GIOVANNI TOGNOLINI

giovannitognolini@gmail.com
(+39) 3343164118

NB: I am not interested in long-term jobs till the end
of my PhD, but I generally have interest in short internships and collaborations.

PERSONAL INFORMATIONS

Date of Birth	August 11, 1996
Address	42 Molino Street. Castegnato (BS), 25045, Italy

EDUCATION

PhD in Applied Cryptography *November 2021 - Ongoing*
Faculty of Mathematics, University of Trento

Master in Mathematics (Cryptography) *Semptember 2018 - March 2021*
Faculty of Mathematics, University of Trento
Thesis: *"Post-Quantum Cryptography: Towards Commutative Supersingular Isogeny Key Exchange"*

Bachelor in Mathematics *September 2015 - July 2018*
Faculty of Mathematics, University of Trento
Thesis: *"Galois correspondence for infinite degree extensions"*

Scientific High School Diploma *September 2010 - June 2015*
Leonardo Scientific High School, Brescia

MAIN COURSES ATTENDED, MASTER'S DEGREE

Algebraic Cryptography, Coding Theory and Applications, Computability and Computational Complexity, Computational Algebra, Formal Methods, Formal Techniques for Cryptographic Protocol Analysis, Introduction To Computer and Network Security, Scientific Computing, Advanced Programming Of Cryptographic Methods, Stochastic Processes, Digital Signal Processing, Data Hiding.

MAIN COURSES ATTENDED, BACHELOR'S DEGREE

Informatics, Probability and Statistics, Programming Languages 2, Group Theory, Galois Theory, Mathematical Statistics, Commutative Algebra, Algebraic Number Theory, Algorithms and Data Structures.

MAIN CONFERENCES, WORKSHOPS AND SCHOOLS ATTENDED

Eurocrypt23 *23-27 April 2023*
Lyon, France

CBCrypto2023 *22-23 April 2023*
Lyon, France

PQCifris2022 *10-14 October 2022*
Trento, Italy

Summer School in Post-Quantum Cryptography *1-5 August 2022*
Budapest, Hungary

PROJECTS

Optimized Implementation of MAYO *Spring 2023*
Re-adaptation of a pre-existing code in order to make it testable with qemu and compatible with the pqm4 framework.

Hive Ransomware Analysis *February 2022*
Analysis made for and with Treos S.C. (Trento). The project fits within a business consultancy for data recovery encrypted with a Hive-type ransomware on multiple servers. By exploiting a weakness in the ransomware implementation we succeeded to mount a known-plaintext attack and rebuild most of the master key's bits used to encrypt and we reconstructed most of the encrypted data.

Front End Developer *January 2021 - ongoing*
Creation and maintenance of the website of the national associatian "De Componendis Cifris".

Security Analysis of a Specific Bitcoin Address *Winter 2021*
Analysis conducted for Prof. Massimiliano Sala, Trento.

Secure Communication With A Remote Database *Autumn 2020*
The project was carried out in a team of two people and aimed at implementing an encrypted communication to a remote server. The exchange of public keys is handled by RSA; the rest of the communication is handled by AES-128. The interface is implemented with JavaFX, while the communication layer is simulated with Java Sockets.

Forensics Analysis *Autumn 2019*
With this project, an algorithm in Matlab has been created that realizes the passive detection of any tampering with an image.

Image Watermarking Embedding and Attacks *Autumn 2019*
With this project, an algorithm in Matlab has been created. Given a watermark and an image it incorporates the first within the second. In addition, a program has been implemented to attack a given image, with the aim of tampering with the watermark and preserving the quality of the image.

Elliptic Curves on Finite Fields: Schoof's Algorithm *Spring 2019*
With this project, a Magma program was developed that implements the Schoof algorithm, which counts the number of points of an elliptic curve defined over a finite field. Following the implementation, an individual report was drawn up. Particular emphasis is given to implementation choices, comparisons with other known algorithms and variants of the algorithm itself.

Symmetric Key Cryptography Using TwoFish *Winter 2018*
With this project we created a Magma program which implements the TwoFish symmetric key cipher. In the individual report, drawn up later, the key principles on which the implementation was devised were listed and discussed in detail.

PUBLICATIONS AND PREPRINTS

- Longo, Riccardo, et al. "Adaptable Cryptographic Primitives in Blockchains via Smart Contracts." Cryptography 6.3 (2022): 32.
- Picozzi, Christian, et al. "A Post-Quantum Digital Signature Scheme from QC-LDPC Codes." Cryptology ePrint Archive (2022).

GIVEN TALKS

Complexity Theory and Zero-Knowledge Protocols *13 April 2023*
Marche Polytechnic University, Ancona
Description of the basic concepts of complexity theory, and how cryptography relates to them.

Towards a Post Quantum OTS Scheme using QC-LDPC Codes *1 December 2022*
Marche Polytechnic University, Ancona
Discussion of the security of the protocol presented in the seminar of October 14.

A Digital Signature Scheme from QC-LDPC Codes *14 October 2022*
PQCifris2022, Trento
In this talk I presented a code-based post quantum signing scheme, which takes advantage of quasi-cyclic ciphers to obtain compact keys, and LDPC ciphers to have good execution performance.

A Cryptographic Kernel for Post-Quantum Support in Blockchains *12 October 2022*
PQCifris2022, Trento
In this talk I presented a work regarding the management of cryptographic primitives in blockchains that allow the use of smart contracts.

The Bombieri-Vinogradov Theorem *21 July 2022*
University of Trento, Trento
Description of the Bombieri-Vinogradov theorem, a result about the error term in the prime number theorem in arithmetic progression.

Latest Developments in Rainbow Cryptanalysis *17 May 2022*
University of Trento, Trento
Description of the state of the art of Rainbow cryptanalysis, with particular reference to the works of Beullens published in 2022.

An Improvement on Ajtai-GGH Hash Function *14 April 2022*
University of Trento, Trento
Description a family of hash functions proposed in the early 2000s, based on lattices, which generalize and improve the hash functions of Ajtai-GGH.

Good and Bad Implementations of Cryptographic Algorithms *27 January 2022*
Digital Innovation Hub, Vicenza
The talk provides an introduction to the three main families of cryptographic algorithms, i.e. public key protocols, private key protocols, and finally digital signatures. For each of these I have discussed the delicate balance which regulates their functioning, showing examples of good implementations and implementations that instead undermine the security of the underlying protocols.

PERSONAL SKILLS

Digital skills

- Good knowledge of Windows and GNU / Linux operating systems.
- Known programming languages: Java, Javascript, TypeScript, C, Magma, Matlab, R.
- Specific languages for model checking: Promela-Spin, SMV-nuXmv.
- Specific languages for web development: HTML, CSS.

Communication skills
Good communication skills acquired with group projects and individual exhibitions carried out throughout the training course.

Management skills
Good organizational and teamwork knowledge acquired during the university course.

Language skills
Italian (mother tongue), English (First certificate, B2)

WORK EXPERIENCES

External Collaborator *October 2022*
Treos S.C., Trento
I wrote a report on post-quantum cryptography, with particular reference to drop-in substitutes for the Diffie-Hellman protocol.

External collaborator *June 2021 - October 2021*

University of Trento & Quadrans, Trento
Post graduate scholarship: temporary collaboration aimed at studying some theoretical and implementation aspect of the post-quantum cryptographic primitives currently being standardized in the NIST PQC. My specific area concerned hash-based signatures, with particular reference to SPHINCS$^+$. The implementation is meant for the Quadrans blockchain.

External collaborator *April 2021 - May 2021*
University of Trento & MicroFabSolutions, Trento
Temporary collaboration aimed at carrying out a detailed analysis on cryptographic primitives correctly implemented in open hardware devices. More precisely, I explored cryptographic primitives useful to guarantee secure integration with blockchain architecture, with particular reference to elliptic curves digital signature algorithms, SHA-256 and RIPEMD. The report aims exactly to describe the state of the art in this regard.

Full Stack Developer *March 2020 - July 2020*
BVTech S.p.A, Milano
Development of a web application: the activity was aimed at creating the "CGR WEB" software on behalf of Regione Lombardia. The development of this software saw several programming and markup languages: the frontend side was managed with the Angular-8 framework, in order to efficiently integrate HTML5, CSS and Typescript; the backend side is managed only by Java, while for the database side we used SQLDeveloper. In addition to that we used SVN as versioning software.

Tutor - Informatics *September 2019 - December 2019*
University of Trento

Tutor - Probability and Statistics *February 2019 - June 2019*
University of Trento

PERSONAL ADDITION

I'm a person who really enjoy being outdoors: I like climbing, going to the mountains, taking pictures, playing the guitar, discovering new cultures and much more. The place where I live must be able to give me the opportunity to express myself in these aspects too, so when I evaluate a long-term stay (say more than three months) in a new place I have to take these factors into account: I live and work better in a place that makes me feel more comfortable.

29/08/2023