Giulia Traverso

PhD candidate

Education

2015–present **PhD student**, *Cryptography and Computeralgebra (CDC), Technical University of Darmstadt*, Darmstadt (Germany).
Long-term security for the framework of distributed storage within the cloud infrastructures. Secret sharing. Homomorphic signature schemes. Steganography. Advisor: Prof. Dr. Johannes Buchmann

2012–2014 **MSc, Mathematics**, *Università degli Studi di Trento*, Trento, Italy, [Final mark: 108/110].

2009–2012 **BSc, Mathematics**, *Università degli Studi di Trento*, Trento, Italy, [Final mark: 101/110].
Thesis title: Sulla esistenza delle tangenti alle curve rettificabili (On the existence of tangents to rectificable curves). Advisor: Prof. Silvano Delladio.
The aim was to define the tangent of a point, on a curve, even for those points where the derivative cannot be calculated. We showed that one can define another notion of tangent using Besicovitch's theorem and that it exists for almost any point one a curve.

2004–2009 **High school degree**, *Liceo Classico, Guarino Veronese Institute*, [Final mark: 100/100], San Bonifacio (Verona), Italy.

Master thesis

title *On some modern applications of cryptography*

supervisors Prof. Massimiliano Sala (supervisor), Dr. Alessandro Tomasi (co-supervisor)

description I investigated two different approaches to protect information sent through an insecure channel. Firstly, I analyzed classical cryptography, focusing on ECC (Elliptic Curve Cryptography). Then I moved to post-quantum cryptography, whose aim is to anticipate the advent of quantum computers. About ECC, I showed that the usual countermeasures suggested even by important standards (such as NIST, FIPS and Certicom) are not sufficient to provide security. In fact, their aim is to prevent attacks to the ECDLP (Elliptic Curve Discrete Logarithm Problem) from being effective, but other kinds of strategies have been studied so far. Specifically, side-channel attacks can break the system by exploiting, for example, weaknesses of the operation defined on the curve itself. I proposed additional tests in order to discard those elliptic curves that can be affected by these attacks and concluded that the elliptic curves proposed by the standards above should not be chosen if we are looking for a secure cryptosystem. As regards to post-quantum cryptography, I analyzed cryptosystems that could be used in the future, instead of the classical ones. I also focused on the cryptanalysis done so far and on the problem of defining new digital signature algorithms based on latter.

Hochschulstrasse 10, 64289 Darmstadt – Germany
☎ *+49 6151 16 20663* • FAX *+49 6151 16 20665*
✉ *gtraverso@cdc.informatik.tu-darmstadt.de*

Research Experience

2016 **Collaboration**, *Technical University of Catalonia (UPC)*, Barcelona, Spain.
I regularly visit Prof. Carles Padrò and Prof. Oriol Farras at UPC to work on secret sharing from a more theoretical perspective compared to TU Darmstadt. We are currently writing a paper on how to design secret sharing schemes over extensions of the binary field. We are also doing research towards ideal threshold secret sharing schemes over small finite fields, yet including a large number of participants. Advisor: Carles Padrò, Oriol Farras

September-November 2014 **Internship**, *Group of Applied Physics (GAP)*, Geneva, Switzerland.
I studied the main theoretical assumptions Quantum Key Distribution is based on and possible conflicts that can arise when we deal with real physical devices. I also collaborated with Bruno Sanguinetti on a new steganographic technique based on digital images. This work has been published on PRA. Advisor: Hugo Zbinden, Charles Lim

2014 **Internship**, *IdQuantique*, Geneva, Switzerland.

The company needed to know if they could recommend their customers some elliptic curves of interest. I analyzed each elliptic curve, highlighting the weaknesses and the possible attacks that could be conceived. Then I worked through post-quantum cryptosystems and post-quantum signature algorithms to help the company in understanding which are the most promising protocols to prevent attacks from quantum computers. Advisor: Patrick Trinkler, Damien Stucki

2013 **Internship**, *Laboratorio di Matematica Industriale e Crittografia (Laboratory of Industrial Mathematics and Cryptography)* , Università degli studi di Trento, Trento (Italy).

I studied and implemented tests to measure the minimum entropy of a source of numbers proposed by the National Institute of Standards and Technology (NIST) in the document NIST SP 800-90B. Then I investigated DUKTP (Derived Unique Key Per Transaction), which is a key management scheme used for HSM (Hardware Security Module). I presented this topic in a seminar at the Departement Of Mathematics where PhD students and post-doctoral fellows were invited.. Advisor: Dr. Alessandro Tomasi

Academic Experience

Spring 2016 **Tutor**, *Supervision of a student for implementations*, Technical University of Darmstadt, Darmstadt (Germany).

Winter 2011 **Teaching assistant**, *Guarino Veronese Institute for Mathematics*, Verona (Italy).
I prepared lessons for 11-13th grade mathematics that I had to teach, helped students for their homeworks and marked the assignments. Professor: Prof. Giampaolo Provoli.

Awards and Scholarships

2015 **First prize, QIPC2015 Poster Competition**, *13-18 September 2015*, Leeds (United Kingdom).

2014 **Student Travel Stipend**, *Post-Quantum Cryptography Summer School (PQCrypto 2014)*, Waterloo (Canada).

2010, 2011, 2014 **Recognition for large number of credits, fast completion and a final prize for my thesis**, *Università degli Studi di Trento*, Trento (Italy).

2009 **Maximum High school result prize by Lions Club of San Bonifacio**, Verona (Italy).

Publications

5. **G. Traverso, D. Demirel, S. M. Habib, J. Buchmann**, *AS^3: Adaptive Social Secret Sharing for Distributed Storage Systems*, The 14th Annual Conference on Privacy, Security and Trust (PST2016), Auckland (New Zealand).
4. **D. Demirel, S. Krenn, T. Loruenser, G. Traverso**, *Efficient and Privacy Preserving Third Party Auditing for a Distributed Storage System*, The 11th International Conference on Availability, Reliability and Security (ARES2016), Salzburg (Austria).
3. **G. Traverso, D. Demirel, J. Buchmann**, *Dynamic and Verifiable Hierarchical Secret Sharing*, The 9th International Conference on Information Theoretic Security (ICITS2016), Tacoma (United States).
2. **G. Traverso, D. Demirel, J. Buchmann**, *Homomorphic Signature Schemes - A Survey*, Springer Briefs In Computer Science, Springer (2016).
1. **B. Sanguinetti, G. Traverso, A. Martin, J. Lavoie and H. Zbinden**, *Perfectly Secure Steganography: Hiding Information in the Quantum Noise of a Photograph*, Phys. Rev. A, 93, 012336 (2016).

Talks and Conference Presentations

Jan 2017 **AS^3: Improving Distributed Storage Systems Through Adaptive Social Secret Sharing**, *Invited Talk*, Institute of Mathematics Oberwolfach (Germany).

Dec 2016 **Improving Distributed Storage Systems Through Adaptive Social Secret Sharing**, *Research Seminar*, University of Auckland (New Zealand).

Dec 2016 **AS^3: Adaptive Social Secret Sharing for Distributed Storage Systems Improving Distributed Storage Systems**, *The 14th Annual Conference on Privacy, Security and Trust (PST2016)*, Auckland (New Zealand).

Oct 2016 **AS^3: Improving Distributed Storage Systems Through Adaptive Social Secret Sharing**, *MAK Crypto Seminar*, Technical University of Catalonia, Barcelona (Spain).

Aug 2016 **Dynamic and Verifiable Hierarchical Secret Sharing**, *The 9th International Conference on Information Theoretic Security (ICITS2016)*, Tacoma (United States).

July 2016 **Secret Sharing and Distributed Storage Systems**, *The 6th International Workshop on Cryptography, Robustness and Provable Secure Schemes for Female Young Researchers (CrossFyre2016)*, Darmstadt (Germany).

March 2016 **Dynamic and Verifiable Hierarchical Secret Sharing**, *MAK Crypto Seminar*, Technical University of Catalonia, Barcelona (Spain).

March 2016 **An Introduction to Secret Sharing**, *Group of Quantum Information Theory*, ICFO, Barcelona (Spain).

Sep 2015 **Homomorphic Signature Schemes and their Applications to the Cloud Infrastructures**, *Group of Applied Physics (GAP)*, University of Geneva, Geneva (Switzerland).

Dec 2014 **ECC: Elliptic Curves Cryptography**, *Cryptography and Quantum Information Group*, University of Italian Switzerland, Lugano (Switzerland).

Posters

2015 **B. Sanguinetti, G. Traverso, A. Martin, J. Lavoie and H. Zbinden**, *Perfectly Secure Steganography: Hiding Information in the Quantum Noise of a Photograph*, Quantum Information Processing and Communication (QIPC2015), Leeds (United Kingdom).

Volunteering

2016 **Co-organizer**, *CROSSING Research Seminars*, Technical University of Darmstadt, Darmstadt (Germany).

Other Experiences

In Summer 2010, I worked for Cartotecnica Basic snc, a small company producing items for automotive, building trade and industry sectors. I evaluated the quality of products they were interested to buy and I assisted them during international expositions in Shanghai (December 2008), Guangzhou (October 2011) and Beijing (April 2013). In September 2016, I joined again the company during the exposition "Automechanika"at Frankfurt Messe to assist them in presenting the new products, especially to people who only spoke German.

Additional Information

Date of birth: 08/07/1990

Languages: Italian (native), English (fluent spoken and written), French (fluent spoken), German (basics).

Last updated: January 2017

Hochschulstrasse 10, 64289 Darmstadt – Germany
☎ *+49 6151 16 20663* • FAX *+49 6151 16 20665*
✉ *gtraverso@cdc.informatik.tu-darmstadt.de*