucci, *"Ideal Contrast Visual Cryptography Schemes with Reversing*, in Information Processing Letters, Volume: 93, Issue: 4 ,pp. 199-206, Elsevier, Amsterdam, The Netherlands, 2005.

[35] C. Blundo, S. Cimato e A. De Bonis, *"Secure E-Coupons"*, in Electronic Commerce Research, vol 5, No. 1, Kluwer Academic Publishers, Norwell MA, USA, 2005.

[36] C. Blundo e S. Cimato, *"A Software Infrastructure for Authenticated Web Metering"*, in IEEE Computer, Vol. 37, No. 4, pp. 28-33, IEEE Computer Society Press, Loas Alamitos CA, USA, 2004.

[37] C. Blundo, S. Cimato e B. Masucci, *"A Note on Optimal Metering Schemes"*, Information Processing Letters, vol. 84/6, pp. 319–326, Elsevier, Amsterdam, The Netherlands, 2002.

[38] P. Ciancarini, S. Cimato e C. Mascolo, *"Engineering Formal Requirements: an Analysis and Testing Method for Z Documents"*, Annals of Software Engineering, vol. 3, pp. 189–220, Kluwer Academic Publisher, The Netherlands, 1997.

5.4 Chapters in books

[39] E. Damiani, V. Bellandi, S. Cimato, G. Gianini, "Possibilistic assessment of process-related disclosure risks on the cloud", in *Computational Intelligence and Quantitative Software*, W. Pedrycz, G. Succi, A. Sillitti, Eds., Springer, in press, pp. 385-405, 2015.

[40] icet15 S. Cimato, S. Mella and R. Susella, "Partial Key Exposure Attacks on RSA with Exponent Blinding", in *E-Business and Telecommunications - 12th International Joint Conference, ICETE 2015*, Colmar, France, July 20-22, 2015, Revised Selected Papers, 2015, pp. 364385.

[41] S. Cimato, V. Ciriani and M. Moroni, "Minimization of ESOP Forms for Secure Computation", in *Problems and New Solutions in the Boolean Domain*, B. Steinbach, Ed., Cambridge Scholars Publishing, in press, pp. 241-254, 2015.

[42] S. Cimato "Image Watermarking Using Visual Cryptography", in *Steganography and Watermarking*, Nova Science Publishers, USA, September 2012. ISBN: 9781626183131

[43] S. Cimato, R. De Prisco, and A. de Santis *Visual Cryptography for Color Images* in "Visual Cryptography and Secret Image Sharing", CRC Press, Boca Raton, USA, August 2011

[44] S. Cimato, R. De Prisco, and A. de Santis *Probabilistic Visual Cryptography* in "Visual Cryptography and Secret Image Sharing", CRC Press, Boca Raton, USA, August 2011

[45] S. Cimato, M. Gamassi, V. Piuri, R. Sassi, F. Scotti, *"Privacy in Biometrics"* in Biometrics: Theory, Methods and Applications, N. Boulgoris, E. Micheli-Tzanakou, K. Patanionis editors (IEEE/Wiley press), 2008

[46] C. Blundo, S. Cimato e B. Masucci, *"Secure Metering Schemes"*, in Network Security, Scott C.-H. Huang, David MacCallum, Ding-Zhu Du (editors), Springer-Verlag New York Inc., 2008

5.5 International Conferences

[47] E. Bellini, I. Aversa, S. Cimato, A. Esposito, "A Blockchain-based Trustworthy Cloud Services Digital Ecosystem", in IEEE International Conference on Cyber Security and Resilience, CSR 2022, Rhodes, Greece, July 27-29, 2022, IEEE, pp. 118124.

[48] E. Bellini, S. Cimato, E. Damiani, B. D. Martino, A. Esposito, "Towards a Trustworthy Semantic-Aware Marketplace for Interoperable Cloud Services", in Complex, Intelligent and Software Intensive Systems - Proceedings of the 15th International Conference on Complex, Intelligent and Software Intensive Systems (CISIS-2021), Asan, Korea, 1-3 July 2021, L. Barolli, K. Yim, T. Enokido, Eds., Springer, pp. 606615.

[49] C. Braghin, S. Cimato, E. Damiani, F. Frati, E. Riccobene, S. Astaneh, "Towards the Monitoring and Evaluation of Trainees' Activities in Cyber Ranges", in Model-driven Simulation and Training Environments for Cybersecurity - Second International Workshop, MSTEC 2020, Guildford, UK, September 14-18, 2020, Revised Selected Papers, G. Hatzivasilis, S. Ioannidis, Eds., Springer, pp. 7991.

[50] L. Mauri, S. Cimato and E. Damiani, "A Formal Approach for the Analysis of the XRP Ledger Consensus Protocol", in Proceedings of the 6th International Conference on Information Systems Security and Privacy, ICISSP 2020, Valletta, Malta, February 25-27, 2020, S. Furnell, P. Mori, E. R. Weippl, O. Camp, Eds., SCITEPRESS, pp. 5263.

[51] A. Bernasconi, S. Cimato, V. Ciriani, M. C. Molteni, "Multiplicative Complexity of Autosymmetric Functions: Theory and Applications to Security", in 57th ACM/IEEE Design Automation Conference, DAC 2020, San Francisco, CA, USA, July 20-24, 2020, IEEE, pp. 16. [bibtex] [pdf] [doi]

[52] S. Cimato, S. Nicol, "Towards Efficient and Secure Analysis of Large Datasets", in 44th IEEE Annual Computers, Software, and Applications Conference, COMPSAC 2020, Madrid, Spain, July 13-17, 2020, IEEE, pp. 13511356.

[53] L. Mauri, E. Damiani and S. Cimato, "Be Your Neighbor's Miner: Building Trust in Ledger Content via Reciprocally Useful Work", in 13th IEEE International Conference on Cloud Computing, CLOUD 2020, Virtual Event, 18-24 October 2020, IEEE, pp. 5362. [bibtex] [pdf] [doi]

[54] S. Cimato, V. Ciriani, E. Damiani, M. Ehsanpour, "An OBDD-Based Technique for the Efficient Synthesis of Garbled Circuits", in Security and Trust Management - 15th International Workshop, STM 2019, Luxembourg City, Luxembourg, September 26-27, 2019, Proceedings, pp. 158167. [bibtex] [pdf] [doi]

[55] C. Braghin, S. Cimato, E. Damiani, F. Frati, L. Mauri, E. Riccobene, "A Model Driven Approach for Cyber Security Scenarios Deployment", in Computer Security - ESORICS 2019 International Workshops, IOSec, MSTEC, and

FINSEC, Luxembourg City, Luxembourg, September 26-27, 2019, Revised Selected Papers, A. P. Fournaris, M. Athanatos, K. Lampropoulos, S. Ioannidis, G. Hatzivasilis, E. Damiani, H. Abie, S. Ranise, L. Verderame, A. Siena, J. Garca-Alfaro, Eds., Springer, pp. 107122.

[56] C. Braghin, S. Cimato, S. R. Cominesi, E. Damiani, L. Mauri, "Towards Blockchain-Based E-Voting Systems", in Business Information Systems Workshops - BIS 2019 International Workshops, Seville, Spain, June 26-28, 2019, Revised Papers, pp. 274286.

[57] C. Braghin, S. Cimato, E. Damiani, M. Baronchelli (2018). Designing smart-contract based auctions. In: 2nd International Conference on Security with Intelligent Computing and Big-data Services (SICBS 2018). Springer, Guilin, China, 2018

[58] C. Braghin, S. Cimato, A. Della Libera (2018). Are mHealth Apps Secure? : A Case Study. In: IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC 2018). p. 335-340, IEEE

[59] L. Mauri, S. Cimato and E. Damiani, "A Comparative Analysis of Current Cryptocurrencies", in Proceedings of the 4th International Conference on Information Systems Security and Privacy, ICISSP 2018, Madeira, Portugal, January 22-24, 2018, pp. 127-138.

[60] S. Cimato, V. Ciriani, E. Damiani, M. Ehsanpour, "A Multiple Valued Logic Approach for the Synthesis of Garbled Circuits", in 2018 IFIP/IEEE 25th International Conference on Very Large Scale Integration, VLSI-SoC 2017, ABU Dhabi, UAE, October 22-25, 2018, pp. 232-236.

[61] M. Ehsanpour, S. Cimato, V. Ciriani, E. Damiani, "Exploiting Quantum Gates in Secure Computation", in Euromicro Conference on Digital System Design, DSD 2017, Vienna, Austria, August 30 - Sept. 1, 2017, pp. 291294.

[62] C. Blundo, S. Cimato and L. Siniscalchi, "PRUCC-RM: Permission-Role-Usage Cardinality Constrained Role Mining", in 41st IEEE Annual Computer Software and Applications Conference, COMPSAC 2017, Turin, Italy, July 4-8, 2017. Volume 2, pp. 149154.

[63] M. Sepehri, S. Cimato and E. Damiani, "Efficient Implementation of a Proxy-based Protocol for Data Sharing on the Cloud", in *Proceedings of the Fifth ACM International Workshop on Security in Cloud Computing, SCC at AsiaCCS 2017*, Abu Dhabi, United Arab Emirates, April 2, 2017, pp. 6774.

[64] E. Damiani, P. J. Houngbo, J. Hounsou, R. Asal, S. Cimato, F. Frati, D. Shehada, C. Y. Yeun, "Porting the Pay with a (Group) Selfie (PGS) payment system to crypto currency", in *Africatek 2017 - Proceedings of The 1st EAI International Conference on Emerging Technologies for Developing Countries*, Marrakech, Morocco, March 27-28, 2017., pp. .

[65] C. Yang, S. Cimato, J. Wu, S. Cai, "3-Out-of-n Cheating Prevention Visual Cryptographic Schemes", in *Proceedings of the 2nd International Conference on Information Systems Security and Privacy, ICISSP 2016*, Rome, Italy, February 19-21, 2016., pp. 400406.

[66] S. Cimato, E. Damiani, S. Mella, C. Yang, "Key Recovery in Public Clouds: A Survey on Cross-VM Side Channel Attacks", in *Cloud Computing and Security - Second International Conference, ICCCS 2016*, Nanjing, China, July 29-31, 2016

[67] M. Sepehri, S. Cimato, E. Damiani, C. Y. Yeuny, "Data Sharing on the Cloud: A Scalable Proxy-Based Protocol for Privacy-Preserving Queries", in *Proceedings of the 7th IEEE International Symposium on Ubisafe Computing in conjunction with 14th IEEE Conference on Trust, Security and Privacy in Computing and Communications,TrustCom/BigDataSE/ISPA*, Helsinki, Finland, August 20-22, 2015, Volume 1, pp. 13571362.

[68] S. Cimato, E. Damiani, F. Frati, J. T. Hounsou, J. Tandjikpon, "Paying with a Selfie: a Hybrid Micro-Payment Framework Based on Visual Cryptography", in *7th EAI International Conference on e-Infrastructure and e-Services for Developing Countries (Africomm15)*, Cotonou, Benin, December 1516, 2015.

[69] M. Sepehri, S. Cimato and E. Damiani, "Data Sharing on the Cloud: A Scalable Proxy-based Protocol for Privacy Preserving Queries", in *Proceedings of the 7th IEEE International Symposium on Ubisafe Computing in conjunction with 14th IEEE Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, Helsinky, Finland, August 20-22, 2015.

[70] S. Cimato, S. Mella and R. Susella, "New Results for Partial Key Exposure on RSA with Exponent Blinding", in *SECRYPT 2015 - Proceedings of the 12th International Conference on Security and Cryptography*, Colmar, Alsace, France, pp. 136147, 20-22 July, 2015.

[71] S. Cimato, V. Ciriani, and M.Moroni, "ESOP Synthesis for Secure Computation", in *10th International Workshop on Boolean Problems (IWSBP14)*, Freiberg , Germany, 17-19 September 2014.

[72] S. Cimato, "Visual Cryptography Schemes for Graph Based Access Structures", in *Proceedings of the 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2013)* page 365-368,Bejing, China, 15-18 October 2013. ISBN: 9780769551203

[73] M. Sepehri, S. Cimato, E. Damiani, "A Multi-Party Protocol for Privacy-Preserving Range Queries", in *Proceedings of the 10th Secure Data Management Workshop (SDM 2013)*,Riva del Garda (Trento), Italy, August 2013. ISBN 978-3-319-06810-7

[74] S. Cimato, E. Damiani, R. Menicocci, and F. Zavatarelli, "Towards the certification of cloud services" in *IEEE 2013 International Workshop On Security and Privacy Engineering, Assurance, and Certification (SPEAC 2013), 2013 IEEE Ninth World Congress on Services (SERVICES 2013)*, page 100-105, Santa Clara, USA, June 2013. ISBN: 9780769550244

[75] M. Sepehri, S. Cimato, and E. Damiani, "A Scalable Multi-Party Protocol for Privacy-Preserving Equality Test" in *International Workshop on Information Systems Security Engineering (WISSE 2013), CAiSE Workshops 2013*, pp. 466-477, Valencia, Spain, June 2013. ISBN: 9783642384899

[76] S. Abbasi, S. Cimato, and E. Damiani, " Toward Secure Clustered Multi-Party Computation: A Privacy-Preserving Clustering Protocol", in *Proceedings of ICT-EurAsia 2013*, LNCS 7804, pp. 447.452, Yogyakarta, Indonesia, 2013. ISBN: 9783642368172

[77] R. Tchokpon, S. Cimato and N. Bennani, "Ensuring XML Integrity using Watermarking Techniques", in *Proceedings of 8th International Conference on Signal Image Technology & Internet Based Systems (SITIS 2012)*, IEEE Computer Society, Sorrento - Naples, Italy, 25-29, November 2012. ISBN: 9781467351522

[78] S. Cimato, Ching-Nung Yang and Chih-Cheng Wu, "Visual Cryptography based Watermarking:Definition and Meaning", in *prooceddings of 11th International Workshop on Digital-forensics and Watermarking (IWDW 2012)*, LNCS 7809, 31 October- 3 November, Shanghai, China, 2012. ISBN: 9783642400988

[79] C. Blundo and S. Cimato "Constrained Role Mining", in *Proceedings 8th International Workshop on Security and Trust Management (STM 2012)* in conjunction with ESORICS 2012, LNCS 7783, Pisa, Italy - September 13-14, 2012. ISBN: 9783642380037

[80] M. Ali Hadavi, E. Damiani, R. Jalili, S. Cimato and Z. Ganjei, "AS5: A Secure Searchable Secret Sharing Scheme for Privacy Preserving Database Outsourcing", in *proceedings of 5th International Workshop on Autonomous and Spontaneous Security (SETOP 2012)*, in conjunction with ESORICS 2012, LNCS 7731, Pisa, Italy - September 13-14, 2012. ISBN: 9783642358890

[81] E. Damiani, S. Cimato, G. Gianini "Risk assessment of credit securities : the notion and the issues.", in *Proceedings 6th IEEE International conference on digital ecosystems technologies - Complex environment engineering : IEEE (DEST-CEE 2012)*, Campione d'Italia. Campione d'Italia, Italy, June 18-20,2012. ISBN: 9781467317023

[82] M. Anisetti, E. Damiani, S. Cimato, F. Frati, G.Gianini Using Incentive Schemes to Alleviate Supply Chain Risks. In: Proc. of the International Conference on Management of Emergent Digital EcoSystems (MEDES) , Bangkok, Thailand, October, 26-29, 2010

[83] F. Benali, N. Bennani, G.Gianini and S.Cimato *A Distributed and Privacy-preserving Method for Network Intrusion Detection* In: Proc. of the 12th International Symposium on Distributed Objects, Middleware, and Applications (DOA'10), Crete, Greece, October 26-29, 2010

[84] N. Bennani, S.Cimato and E. Damiani *Toward cloud-based key management for outsourced databases* . In: Proc. of the 2nd IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2010), Seoul, Korea, July 19-23, 2010

[85] C. Blundo, S. Cimato, *"A Simple Role Mining Algorithm"*. In: Proc. of the 25th ACM Symposium on Applied Computing 2010. (SAC 2010). Crans-Montana, Switzerland, March 22-25, 2010.

[86] C. Blundo, S. Cimato, S. De Capitani Di Vimercati, A. De Santis, S. Foresti, S. Paraboschi, P. Samarati, *"Efficient Key Management for Enforcing Access Control in Outsourced Scenarios"*, in Proc. of the 24th IFIP TC-11 International Information Security Conference (SEC 2009). Cyprus, Greece, May 18-20S.

[87] Stelvio Cimato, Ernesto Damiani, and Gabriele Gianini *"Privacy Preserving Risk Assessment of Credit Securities"*, in Proceedings of 5th International Conference on Signal Image Technology and Internet Based Systems (SITIS 09), Workshop on Security and Privacy in Telecommunication Systems (SePTIS), Marrakech, Morocco, 29-11, 4-12, 2009

[88] S. Cimato, M. Gamassi, V. Piuri, R. Sassi and F. Scotti , *"Privacy-aware Biometrics: Design and Implementation of a Multimodal Verification System"* in Proceedings of Annual Computer Security Applications Conference (ACSAC) 2008 , Anheim, California, USA, Dec. 8-12 2008.

[89] P. Ceravolo, S. Cimato, F. Frati. C. Fugazza, E. Damiani, G. Gianini, S. Marrara, O. Scotti *"Hazards in Full-Disclosure Supply Chains"* in Advanced Information Technologies for Management (AITM'2008), Wroclaw, Poland 2008

[90] P. Ceravolo, S. Cimato, E. Damiani, G. Gianini, C. Fugazza, S. Marrara *"Risk Management and information Disclosure in Supply Chain Analysis"* in Advanced Information Technologies for Management (AITM'2008), Wroclaw, Poland 2008

[91] S. Cimato, *"A Lightweight Protocol for Dynamic RFID Identification"*, in 3rd IEEE International Workshop on Security, Trust, and Privacy for Software Application(STPSA 2008) in conjunction with IEEE COMPSAC 2008, Turku, Finland, IEEE Computer Press, Luglio 2008

[92] E. Damiani, P. Ceravolo, S. Cimato, G. Gianini, *"Obfuscation for the common good"* accettato in 3rd conference on Security of Network Architectures and Information Systems (SAR/SSI2008), Loctudy, Francia, Publibook, 2008

[93] S. Cimato, M. Gamassi, V. Piuri, R. Sassi e F. Scotti, *"A multi-biometric verification system for the privacy protection of iris templates"*, accettato per pubblicazione in Proceedings of the second International Conference on Complex Intelligent and Software Intensive Systems (CISIS 2008), genova, Italy, Springer, September 2008

[94] S. Cimato, M. Gamassi, V. Piuri, R. Sassi e F. Scotti, *"A biometric verification system addressing privacy concerns"*, in IEEE International Conference on Computational Intelligence and Security (CIS 2007) Harbin, China, December 2007, IEEE Computer Society Press, Washington USA, 2007.

[95] V. Auletta, C. Blundo, S. Cimato, E. De Cristofaro and G. Raimato, *"Authenticated Web Services: A WS-Security Based Implementation "*, in International Conference on New Technologies, Mobility and Security (NTMS'07), Paris, France, Kluwer Academic Publishers Group, The Netherlands, May 2007.

[96] S. Cimato, M. Gamassi, V. Piuri, D. Sana, R. Sassi and F. Scotti, *"Personal identification and verification using multimodal biometric data"*, in IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety (CIHSPS 2006), New York, IEEE Computer Society Press, USA, October 2006.

[97] V. Auletta, C. Blundo, S. Cimato, e G. Raimato, *"A Web Service Based Micro-payment System"*, in Proceedings of IEEE Symposium on Computers and Communications (ISCC'06), Pula, Italia, IEEE Computer Society Press, Washington USA, Giugno 2006.

[98] S. Cimato, C. Galdi, R. Giordano, B. Masucci e G. Todisco, *"Design and Implementation of a Certified Email Service"*, in Proceedings of 4th International Conference. on Cryptology and Network Security (CANS 2005), vol. 3810 di Lecture Notes in Computer Science, pp. 186-199, Xiamen, Cina, Springer Verlag Berlin Heidelberg, Germany, Dicembre 2005.

[99] C. Blundo, S. Cimato and R. De Prisco, *"A Lightweight Approach to Authenticated Web Caching"*, in Proceedings of 2005 International Symposium on Applications and the Internet (SAINT 2005), pp. 157–163, Trento, Italy, IEEE Computer Society Press, Washington, USA, January 2005.

[100] C. Blundo e S. Cimato, *"A Framework for Authenticated Web Services"*, in *Proceedings of European Conference on Web Services (ECOWS 04)*, vol. 3250 di Lecture Notes in Computer Science, pp. 61-71, Springer Verlag, Erfurt, Germany, September 2004.

[101] S. Cimato, R. De Prisco and A. De Santis, "Colored Visual Cryptography without Color Darkening", in *Proceedings of Fourth Conference on Security in Communication Networks '04 (SCN 04)*, vol. 3352 di Lecture Notes in Computer Science, pp. 235-248, Springer Verlag, Amalfi, Italy, September 2004.

[102] V. Auletta, C. Blundo, S. Cimato and G. Raimato *"A Web Service for Certified Email"*, in pubblicazione nei *Proceedings of International Workshop on Certification and Security in Inter-Organizational E-Services (CSES 2004)*, Toulouse , France, Springer-IFIP, USA, August 2004.

[103] C. Blundo e S. Cimato, *"A Platform for Secure E-Gambling"*, *Proceedings of the International Conference on Information Technology: Coding and Computing, (ITCC'04)*, pp.768-772 IEEE Computer Society Press, Washington USA, 2004.

[104] C. Blundo, S. Cimato, R. De Prisco e A. Ferrara, *"Modeling A Certified Email Protocol using I/O Automata"*, accettato e in fase di pubblicazione in *Proceedings of the First MEFISTO Workshop*, Electronic Notes in Theoretical Computer Science, vol. 99, pp. 339-359, Elsevier, 2004.

[105] S. Cimato, P. D'Arco e I. Visconti, *"Anonymous Group Communication in Mobile Networks"*, *Proceedings of the 8th Italian Conference on Theoretical Computer Science, (ICTCS'03)*, vol. 2841 di Lecture Notes in Computer Science, pp. 316-328, Springer Verlag, 2003.

[106] C. Blundo, S. Cimato e R. De Prisco, *"Certified Email: Design and Implementation of a New Optimistic Protocol"*, *Proceedings of the 8th IEEE Symposium on Computers and Communications (ISCC'03)*, pp. 828–833, IEEE Computer Society Press, Washington USA, 2003.

[107] S. Cimato, R. De Prisco e A. De Santis, *"Contrast Optimal Colored Visual Cryptography Schemes"*, *Proceedings of 2003 IEEE International Theory Workshop (ITW'03)*, pp. 139–142, IEEE, 2003.

[108] C. Blundo e S. Cimato, *"SAWM: A Tool for Authenticated Web Metering"*, *Proceedings 14th International Conference on Software Engineering and Knowledge Engineering (SEKE'02)*, pp. 641–648, ACM Press, New York, USA, 2002.

[109] C. Blundo, S. Cimato e A. De Bonis, *"A Ligthweight Protocol for the Generation and Distribution of Secure E-Coupons"*, *Proceedings of the 11th World Wide Web Conference (WWW'02)*, pp. 542–552, ACM Press, New York, USA, 2002.

[110] C. Blundo e S. Cimato, *"Authenticated Metering"*, *Poster Proceedings of the 11th World Wide Web Conference (WWW'02)*, ACM Press, 2002.

[111] S. Cimato, *"Design of an Authentication Protocol for GSM Javacards"*, in *Proceedings of the 4th International Conference on Information Security and Cryptology (ICISC 2001)*, vol. 2288 di Lecture Notes in Computer Sciences, pp. 355–368, Springer Verlag, London, UK, 2001.

[112] S. Cimato e A. De Bonis, *"Online Advertising: Secure E-Coupons"*, *Proceedings of the 7th Italian Conference on Theoretical Computer Science (ICTCS'01)*, vol. 2202 di Lecture Notes in Computer Sciences, pp. 370–383, Springer Verlag, London, UK, 2001.

[113] S. Cimato e P. Ciancarini, *"A Formal Approach to the Specification of Java Components"*, in *Workshop on Formal Techniques for Java Programs (ECOOP'99)*, Lisbon, Portugal, 1999. Appeared also in *Object-Oriented Technology, ECOOP'99 Workshop Reader, Workshops, Panels, and Posters*, vol. 1743 di Lecture Notes in Computer Sciences, pp. 107–108, Springer Verlag, London, UK, 1999.

[114] S. Cimato, *"Specifying Component-based Java Applications"*, *Proceedings of the Third International Conference on Formal Methods for Open Object–Based Distributed Systems (FMOODS '99)*, pp. 105-112, Kluwer Academic Publishers, The Netherlands, 1999.

[115] P. Ciancarini e S. Cimato, *"Specifying Component-based Software Architectures"*, *Workshop on Foundations of Component Based Systems (ESEC/FSE'97)*, pp. 60–70, 1997.

[116] S. Cimato e C. Mascolo, *"Analyzing and Animating Declarative Specifications"*, *Proceedings of Joint Conference on Declarative Programming (APPIA-GULP-PRODE)*, M. Martelli and M. Navarro, Eds., 1996.

[117] P. Ciancarini e S. Cimato, *"Animating a Non-executable Formal Specification with a distributed symbolic language"*, *Proceedings of the International Symposium on Design and Implementation of Symbolic Computation Systems (DISCO'96)*, vol. 1128 di Lecture Notes in Computer Science, pp. 200–201 Springer-Verlag, London, UK, 1996.

[118] P. Ciancarini, S. Cimato e C. Mascolo, *"Engineering Formal Requirements: Analysis and Testing"*, *Proceedings of 8th International Conference on Software Engineering and Knowledge Engineering (SEKE'96)*, pp. 385–392, ACM Press, 1996.

5.6 Patents

[119] Cimato S., Gamassi M., Piuri V., Sana D., Sassi R., Scotti F. METHOD FOR GENERATING AND VERIFYING SECURITY INFORMATION OBTAINED BY MEANS OF BIOMETRIC READINGS *Metodo di generazione*

e di verifica di una informazione di sicurezza ottenuta mediante letture biometriche N. MI2006A000641. Università degli Studi di Milano. Domanda di brevetto depositata il 31 Marzo 2006.

5.7 Other Publications

[120] Fabio Scotti, Stelvio Cimato and Roberto Sassi *Biometric Privacy* in Encyclopedia of Cryptography and Security (2nd Ed.) 2011: 101-104.

[121] S. Cimato, M. Gamassi, V. Piuri, R. Sassi, F. Scotti,*Privacy Issues in Biometric Identification*, in Information Security 2006, Nigel Llyod ed., Touch Briefings, pp 40-42, 2006