LIST OF TITLES AND PUBLICATIONS OF THE CANDIDATE

STELVIO CIMATO

Birth date 21/07/1968

Scientific publications

1. 2013 - Contributo in Atti di convegno

2. 2013 - Contributo in Atti di convegno

3. 2013 - Contributo in volume (Capitolo o Saggio)

4. 2013 - Contributo in Atti di convegno

5. 2013 - Contributo in Atti di convegno

6. 2013 - Articolo in rivista

7. 2013 - Contributo in Atti di convegno

8. 2013 - Contributo in Atti di convegno

9. 2012 - Contributo in Atti di convegno

10. 2012 - Contributo in Atti di convegno

11. 2011 - Curatela

12. 2011 - Contributo in volume (Capitolo o Saggio)

13. 2011 - Contributo in volume (Capitolo o Saggio)

14. 2011 - Voce (in dizionario o enciclopedia)

15. 2011 - Articolo in rivista

16. 2010 - Articolo in rivista

17. 2010 - Contributo in Atti di convegno

18. 2010 - Contributo in Atti di convegno

19. 2010 - Contributo in Atti di convegno


20. 2010 - Contributo in Atti di convegno


21. 2010 - Contributo in volume (Capitolo o Saggio)


22. 2010 - Contributo in volume (Capitolo o Saggio)


23. 2009 - Contributo in Atti di convegno


24. 2009 - Contributo in Atti di convegno


25. 2009 - Contributo in Atti di convegno


26. 2009 - Contributo in volume (Capitolo o Saggio)


27. 2008 - Contributo in Atti di convegno


28. 2008 - Contributo in Atti di convegno


29. 2008 - Contributo in Atti di convegno

30. 2008 - Contributo in Atti di convegno

31. 2008 - Contributo in Atti di convegno

32. 2008 - Articolo in rivista

33. 2008 - Curatela

34. 2007 - Contributo in Atti di convegno

35. 2007 - Contributo in Atti di convegno

36. 2007 - Articolo in rivista

37. 2007 - Brevetto

38. 2006 - Articolo in rivista

39. 2006 - Contributo in Atti di convegno

40. 2006 - Contributo in Atti di convegno
Cimato S, M. Gamassi, V. Piuri, D. Sana, R. Sassi and F. Scotti (2006). Personal identification and...

41. 2006 - Articolo in rivista

42. 2006 - Brevetto

43. 2006 - Articolo in rivista

44. 2005 - Articolo in rivista

45. 2005 - Articolo in rivista

46. 2005 - Contributo in Atti di convegno

47. 2005 - Contributo in Atti di convegno

48. 2005 - Curatela

49. 2005 - Articolo in rivista

50. 2005 - Articolo in rivista

51. 2004 - Contributo in Atti di convegno
52. 2004 - Contributo in Atti di convegno


53. 2004 - Contributo in Atti di convegno


54. 2004 - Articolo in rivista


55. 2004 - Articolo in rivista


56. 2004 - Contributo in Atti di convegno


57. 2003 - Contributo in Atti di convegno


58. 2003 - Contributo in Atti di convegno


59. 2003 - Contributo in Atti di convegno


60. 2003 - Curatela


61. 2002 - Articolo in rivista

C. BLUNDO, CIMATO S, B. MASUCCI (2002). A note on optimal metering schemes. INFORMATION PROCESSING LETTERS, vol. 84, p. 319-326, ISSN: 0020-0190 [with attachment and copyright]

62. 2002 - Contributo in Atti di convegno


63. 2002 - Contributo in Atti di convegno


64. 2002 - Contributo in Atti di convegno


65. 2001 - Contributo in Atti di convegno

66. 2001 - Contributo in Atti di convegno

67. 1999 - Contributo in Atti di convegno

68. 1997 - Articolo in rivista

69. 1997 - Contributo in Atti di convegno

### Titles

Scientific participation in international and national research projects, selected for funding based on calls that involved competitive peer review

<table>
<thead>
<tr>
<th>Project</th>
<th>Period</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>European Project FP7: PRACTICE (Privacy-Preserving Computation in the Cloud) FP7- 609611 (2013-16)</td>
<td>36</td>
<td>Participant</td>
</tr>
<tr>
<td>European Project FP7: CUMULUS (Certification infrastructure for multi-layer cloud services) FP7-318580 (2012-2015)</td>
<td>36</td>
<td>Participant</td>
</tr>
<tr>
<td>European Project FP7: ASSERT4SOA (Advanced Security Service cERTificate for SOA) FP7-257351 (2010-2013)</td>
<td>36</td>
<td>Participant</td>
</tr>
<tr>
<td>European Project FP7: SecureSCM (Secure Supply Chain Management) FP7- 213531 (2008-2011)</td>
<td>36</td>
<td>Participant</td>
</tr>
<tr>
<td>PRIN 2010: GenData 2020 (Data-Centric Genomic Computing), Responsabile Prof. S. Ceri, Unità di ricerca di Milano, resp. prof. P. Samarati</td>
<td>36</td>
<td>Participant</td>
</tr>
<tr>
<td>PRIN 2008: PEPPER: Privacy E Protezione di dati PERsonali, Responsabile Prof. S. Paraboschi, Unità di ricerca di Milano, resp. prof. P. Samarati</td>
<td>24</td>
<td>Participant</td>
</tr>
<tr>
<td>PRIN 2006: Basi di dati crittografate, Responsabile Prof. S. Paraboschi, Unità di ricerca di Milano,</td>
<td>24</td>
<td>Participant</td>
</tr>
</tbody>
</table>
resp. prof. P. Samarati

PRIN 2002 MEFISTO: Metodi Formali per la Sicurezza e il Tempo, Responsabile Prof. R. Gorrieri, 24 Participant
Unità di Ricerca di Salerno, resp. prof. M. Napoli

CNR-Agenzia 2000 (G008BS3): Pubblicità Online: Nuove Misure per Nuovi Media. Auditing e Accounting Sicuro sul Web 12 Participant

Partecipation in editorial boards of journals, collections of books, encyclopedias and treatises

<table>
<thead>
<tr>
<th>Type</th>
<th>Title</th>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Riviste</td>
<td>Recent Patents on Computer Science, Bentham publisher</td>
<td>01/2008</td>
<td>10/2013</td>
</tr>
</tbody>
</table>

achievements in technology transfer in terms of participation in the creation of new enterprises (spin off), development, deployment and commercialisation of patents

-From January 2008 to April 2010 he has been associate co-founder and scientific advisor for SENSURE, spin-off created by Università degli Studi di Milano (Dipartimento di Tecnologie dell'Informazione) and Politecnico di Milano - Dipartimento di Elettronica e Informazione

other titles

ACADEMIC QUALIFICATIONS
-February 99 Ph.D in Computer Science at Università degli Studi di Bologna consortiumed with Università degli Studi di Padova e Venezia.
-June94 Laurea degree in Scienze dell'Informazione at Università degli Studi di Salerno, 110/110 cum laude.

TEACHING ACTIVITIES
He taught the following courses for the Laurea in Sicurezza dei Sistemi e delle Reti Informatiche (Crema) and the Laurea Magistrale in Scienze e Tecnologie dell'Informazione (Crema) at the Department of Computer Science, Matematiche, Fisiche e Naturali of the Università degli Studi di Milano:
- Teacher for the "Corso di Crittografia" (6 cfu 48 hours, 2004-today)
- Teacher for the "Corso di Crittografia (ONLINE)" (6 cfu 48 hours, 2005-today)
- Teacher for the "Corso di Laboratorio di Crittografia Applicata" (6 cfu - 48 hours 2005-2008)
-from 1999 to 2004, he has been involved in several teaching activities for graduate, post graduate, and post high-schools courses organized by the Università degli Studi di Salerno and Università degli Studi di Bologna
- Thesis supervision
From 2005 he has been supervisor for more than 50 students attending the course for the Laurea triennale in Sicurezza dei Sistemi e delle Reti Informatiche (Bachelor students) and more than 16 students attending the course for the Laurea Magistrale in Scienze e Tecnologie dell'Informazione (M.sc students) at the Faculty of Scienze Matematiche, Fisiche e Naturali of the Università degli Studi di Milano.

ACTIVITIES FOR STUDENT RECRUITMENT
- Organization and training for Olympiad in Informatics. The competition tasks are of algorithmic nature: the contestants have to show strong IT skills in problem analysis, design of algorithms and data structures, programming and testing.
- Organization and teaching courses for high school students on "Problem Solving" and "Apps programming for Android platform"

**ACTIVITIES FOR DOCTORAL SCHOOLS**

- In September 2012 he has been member of the thesis committee for the Ph.D student Jacques Machizaud at Université Jean Monnet, Saint Etienne, France ("Cryptographie Visuelle pour l'authentification de documents", under the supervision of prof. Thierry Fournel)
- From 2010 he is member of the Teaching Committee for the Multimedia, Distributed and Pervasive Systems doctoral school organized by the Doctoral school in Computer Science of the Università degli Studi di Milano, by the Chair of Distributed Information Systems of the Faculty of Informatics and Mathematics of the University of Passau and by INSA - University of Lyon.
- From 2011 he is member of the Teaching Committee for the Doctorate School in Computer Science of the Università degli Studi di Milano

**HE**

- Has been co-supervisor for the thesis in Computer Science XXIII Course of the student F. Pagano, titled "A Distributed Approach to Privacy on the Cloud" (completed in 2012)
- He is actually co-supervisor of the following students attending the Doctorate School in Computer Science of the Università degli Studi Milano: Romaric Tchockpon, XXIV course, Maryam Sepehri, XXV course, Arezoo Sedigheh Abbasi, XXVI course

**ACADEMIC SERVICES**

- Member of the Commissione Tirocini e Tesi (Stage and Thesis Committee) from 2007- present
- Member of the Commissione Orientamento (Student Recruitment Committee) from 2010-2012

**COORDINATION OF RESEARCH GROUPS**

- Responsible and coordinator for the Cryptography and Secure Computation Laboratory at the Department of Computer Science of the Università degli Studi di Milano
- Local Projects
- 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.

**INVITED TALKS**

- Visual Cryptography: Watermarking and Novel Applications, invited by Prof. Feng Liu, Director of the Executive Office of State Key Laboratory of Information Security, Institute of Information Engineering Chinese Academy of Sciences, Beijing China, 17 October 2013
- Visual Cryptography: Research Issues and Novel Applications, invited by Prof. T. Fournel, Université de Saint-Etienne, Laboratoire Hubert Curien, Saint-Etienne, France, 26 September 2012
- Data Analysis with Privacy Constraints, CRiSIS 2011. 6th International Conference on. Risks and Security of Internet and Systems, Timisoara, Romania, 26-28 September 2011

INRIA-IRISA, University of Rennes, Francia, October 1998.
ACTIVITIES FOR REVIEWS AND CONFERENCES

- Editorial Board
He has been member of the IEB for the Special Issue of Information Systems Frontiers on Intelligent Systems and Smart Homes, Springer (2007)

-Organization of Conferences:
Organizer and program chair of SAPSE, IEEE International Workshop on Security Aspects of Process and Services Engineering in conjunction with COMPSAC IEEE conference (2009- today):
5th IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2013), Kyoto, Japan, July 22-26, 2013
4th IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2012), Izmir, Turkey July 16-20, 2012
3rd IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2011), Munich, Germany, Jul 18-21, 2011
2nd IEEE International Workshop on Security Aspects of Process and Services Engineering (SAPSE 2010), Seoul, Korea, July 19-23, 2010
General Chair of the 4th Conference on Security in Communication Networks (SCN'04), Amalfi, Italy, September 2004.
Member of the organizing committee of the 17th International Conference on Distributed Computing (DISC'03), Sorrento, Italia, October 2003.
Member of the organizing committee of the conference Security in Communication Network (SCN'02), Amalfi, Italy, September 2002.

-Program Committee for Conferences
He has been member of the following program committees:
IMMM, International Conference on Advances in Information Mining and Management (2011-2012)
SEKE, International Conference on Software Engineering and Knowledge Engineering (2011-2014)
ICME, IEEE International Conference on Multimedia and Expo (2011-2014)
CIS, International Conference on Computational Intelligence and Security (2005-2013)
IDEAL, International Conference on Intelligent Data Engineering and Automated Learning, (2010-2011)

-Refereeing Activities
He is/has been referee for:
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 Internet Computing
IEEE Computers
Journal of Systems and Software, Elsevier
Journal of Computer Security, IOS Press
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
Optical Engineering, SPIE
Telecommunication Systems, Springer
Multimedia, Tools and Applications, Springer

PAPERS ACCEPTED FOR PUBLICATION

PUBLICATIONS SUMMARY
Refereed international journals articles: 15
Refereed papers in proceedings of international conference: 37
Refereed chapters in books: 6
Patents: 1 (with further PCT extension)
Edited Books: 1
Edited Conference Proceedings: 3
Entry in enciclopedy: 1

RESEARCH CONTRIBUTIONS
His main research interests are in the area of cryptography and data security. He is/has been involved in several research projects, has co-edited books, and has written several papers for international journals and conferences. More in detail, research topics include:

1) visual cryptography: research has been directed to the investigation of theoretical limits for both B&W VCS and colored VCS regarding contrast and pixel expansion[41,49,57]. An original model for VCS, i.e. probabilistic VCS, has been proposed and the relationship with traditional model investigated [43]. Novel VCS schemes based on the reversing operation proposed and bounds on contrast have been proposed[44].
An original model for colored VCS has been also introduced and some novel constructions proposed [36,51]. Finally, most recent research contributions have been collected in the edited book [11,12,13] and relationship between VCS and watermarking investigated [3,7]. VCS for graph based access structures have been investigated in [8]

2) biometrics: a novel multi-biometric algorithm has been presented and patented. The privacy implications and some experimental results, obtained considering different combination of biometric traits have been presented in different works[14,23,25,26,28,31,34,37,40,42].
3) web metering and web authentication: Web metering systems let online advertisers control ad exposure and test the effectiveness of their advertising campaigns. Theoretical bounds have been investigated and novel construction proposed [61]. A novel approach has been proposed based on hash chains, which minimizes the communication overhead and provides additional security guarantees. On the same line, protocols for authentication to web services, micro-payment systems and authenticated web caching have been proposed [22,34,39,47,53,54,56,63,64].
4) application of secure computation protocols: secure multi-party computation provides a way to perform advanced data analysis still respecting the privacy requirements of the parties. Application of SMC to the computation of the risk profile of
securitized assets have been considered as well as application to intrusion detection systems. In the context of the SecureSCM project, SMC computation protocols have been practically applied to supply chain management and novel means to define risk profiles for the participants to the collaborative computation proposed[9,15,19,20,21,27,29,31].

5) e-coupons: an innovative approach for e-coupon generation and distribution has been proposed, and its security analyzed considering fake coupons creation and unwanted data modifications[50,62,66].

6) access control: a novel family of RBAC heuristics has been proposed and the extension to the case of constraints on the resulting role-set considered[4, 17]. A novel heuristic for managing key hierarchies (in the context of PRIN 2006-2008 project) and key management for accessing outsourced database have been proposed [16,18,24].

7) certified email: novel protocols for certified mail distribution have been proposed, satisfying additional security properties and considering different scenarios, where a TTP is inline or offline. A formal model of the protocol has also been proposed [46,52,55,58].

Other contributions: theoretical model for unifying key distribution techniques [38], dynamic RFID identification protocol[30], obfuscation of Java code [45], anonymity in group communication protocol [59], authentication protocol for GSM Javacards[65], architectural modeling of software components [67,69] and animation of formal specifications[68].