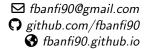
Fabio Banfi

Curriculum Vitae



Experience

Professional

- 04.2024–now **Advanced Security Engineer**, *Zühlke Engineering AG*, Zurich, Switzerland Security assessments, penetration tests, cryptography consulting, post-quantum cryptography migrations, and development of security test suites for industrial control devices
 - 02–06.2017 **Part-Time Software Engineer**, *University of Zurich*, Zurich, Switzerland Data analysis and visualization in Python
 - 04–09.2012 **Software Engineering Internship**, *Siemens Schweiz AG*, Steinhausen, Switzerland Development of several Windows based network services interfacing with various building automation protocols and related GUIs for configuration in C#

Teaching

- 2020–2022 **Head Teaching Assistant**, *ETH Zurich*, Switzerland Current Topics in Cryptography (graduate seminar)
- 2018–2019 **Head Teaching Assistant**, *ETH Zurich*, Switzerland Cryptography Foundations (graduate course)
- 2017–2022 **Teaching Assistant**, *ETH Zurich*, Switzerland Discrete Mathematics (undergraduate course)
 - 2017 **Teaching Assistant**, *ETH Zurich*, Switzerland Algorithms and Probability (undergraduate course)

Education

2017–2023 PhD in Computer Science, ETH Zurich, Switzerland

Thesis title: A Composable Treatment of Anonymous Communication Supervisor: Prof. Ueli Maurer

- 2015-2017 Master of Science ETH in Computer Science, ETH Zurich, Switzerland
- 2012-2015 Bachelor of Science ETH in Computer Science, ETH Zurich, Switzerland

Computer Skills

- ●●● C/C++, LATEX
- ●●● Python, C#, Java
- ●●○ Bash, MATLAB, Haskell, Assembly (x86, MIPS, ARM)
- ● HTML, PHP, CSS, SQL, JavaScript, Markdown

Languages

●●● Italian	First language
●●● English	Fluent in speaking, comprehension, writing and reading
●●● German	Fluent in speaking, comprehension, and reading; good in writing
●●○ French	Fairly good in speaking, comprehension, writing and reading
●○○ Spanish	Fairly good in comprehension and reading; basic in speaking and writing

Publications

Christian Badertscher, Fabio Banfi, and Jesus Diaz. What did come out of it? Analysis and improvements of DIDComm messaging. In ACM SIGSAC Conference on Computer and Communications Security – ACM CCS 2024. doi:10.1145/3658644.3690300.

Christian Badertscher, Fabio Banfi, and Ueli Maurer. A constructive perspective on signcryption security. In *Security and Cryptography for Networks – SCN 2018*. doi:10.1007/978-3-319-98113-0_6.

Fabio Banfi. SCB mode: Semantically secure length-preserving encryption. In *Fast Software Encryption – FSE 2023*. doi:10.46586/tosc.v2022.i4.1-23.

Fabio Banfi, Konstantin Gegier, Martin Hirt, Ueli Maurer, and Guilherme Rito. Anamorphic encryption, revisited. In *Advances in Cryptology – EUROCRYPT 2024*. doi:10.1007/978-3-031-58723-8_1.

Fabio Banfi and Ueli Maurer. Anonymous authenticated communication. In *Security and Cryptography for Networks – SCN 2022*. doi:10.1007/978-3-031-14791-3_13.

Fabio Banfi and Ueli Maurer. Anonymous symmetric-key communication. In *Security and Cryptography for Networks – SCN 2020*. doi:10.1007/978-3-030-57990-6_23.

Fabio Banfi, Ueli Maurer, Christopher Portmann, and Jiamin Zhu. Composable and finite computational security of quantum message transmission. In *Theory of Cryptography – TCC 2019*. doi:10.1007/978-3-030-36030-6_12.