Daniele Venturi

Curriculum Vitae

Sapienza University
Via Salaria 113, Rome (IT)
+393334796087
venturi@di.uniroma1.it
Date of birth: 29/06/1983
wwwusers.di.uniroma1.it/~venturi

RESEARCH INTERESTS

My main area of interest is theoretical and applied *cryptography*. Current topics include: public-key cryptography, non-malleability, leakage and tamper resilience, secure protocols in the cloud, multiparty computation, abstract and constructive cryptography, zero knowledge.

PROFESSIONAL EXPERIENCE

Sep 13–now **Postdoc in Cryptography**, *Department of Computer Science*, Sapienza University of Rome, Italy.

Promoters Giuseppe Ateniese.

Feb 12–Sep 13 **Postdoc in Cryptography**, *Department of Computer Science*, Aarhus University, Denmark.

Promoters Ivan Damgård and Jesper Buus Nielsen.

Grant Supported from the Danish National Research Foundation, the National Science Foundation of China (under the grant 61061130540), the Danish Council for Independent Research (under the DFF Starting Grant 10-081612) and the CFEM research center.

EDUCATION

Nov 08–Apr 12 **PhD in Information and Communication Engineering**, *Department of Engineering, Electronics and Telecommunications (DIET)*, Sapienza University of Rome, Italy.

Advisor Andrea Baiocchi.

PhD Focus Tamper and leakage resilient cryptography.

Classes During my PhD studies I had the opportunity to follow three classes:

1. A class on the *uses of elliptic curves in cryptography*, taught by Renè Schoof for the master students in Mathemathics, Torvergata University of Rome (7CFU).

2. A class on *information theory*, taught by Jànos Körner for the master students in Computer Science, Sapienza University of Rome (6CFU).

3. A class on *graph theory*, taught by Paul Wollan for the master students in Computer Science, Sapienza University of Rome (6CFU).

Abroad Term I spent 1 year of my PhD abroad, working with Krzysztof Pietrzak and Eike Kiltz at Centrum Wiskunde & Informatica (CWI), Amsterdam

Sep 05–Dec 07 **M. Sc. Communication Engineering**, *Sapienza University of Rome*, Italy.

Final grade Full marks (110/110) and *summa cum laude*.

GPA 31.4/30.

Thesis *Interaction analysis between TCP-like congestion control and multiple access wideband channel*.

Advisor Prof. Andrea Baiocchi and Dott. Alfredo Todini.

Sep 02–Sep 05 **B. Sc. Electrical Engineering**, *ROMATRE University of Rome*, Italy.

Final grade Full marks (110/110) and *summa cum laude*.

GPA 28.4/30.

Thesis *Simulation of reconstruction processes in digital holography and study of the relative degrees of freedom*.

Advisor Prof. Franco Gori.

Sep 97–Jul 02 **High school**, *Scientific Lyceum "Stanislao Cannizzaro"*, Rome, Italy.

Final grade Full marks (100/100).

PUBLICATIONS

Conference Proceedings

[C22] **(De)-Constructing TLS 1.3** (with with Markulf Kohlweiss, Ueli Maurer, Cristina Onete and Björn Tackmann), Proceedings of the 16th International Conference on Cryptology in India (Indocrypt 2015), to appear.

[C21] **Subversion-Resilient Signature Schemes** (with Giuseppe Ateniese and Bernardo Magri), Proceedings of the 22nd ACM Conference on Computer and Communications Security (ACM CCS 2015), to appear.

[C20] **Entangled Encodings and Data Entanglement** (with Giuseppe Ateniese, Özgür Dagdelen, and Ivan Damgård), Proceedings of the 3rd International Workshop on Security in Cloud Computing (SCC@ASIACCS 2015), 3-12, ISBN 978-1-4503-3447-1.

[C19] **Mind Your Coins: Fully Leakage-Resilient Signatures with Graceful Degradation** (with Antonio Faonio and Jesper Buus Nielsen), Proceedings of the 42nd International Colloquium on Automata, Languages and Programming (ICALP 2015), 456-468, Lecture Notes in Computer Science 9134, ISBN 978-3-662-47671-0.

[C18] **The Chaining Lemma and Its Application** (with Ivan Damgård, Sebastian Faust and Pratyay Mukherjee), Proceedings of the 8th International Conference on Information Theoretic Security (ICITS 2015), 181-196, Lecture Notes in Computer Science 9063, ISBN 978-3-319-17469-3.

[C17] **A Tamper and Leakage Resilient von Neumann Architecture** (with Sebastian Faust, Pratyay Mukherjee, and Jesper Buus Nielsen), Proceedings of the 18th International Conference on Practice and Theory in Public-Key Cryptography (PKC 2015), 579-603, Lecture Notes in Computer Science 9020, ISBN 978-3-662-46446-5.

[C16] **From Single-Bit to Multi-Bit Public-Key Encryption via Non-Malleable Codes** (with Sandro Coretti, Ueli Maurer, and Björn Tackmann), Proceedings of the 12th Theory of Cryptography Conference (TCC 2015), 532-560, Lecture Notes in Computer Science 9014, ISBN 978-3-662-46493-9.

[C15] **A Multi-Party Protocol for Privacy-Preserving Cooperative Linear System of Equations** (with Özgür Dagdelen), Proceedings of the 1st International Conference in Cryptography and Information Security in the Balkans (BalkancryptSec 2014), 161-172, Lecture Notes in Computer Science 9024, ISBN 978-3-319-21355-2.

[C14] **A Second Look at Fischlin's Transformation** (with Özgür Dagdelen), Proceedings of the 7th International Conference on Cryptology (Africacrypt 2014), 356-376, Lecture Notes in Computer Science 8469, ISBN 978-3-319-06733-9.

[C13] **Efficient Non-Malleable Codes and Key-Derivation for Poly-Size Tampering Circuits** (with Sebastian Faust, Pratyay Mukherjee, and Daniel Wichs). Proceedings of the 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt 2014), 111-128, Lecture Notes in Computer Science 8441, ISBN 978-3-642-55219-9.

[C12] **Leakage-Resilient Signatures with Graceful Degradation** (with Jesper Buus Nielsen and Angela Zottarel), Proceedings of the 17th International Conference on Practice and Theory in Public-Key Cryptography (PKC 2014), 362-379, Lecture Notes in Computer Science 8383, ISBN 978-3-642-54630-3.

[C11] **Continuous Non-Malleable Codes** (with Sebastian Faust, Pratyay Mukherjee, and Jesper Buus Nielsen), Proceedings of the 11th Theory of Cryptography Conference (TCC 2014), 465-488, Lecture Notes in Computer Science 8349, ISBN 978-3-642-54241-1.

[C10] **Bounded Tamper Resilience: How to go beyond the Algebraic Barrier** (with Ivan Damgård, Sebastian Faust and Pratyay Mukherjee), Proceedings of the 19th International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2013), 140-160, Lecture Notes in Computer Science 8270, ISBN 978-3-642-42044-3.

[C09] **Outsourced Pattern Matching** (with Sebastian Faust and Carmit Hazay), Proceedings of the 40th International Colloquium on Automata, Languages, and Programming (ICALP 2013), 545-556, Lecture Notes in Computer Science 7966, ISBN 978-3-642-39211-5.

[C08] **Anonymity-Preserving Public Key Encryption: A Constructive Approach** (with Markulf Kohlweiss, Ueli Maurer, Cristina Onete and Björn Tackmann), Proceedings of the 13th International Symposium on Privacy Enhancing Technologies (PETS 2013), 19-39, Lecture Notes in Computer Science 7981, ISBN 978-3-642-39076-0.

[C07] **On the Connection between Leakage Tolerance and Adaptive Security** (with Jesper Buus Nielsen and Angela Zottarel), Proceedings of the 16th International Conference on Practice and Theory in Public-Key Cryptography (PKC 2013), 497-515, Lecture Notes in Computer Science 7778, ISBN 978-3-642-36361-0.

[C06] **Rate-Limited Secure Function Evaluation** (with with Özgür Dagdelen and Payman Mohassel), Proceedings of the 16th International Conference on Practice and Theory in Public-Key Cryptography (PKC 2013), 461-478, Lecture Notes in Computer Science 7778, ISBN 978-3-642-36361-0.

[C05] **On the Non-malleability of the Fiat-Shamir Transform** (with Sebastian Faust, Markulf Kohweiss and Giorgia Azzurra Marson), Proceedings of the 13th International Conference on Cryptology in India (Indocrypt 2012), 60-79, Lecture Notes in Computer Science 7668, ISBN 978-3-642-34930-0.

[C04] **Tamper-Proof Circuits: How to Trade Leakage for Tamper-Resilience** (with Sebastian Faust and Krzysztof Pietrzak), Proceedings of the 38th International Colloquium on Automata, Languages and Programming (ICALP 2011), 391-402, Lecture Notes in Computer Science 6755, ISBN 978-3-642-22005-0.

[C03] **Efficient Authentication from Hard Learning Problems** (with Eike Kiltz, Krzysztof Pietrzak, David Cash and Abishek Jain), Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt 2011), 7-26, Lecture Notes in Computer Science 6632, ISBN 978-3-642-20464-7.

[C02] **Leakage-Resilient Storage** (with Francesco Davì and Stefan Dziembowski), Proceedings of the 7th International Conference on Security and Cryptography for Networks (SCN 2010), 121-137, Lecture Notes in Computer Science 6280, ISBN 978-3-642-15316-7.

[C01] **Inadequacy of the Queue-Based Max-Weight Optimal Scheduler on Wireless Links with TCP Sources** (with Alfredo Todini and Andrea Baiocchi), Proceedings of IEEE International Conference on Communications (ICC 2009), 1-6.

Journals

[J04] **Efficient Non-Malleable Codes and Key-Derivation for Poly-Size Tampering Circuits** (with Sebastian Faust, Pratyay Mukherjee, and Daniel Wichs), full version of [C13], submitted to IEEE Transaction on Information Theory.

[J03] **Outsourced Pattern Matching** (with Sebastian Faust and Carmit Hazay), full version of [C09], submitted to Designs, Codes, and Cryptology.

[J02] **Efficient Authentication from Hard Learning Problems** (with Eike Kiltz, Krzysztof Pietrzak, David Cash and Abishek Jain), full version of [C03], accepted to the Journal of Cryptology, pending revisions.

[J01] **Bounded Tamper Resilience: How to go beyond the Algebraic Barrier** (with Ivan Damgård, Sebastian Faust and Pratyay Mukherjee), full version of [C10], Journal of Cryptology, to appear.

Books & Surveys

[S03] **Tampering in Wonderland**, Sapienza Università Editrice, 2013.

[S02] **Crittografia nel Paese delle Meraviglie**, Collana UNITEXT, Springer 2012, ISBN 978-88-470-2480-9.

[S01] **Lecture Notes on Algorithmic Number Theory**, Technical Report ECCC—TR09-06, Electronic Colloquium on Computational Complexity, 28 July 2009.

HONORS & AWARDS

September 13 **Premio Tesi di Dottorato**, *Sapienza Università editrice*, PhD Thesis [S03] awarded amongst the best six thesis defended at Sapienza University between 2010 and 2012.

April 11 **Best paper award at Eurocrypt 2011 for [C03]**, *invited to Journal of Cryptology*.

October 08 **Degree Prize**, 2000€ *for deserving curriculum studiorum*, Sapienza University of Rome, Engineering Faculty.

PROFESSIONAL ACTIVITIES

Program Committees PKC 2016 (19th International Conference on the Theory and Practice of Public-Key Cryptography), Eurocrypt 2016 (35th Annual International Conference on the Theory and Applications of Cryptographic Techniques)

Grants **Official substitute Management Committee member**, *COST "Cryptography for Secure Digital Interaction"*, ICT COST Action IC1306.

Official Management Committee member, *Geopolitics-Aware INternet Strategies (GAINS)*, see `http://www.gains-project.eu/`.

Reviews **External reviewer for**, *Computer Communications (2011), PKC (2011,2014,2015), ICC (2012), Transaction on Computers (2012,2014), ESORICS (2014), TCC (2012,2013,2015), Asiacrypt (2012,2014), Eurocrypt (2013,2015), Crypto (2013), ACM CCS (2013), IEEE Transaction on Information Theory (2014), IEEE Transaction on Emerging Technologies (2014), Journal of Cryptology (2014).*

STUDENTS

Master Students **Giorgia Azzurra Marson**, *Practical Scenarios for the Fiat-Shamir Heuristic: Simulation Soundness and Leakage Resilience*, Master of Science, Faculty of Mathematics, Sapienza University of Rome, December 2011.

Jesper Broni Andersen, *On Pseudorandom Functions based on DDH-like Assumptions, with Applications to E-cash*, Master of Science, Faculty of Computer Science, Aarhus University, November 2012.

SELECTED TALKS

Signature Schemes under Tampering and Subversion

-*Invited talk*, Ruhr-Bochum University (Germany), July 2015.

Recent Advances in Non-Malleable Codes

-*Invited talk*, CWI Amsterdam RISC Seminar (The Netherlands), May 2014.

-*Invited talk*, Sapienza University of Rome (Italy), December 2013.

-*Invited talk*, ETH Zurich (Switzerland), November 2013.

On The Connection between Leakage Tolerance and Adaptive Security

-*Invited talk*, Workshop on Leakage, Tampering and Viruses. Warsaw (Poland), June 2013.

-*PKC 2013*, 16th International Conference on Practice and Theory in Public-Key Cryptography. Nara (Japan) February 2013.

Tamper-Proof Circuits: How to Trade Leakage for Tamper-Resilience

-*RISC Seminar*, CWI, Amsterdam (The Netherlands), May 2010.

-*Student track of the Summer School on Applied Cryptographic Protocols*, Mykonos (Greece), September 2010.

-*ICALP 2011*, 38th International Colloquium on Automata, Languages and Programming. ETH Zurich (Switzerland), July 2011.

Efficient Authentication from Hard Learning Problems

-*Invited talk*, CASED TU Darmstadt (Germany), February 2011.

-*Invited talk*, ESAT/COSIC K. U. Leuven (Belgium), March 2011.

-*Invited talk*, Aarhus University, Aarhus (Denmark), August 2011.

Leakage-Resilient Storage

-*Invited talk*, ESAT/COSIC K. U. Leuven (Belgium), February 2010.

TEACHING

2015-2016 *Lecturer* for the class "Ricerca Operativa", Università degli Studi di Cassino e del Lazio Meridionale

2014-2015 *Lecturer* for the class "Cryptography", Master di I livello in "Sicurezza dei sistemi e delle reti informatiche per l'impresa e la Pubblica Amministrazione", Sapienza University of Rome

Teaching assistant for the class "Cryptography", taught by Giuseppe Ateniese, Sapienza University of Rome

2013-2014 *Lecturer* for the class "Cryptography", Master di I livello in "Sicurezza dei sistemi e delle reti informatiche per l'impresa e la Pubblica Amministrazione", Sapienza University of Rome

Teaching assistant for the class "Cryptography", taught by Giuseppe Ateniese, Sapienza University of Rome

2010-2011 *Teaching assistant* for the class "Communication Security", taught by Andrea Baiocchi, Sapienza University of Rome

2009-2010 *Teaching assistant* for the class "Communication Security", taught by Andrea Baiocchi, Sapienza University of Rome

INDUSTRY EXPERIENCE

Apr 08–Sep 08 **Trainee**, *Telecom Italia LAB (TILAB)*, Via di Val Cannuta 250, Rome, ITALY.

Description Engineering activities on new generation (NGN2) wired networks (Fiber To The Home (FTTH) and Fiber To The Building (FTTB) architectures).

Jan 08–Apr 08 **Trainee**, *Ericsson Telecomunicazioni s.p.a*, Via Anagnina 203, Rome, ITALY.

Description Development, integration and testing of new Intelligent Network (IN) services on INS platform.

CERTIFICATIONS

Mar 07–Jul 07 **EC-ASP: ELSAGDATAMAT Certification for AMTEC Security Professional**, *Elsag Datamat s.p.a.*, Finmeccanica Group.

Skill Covered Basic routing network configuration, planning and design of security infrastructures, use of a management and deployment configuration system, installation and integration of SVPN infrastructures, troubleshooting activities.

COMPUTER SKILLS

Operating systems: Microsoft Windows 3.11/9X/NT/2000/XP, GNU/Linux and others UNIX-like.

Programming: JAVA, bash, LaTeX.

Scientific software: MATHEMATICA, MATLAB, MathCad, ns2.

Others: Inkscape, GIMP, Office and OpenOffice suite.

Languages

Italian: Mother tongue.

English: Self-assessment (Common European Framework of Reference for Languages, CEFR).

Reading C2 (Proficient user).

Listening C2 (Proficient user).

Speaking C2 (Proficient user).

Writing C2 (Proficient user).

SPARE TIME ACTIVITIES

Sports: Judo: since the age of nine, black belt $2^{\text{-th}}$ DAN, Kime-no-Kata regional champion, years 2006 and 2007.

Hobbies: Music: Electric guitar, Acoustic guitar (finger/flat-picking).

Interests: Reading and mathematics.

REFERENCES

These persons are familiar with my professional qualifications and my character:

Ivan Damgård

Department of Computer Science, Aarhus University

Åbogade 24, 8200 Aarhus

e-mail: ivan@cs.au.dk

Jesper Buus Nielsen

Department of Computer Science, Aarhus University

Åbogade 24, 8200 Aarhus
e-mail: jbn@cs.au.dk

Ueli Maurer
Department of Computer Science, ETH Zurich
CH, 8092 Zurich
e-mail: maurer@inf.ethz.ch

"Treatement of personal informations is authorised according to the local privacy laws (D. Lgs 196/2003)".