europass

Alessandro Tomasi

WORK EXPERIENCE

Head of Unit

Fondazione Bruno Kessler [08/01/2023 – Current]

City: Trento | **Country:** Italy

Head of the Applied Cryptography Research Unit, aleph.fbk.eu in the Center for Cybersecurity cs.fbk.eu
Research and development projects in applied cryptography and cybersecurity, in particular for digital identity, electronic voting, and cloud-to-edge services.
Research on authentication and authorization protocols, threat modelling, risk and security assessments, compliance with standards and regulations.
Proof-of-Concept development for research and demonstration purposes in android, nodejs, and python.
Funding applications and project management.
Lectures on applied cryptography and vulnerabilities, and digital identity and access management. Supervision of interns, BSc and MSc students.

Researcher

Fondazione Bruno Kessler [08/2017 – 31/12/2022]

City: Trento | **Country:** Italy

Research and development projects in applied cryptography and cybersecurity, in particular for digital identity, access control, electronic voting, automotive security, and blockchain technologies.
Research on authentication and authorization protocols, threat modelling, risk and security assessments, compliance with standards and regulations.
Proof-of-Concept development for research and demonstration purposes in android, nodejs, and python.
Funding applications and project management.
Lectures on applied cryptography and vulnerabilities, and digital identity and access management. Supervision of interns, BSc and MSc students.

University research assistant

University of Trento [08/2012 – 09/2016] **City:**

Trento | **Country:** Italy

Mathematical modeling and analysis of quantum random number generators for cryptography in the SiQuro project. Design and comparison of generation methods based on measurements of quantum mechanical experiments; assessment of output bit rate and entropy; research on output conditioning algorithms. Co-author of two patents granted.
Coding theory and cryptography for biometric authentication systems. MSc thesis supervision, project proposal preparation (private and public sector, e.g. H2020), guest lectures on statistics and random number generation. Management of small teams in research and software development projects, with a strong focus on deliverables and meeting tight deadlines.

University teaching assistant

University of Sussex [08/2003 – 06/2006]

City: Brighton | **Country:** United Kingdom

Weekly workshop tutoring with associated preparation, marking and assistance with students' end-of-term projects in the subjects of Applied and Numerical Mathematics, Matlab, Linear Algebra, ODEs in the physical sciences, Mathematics for Engineers.
Maintenance and development of departmental website elements, including the set-up and use of a MySQL database displayed through a cgi interface handled by Perl scripts.

EDUCATION AND TRAINING

MSc Financial Mathematics

London School of Economics and Political Science [08/2009 – 06/2011]

City: London | **Country:** United Kingdom | **Website:** https://www.lse.ac.uk/

DPhil Mathematics

University of Sussex [12/2002 – 01/2009]

City: Brighton | **Country:** United Kingdom | **Website:** https://www.sussex.ac.uk/

MPhys Theoretical Physics

University of Sussex [09/1998 – 07/2002]

City: Brighton | **Country:** United Kingdom | **Website:** https://www.sussex.ac.uk/ **PUBLICATIONS**

Scopus

ORCID

[2024]

On cryptographic mechanisms for the selective disclosure of verifiable credentials Verifiable credentials are a digital analogue of physical credentials. Their authenticity and integrity are protected by means of cryptographic techniques, and they can be presented to verifiers to reveal attributes or even predicates about the attributes included in the credential. One way to preserve privacy during presentation consists in selectively disclosing the attributes in a credential. In this paper we present the most widespread cryptographic mechanisms used to enable selective disclosure of attributes identifying two categories: the ones based on hiding commitments - e.g., mdl ISO/ IEC 18013-5 - and the ones based on non-interactive zero-knowledge proofs - e.g., BBS signatures. We also include a description of the cryptographic primitives used to design such cryptographic mechanisms.

We describe the design of the cryptographic mechanisms and compare them by performing an analysis on their standard maturity in terms of standardization, cryptographic agility and quantum safety, then we compare the features that they support with main focus on the unlinkability of presentations, the ability to create predicate proofs and support for threshold credential issuance.

Finally we perform an experimental evaluation based on the Rust open source implementations that we have considered most relevant. In particular we evaluate the size of credentials and presentations built using different cryptographic mechanisms and the time needed to generate and verify them. We also highlight some trade-offs that must be considered in the instantiation of the cryptographic mechanisms.

Andrea Flamini; Giada Sciarretta; Mario Scuro; Amir Sharif; Alessandro Tomasi; Silvio Ranise

[2022]

Adaptation of an i-voting scheme to Italian Elections for Citizens Abroad We adapt the Araújo-Traoré protocol to Italian elections, with emphasis on anti-coercion measures. In this short paper we focus on a new method for managing anti-coercion credentials for each voter.

Riccardo Longo; Umberto Morelli; Chiara Spadafora; Alessandro Tomasi

[2021]

TLSAssistant Goes FINSEC: A Security Platform Integration Extending Threat Intelligence Language We present the integration of TLSAssistant, a tool for TLS vulnerability scanning and mitigation, with an online platform of services for cybersecurity in critical infrastructure. We highlight the added value of intelligence sharing and synergies with other services on the platform, as well as the non-trivial challenges encountered in the process.

Salvatore Manfredi; Silvio Ranise; Giada Sciarretta; Alessandro Tomasi

[2020]

Verifiable Contracting A Use Case for Onboarding and Contract Offering in Financial Services with eIDAS and Verifiable Credentials

Sérgio M Nóbrega Gonçalves; Alessandro Tomasi; Andrea Bisegna; Giulio Pellizzari; Silvio Ranise

[2018]

Model, Validation, and Characterization of a Robust Quantum Random Number Generator Based on Photon Arrival Time Comparison A Quantum Random Number Generator (QRNG) based on the detection of the arrival time of photons is presented. A stochastic model of the QRNG prototype is derived, showing its consistency with output data sets, in order to estimate the entropy produced by the device. Experimental data, in accord with the model, demonstrates the robustness of the approach versus possible variations of external parameters such as temperature or intensity of the light.

A Tomasi; Alessio Meneghetti; Nicola Massari; Leonardo Gasparini; Daniele Rucatti; Hesong Xu

[2017]

Code generator matrices as RNG conditioners We quantify precisely the distribution of the output of a binary random number generator (RNG) after conditioning with a binary linear code generator matrix by showing the connection between the Walsh spectrum of the resulting random variable and the weight distribution of the code. Previously known bounds on the performance of linear binary codes as entropy extractors can be derived by considering generator matrices as a selector of a subset of that spectrum. We also extend this framework to the case of non-binary codes.

Alessandro Tomasi; Alessio Meneghetti; Massimiliano Sala

[2009]

Color image segmentation by the vector-valued Allen-Cahn phase-field model: A multigrid solution We present an efficient numerical solution of a PDE-driven model for color image segmentation and give numerical examples of the results. The method combines the vector-valued Allen-Cahn phase field equation with initial data fitting terms with prescribed interface width and fidelity constants. Efficient numerical solution is achieved using a multigrid splitting of a finite element space, thereby producing an efficient and robust method for the segmentation of large images. We also present the use of adaptive mesh refinement to further speed up the segmentation process.

David A Kay; Alessandro Tomasi **PATENTS**

[15/12/2020]

EP3529694 - Random number generator, in particular improved true random number generator

Link: https://register.epo.org/application?number=EP17804656

[02/10/2018]

EP3175354 - TRUE RANDOM NUMBER GENERATOR

Link: https://register.epo.org/application?number=EP15734727

PROJECTS

[21/03/2024 – 20/03/2026]

Interet Voting Research on scalable cryptographic algorithms; rust library development; security analysis and threat model.

[06/2021 – 06/2023]

Electronic voting Scenario: remote voting from abroad or while away for work, education, or health reasons.

Technology: Proof-of-Concept implementation of cryptographic primitives leveraging Miracl, containerized web apps, OIDC-based authentication

Cryptography: Multi-party threshold cryptography, additively homomorphic encryption (e.g., Paillier), zero-knowledge proofs

Funding: Futuro & Conoscenza Srl

Role: project manager, designer, security analyst

[03/2021 – 03/2023]

PROTECTOR Scenario: Integrated services for site of worship protection Technology: Cloud service DevSecOps, IAM

Cryptography: WebAuthn integration in AAC

Funding: ISFP-2020-AG-PROTECT

Role: Data management and DevSecOps

Link: https://www.protector-project.eu/

[08/2019 – 12/2021]

CherryChain - blockchain-based FinTech Scenario: Digital identity for financial service onboarding and contracting

Techonology: CIE 3.0 (X.509, NFC), Decentralized Identifiers, Verifiable Credentials

Cryptography: RSA PKCS1 v1.5, Linked Data Cryptographic Suites

Funding: Autonomous Province of Trento

Role: funding application, requirements elicitation, security design and assessment

Link: https://www.cherrychain.it/ricerca-e-sviluppo-e-incentivo-pat/

[03/2018 – 03/2021]

FINSEC Scenario: Automated security of financial service critical infrastructures

Technology: Docker container design and kubernetes service integration of TLSAssistant, a TLS server configuration analyzer and mitigation suggestion provider

Cryptography: Transport Layer Security recommendations

Funding: H2020-CIP-2016-2017

Role: Developer

Link: https://www.finsec-project.eu/

[12/2017 – 12/2018]

Digital Chain of Trust Scenario: Chain of custody event logging and attribute-based encryption for Attribute-Based Access Control

Technology: Hyperledger Fabric, Rust-ABE

Cryptography: blockchain-based attribute-based encryption

Funding: co-funded by EIT DIGITAL - action line Digital Infrastructures Role: Security analyst and mobile client developer

Link: https://www.eng.it/en/case-studies/dcot-digital-chain-of-trust

[08/2017 – 04/2018]

Securing the CAN bus Scenario: Automotive security

Technology: Controller Area Network

Cryptography: Message Authentication Codes

Funding: commercial R&D

Role: Researcher

[08/2014 – 08/2016]

SiQuro - On silicon chip quantum optics for quantum computing and secure communications Scenario: quantum random number generator based on photodetectors

Technology: Single Photon Avalanche Diodes, Time to Digital Converters

Cryptography: hash functions, linear codes, compliance with NIST recommendations for entropy sources SP 800-90B Funding: Autonomous Province of Trento

Role: modeling, data analysis, post-processing, compliance assessment

Link: http://events.unitn.it/en/siquro

[08/2013 – 06/2014]

Biometric authentication Scenario: Biometric authentication via signature and gesture

Technology: Android tablet with stylus, Windows touchscreen tabletop

Cryptography: Juels-Wattenberg fuzzy commitment

Funding: commercial R&D

Role: project manager

LECTURES, SEMINARS, AND OUTREACH EVENTS

[2018 – 2024]

Applied cryptography and vulnerabilities

Lectures in Cyberchallenge.it, 2020-2024, Trento node

Guest lecture Introduction to Computer and Network Security BSc/MSc, 2018-2020, University of Trento

[2021 – 2024]

Access Control

Lectures in Cybersecurity and Critical Infrastructure Protection MSc, 2021, University of Genova
Lectures in Access Control for Identity and Access Management in the Cybersecurity and Critical Infrastructure Protection professional specialization course, 2021, SMACT

[2018 – 2023]

Digital Identity

Revocation mechanisms for Digital Identity - guest lecture in the Mathematics PhD program at the University of Trento, 2023
Digital Identity and Decentralized Identifiers seminar, University of Trento, Department of Mathematics, 2020 Notte dei Ricercatori

- European researchers' night, 2019, 2021, Trento

ISACA CommunITy outreach event, October 2019, Trento

[2017 – 2020]

Blockchain techonolgies

Guest lecture in Introduction to Computer and Network Security BSc/MSc, 2018-2020, University of Trento
Guest lecture in Social Foresight MSc, 2020, University of Trento

LANGUAGE SKILLS

Mother tongue(s): Italian

Other language(s):

English

LISTENING C2 **READING** C2 **WRITING** C2

SPOKEN PRODUCTION C2 **SPOKEN INTERACTION** C2

German

LISTENING A2 **READING** B1 **WRITING** A2

SPOKEN PRODUCTION A2 **SPOKEN INTERACTION** A2

Levels: A1 and A2: Basic user; B1 and B2: Independent user; C1 and C2: Proficient user

DIGITAL SKILLS

Office

Microsoft Word / Microsoft Excel / Google Drive / PowerPoint / Gmail / LaTeX

Development

python / matlab / C++