

Antonio Faonio



Antonio Faonio
✌ Computer Science Department,
Aabogade 34, Aarhus N, 8200, Denmark
✉ afaonio@gmail.com,
➡ <https://00af.keybase.pub/>,
☎ { +45 9187 0127, +39 348 7924560 }

Research interests

My current research topics includes design and study of Efficient Cryptographic Protocols both from theoretical and practical aspects. Currently, I am working on: Efficient Leakage and Tamper Resilient Secure protocols, new paradigms of security against space-bounded adversary, Bitcoin and Blockchain related technologies, and Extremely succinct argument systems and their applications.

Current Position

I am a Post Doc fellow at Aarhus University since December 2014.

Education

Nov 2012–Oct 2014	Ph.D. in Computer Science, Sapienza University of Rome, Italy. Advisor: Prof. Giuseppe Ateniese. Thesis: “ <i>Leakage Resilient Identification Schemes and Signatures</i> ”.
Sept 2008–Dec 2011	Laurea degree (M.S. equivalent) in Computer Science, Sapienza University of Rome, Italy. Advisor: Prof. Nicola Galesi. Thesis: “ <i>Proof Complexity for propositions over Circuit Complexity statement</i> ”. Graduation grade: 110/110 cum laude.
Sept 2005–Dec 2008	Laurea degree (B.S. equivalent) in Computer Science, Sapienza University of Rome, Italy. Advisor: Prof. Riccardo Silvestri. Thesis: “ <i>On Generating safe S-Box for AES</i> ”. Graduation grade: 102/110.

Further educational experiences

May 2010	Short course on constant-depth boolean Circuit lowerbounds , Spain
Jul 2010	Graph Partitioning and Expanders , Italy
Oct 2012	ECRYPT II Summer School on Lattices , Portugal
Feb–July 2014	Visiting Student at Aarhus University supervised by J. B. Nielsen , Denmark
May 2014	Workshop on the theory and practice of Secure Multiparty Computation , Denmark
May 2016	Workshop on the theory and practice of Secure Multiparty Computation , Denmark
Jul 2014	Summer School in Black-Box Impossibility Results , Italy

Awards

Nov 2011	Ph.D. scholarship awarded based on examination.
2010	Admitted to Special Course for Excellent Student.

Teaching and Tutoring

Mar–Nov 2012	T.A. for the Italian Olympiad in Computer Science. As a tutor, I helped preparing high-school students for the regional selection phases. I was tutor in the following courses: Introduction to C programming and Introduction to Python programming
Oct 2013–Jan 2014	T.A. for the Modern Cryptography course. (Laurea Specialistica in Informatica, M.S. in Computer Science equivalent.) Taught some lectures and run exam training sessions.
Mar 2015–Apr 2015	T.A. for EVU course “It-sikkerhed og kryptologi”. (IT security and Cryptology for the Continuing Education Program.) Supervised two groups of students with their projects related to the Bitcoin’s technology.

Participation in EU International projects

Mar Jul 2011	University of Warsaw , Warsaw, Poland I participated to the project Cryptographic Protocols Provable-Secure Against Physical Attacks (FNP Welcome grant WELCOME/2010-4/2) led by Stefan Dziembowski.
Dec 2014	Aarhus University , Aarhus, Denmark I am participating to the project Basic Research In Cryptographic Protocol Theory Cryptographic Protocols (ERC Starting Grant 279447) led by Jesper Buus Nielsen.

Seminars and Workshops

Jun 2012	Presentation given at Sm@rt seminar, C.S. Dept, Sapienza University, Rome I presented the state-of-art, new possible directions and applications for Cryptographic Accumulator
May 2013	Presentation given at Sm@rt seminar, C.S. Dept, Sapienza University, Rome I presented “How to authenticate in a fully compromised system”, joint work with G.Ateniese (Sapienza, Univ. of Rome), S.Kamara (Microsoft Research)
Jun 2013	Presentation given at “Workshop on Leakage, Tampering and Viruses”, Warsaw I presented “How to authenticate in a fully compromised system”, joint work with G.Ateniese (Sapienza, Univ. of Rome), S.Kamara (Microsoft Research)
Mar 2014	Talk given at “Theory Seminar”, Aarhus Mar 2014 I presented “Leakage-Resilient Identification Schemes from Zero-Knowledge Proofs of Storage”, joint work with G.Ateniese (Sapienza, Univ. of Rome), S.Kamara (Microsoft Research)
Sept 2014	Presentation given at the 9th International Conference on Security and Cryptography for Networks, Amalfi I presented “Proof of Space: When Space is of the Essence”, joint work with G.Ateniese (Sapienza, Univ. of Rome), Ilario Bonacina (Sapienza, Univ. of Rome) and Nicola Galesi (Sapienza, Univ. of Rome).
Sept 2014	Invited talk given at IBM Research Zurich (hosted by Dr. Jan Camenisch) I presented “Fully Leakage-Resilient Signatures with graceful degradation”, joint work with J.B. Nielsen (Aarhus Univ.) and D.Venturi (Sapienza, Univ. of Rome).
July 2015	Presentation given at ICALP 2015 I presented “Mind Your Coins: Fully Leakage-Resilient Signatures with Graceful Degradation,”, joint work with J.B. Nielsen (Aarhus Univ.) and D. Venturi (Sapienza, Univ. of Rome).
July 2015	Invited Talks given at NTT, Tokyo (hosted by Dr. Tatsuaki Okamoto) I presented “Mind Your Coins: Fully Leakage-Resilient Signatures with Graceful Degradation,” and “Proof of Space: When Space is of the Essence”.
Dec 2015	Presentation given at IMACC 2015 I presented “Leakage-Resilient Identification Schemes from Zero-Knowledge Proofs of Storage”, joint work with G.Ateniese (Sapienza, Univ. of Rome), S.Kamara (Microsoft Research).
March 2016	Invited Talk given at IIIS Tsinghua University, Beijing (hosted by Prof. John Steinberger) I presented “Fully Leakage-Resilient Codes”, joint work with J. B. Nielsen (Aarhus University).
June 2016	Invited Talk given at KIT, Karlsruhe (hosted by Prof. Dennis Hofheinz) I presented “Fully Leakage-Resilient Signatures with Graceful Degradation”, joint work with J. B. Nielsen (Aarhus University) and Daniele Venturi (University of Trento).
July 2016	Invited Talk given at UC Louvain, Louvain la Neuve (hosted by Prof. Francois-Xavier Standaert) I presented “Fully Leakage-Resilient Codes”, joint work with J. B. Nielsen (Aarhus University).

Papers and Technical Reports

- ✓ Giuseppe Ateniese, A.F., Bernardo Magri, Breno De Mederios,
Certified Bitcoins, ACNS '14;
- ✓ Giuseppe Ateniese, Ilario Bonacina, A.F., Nicola Galesi,
Proofs of Space: When Space is of the Essence, SCN '14;
- ✓ Giuseppe Ateniese, A.F., Seny Kamara,
Leakage-Resilient Identification Schemes from Zero-Knowledge Proofs of Storage, IMACC 2015;
- ✓ A.F., Jesper Buus Nielsen, Daniele Venturi,
Mind Your Coins: Fully Leakage-Resilient Signatures with Graceful Degradation, ICALP 2015;
- ✓ A.F., Daniele Venturi,
Efficient Public-Key Cryptography with Bounded Leakage and Tamper Resilience, ASIACRYPT 2016, To Appear; ia.cr/2016/529;
- 📎 A.F., Jesper Buus Nielsen, Daniele Venturi,
Predictable Arguments of Knowledge, Tech. Report ia.cr/2015/740;
- 📎 A.F., Jesper Buus Nielsen,
Fully Leakage-Resilient Codes, Tech. Report ia.cr/2015/1151;

External Reviewer

CCS 2013, CRYPTO 2014, USENIX 2015, ASIACRYPT 2015, TCC 2016-A, EUROCRYPT 2016, PKC 2016, AFRICACRYPT 2016, IET Information Security, Theor. Comput. Sci., TCC 2016-B, IEEE Transactions on Dependable and Secure Computing.

Computer skills

Programming languages: Proficient: Java, Familiar: C,C++, Matlab, Python,Sage, StandardML.

Operating systems: GNU/Linux (Ubuntu, Debian, Fedora and Archlinux), Windows.

Mobile IT: Basic: Android-OS

Software design: Knowledge of basic principles of software engineering

Databases: Knowledge of basic principles of databases design and familiar with SQL basic constructs.

Languages

Italian: Mother tongue; English: Good.

Personal Interests

Middle distance runner, swimmer, MTB and hiking enthusiast, Lindy Hop (intermediate) dancer.