

# Fabio Banfi

## Curriculum Vitae

☎ +41 79 794 32 40  
✉ fbanfi90@gmail.com  
🌐 github.com/fbanfi90  
🌐 n.ethz.ch/~fbanfi

### Education

- 2017–now **PhD Student in Computer Science, ETH Zurich**  
2015–2017 **Master of Science ETH in Computer Science, ETH Zurich**  
2012–2015 **Bachelor of Science ETH in Computer Science, ETH Zurich**

### Experience

#### Professional

- 09.2017 **Software Engineer, PDF Tools AG, Zurich, Switzerland**  
Development and configuration of Windows based services in C# and XML
- 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)

### 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 Ueli Maurer. A constructive perspective on signcryption security. In Dario Catalano and Roberto De Prisco, editors, *Security and Cryptography for Networks – SCN 2018*, volume 11035 of *LNCS*, pages 102–120. Springer, 9 2018.

Fabio Banfi. SCB mode: Semantically secure length-preserving encryption. *IACR Trans. Symm. Cryptol.*, 2022(4):1–23, 2022.

Fabio Banfi and Ueli Maurer. Anonymous symmetric-key communication. In Clemente Galdi and Vladimir Kolesnikov, editors, *Security and Cryptography for Networks – SCN 2020*, volume 12238 of *LNCS*, pages 471–491. Springer, 9 2020.

Fabio Banfi and Ueli Maurer. Anonymous authenticated communication. In Clemente Galdi and Stanislaw Jarecki, editors, *Security and Cryptography for Networks – SCN 2022*, volume 13409 of *LNCS*, pages 289–312. Springer, 9 2022.

Fabio Banfi, Ueli Maurer, Christopher Portmann, and Jiamin Zhu. Composable and finite computational security of quantum message transmission. In Dennis Hofheinz and Alon Rosen, editors, *Theory of Cryptography – TCC 2019*, volume 11891 of *LNCS*, pages 282–311. Springer, 12 2019.