Acknowledgements

First of all, I want to thank my promotor Serge Fehr. It was a pleasure to work with him and taught me a lot about both research and communicating ideas effectively. During our discussions, he always insisted on not only producing results, but also providing an intuitive understanding of *why* the results are correct. I realized that this is not only a convenience for the reader – which already is important enough by itself – but can also lead to stronger results. I am also grateful for his patience especially when the final part of my dissertation turned out to take much longer than anticipated.

I want to thank Léo Ducas for collaborating on our sideproject on homomorphic encryption, and Ronald Cramer for many interesting discussions ranging from mathematics to politics.

I would like to thank Christian Schaffner whose cryptography course at the Universiteit van Amsterdam sparked my interest in the subject, and Marc Stevens for the opportunity to follow up on this interest with a Master thesis as an intern at the CWI Cryptology Group.

I would like to thank my fellow PhD students at the CWI, especially Gabriele Spini and Diego Mirandola, for many fun evenings at the pub, movie nights, table soccer matches, and so on.

Finally, I want to thank my family and friends!

Curriculum Vitae

Maximilian Fillinger was born in Wuppertal, Germany, on March 22, 1988 and grew up first in the nearby city Remscheid, and later in Wuppertal.

He began his studies at the Heinrich-Heine-Universität Düsseldorf in 2005 and obtained Bachelor degrees in philosophy and mathematics in 2008 and 2009, respectively.

He then enrolled in the Master of Logic programme at the Institute for Logic, Language and Computation of the Universiteit van Amsterdam. During his studies there, he became interested in cryptography. In 2013, he obtained his Master degree. His thesis, titled "Reconstructing the Cryptanalytic Attack behind the Flame Malware", was written during an internship at the cryptology group of the Centrum Wiskunde & Informatica (CWI) in Amsterdam, supervised by Christian Schaffner and Marc Stevens. Later in 2013, he obtained a PhD position at the cryptology group of the CWI under the supervision of Serge Fehr.

Since 2018, he works as a software developer at Fox-IT in Delft.

Publications

- Guillaume Bonnoron, Léo Ducas and Max Fillinger. *Large FHE Gates from Tensored Homomorphic Accumulator.* In *Progress in Cryptology - AFRICACRYPT 2018*, pages 217-251.
- Serge Fehr and Max Fillinger. *On the Composition of Two-Prover Commitments, and Applications to Multi-round Relativistic Commitments.* In *Advances in Cryptology - EUROCRYPT 2016, part II*, pages 477-496. An earlier version was presented at *QCRYPT 2015*. An extended version is available at `https://arxiv.org/abs/1507.00240`.
- Max Fillinger and Marc Stevens. *Reverse-engineering of the cryptanalytic attack used in the Flame super-malware.* In *Advances in Cryptology - ASIACRYPT 2015, part II*, pages 586-611.
- Serge Fehr and Max Fillinger. *Multi-Prover Commitments Against Non-Signaling Attacks.* In *Advances in Cryptology - CRYPTO 2015, part II*, pages 403-421. Also presented at *QCRYPT 2015* .