

Dr Franziskus Kiefer

✉ mail@franziskuskiefer.de
📄 franziskuskiefer.de

About Me

Summary I'm a security & cryptography engineer and researcher based in Berlin.

I'm currently heading the cryptography group at [Fraunhofer AISEC](#). Before joining AISEC I was working on [Mozilla's](#) cryptography library [NSS](#). I'm interested in everything around applied cryptography, in particular authentication and key exchange protocols, [formally verifiable specifications](#) and implementations of cryptographic primitives, and privacy preserving data collection and computation.

Experience

Industry

- since 01/2020 **Head of Cryptography Engineering**, *Fraunhofer AISEC*, Berlin, Germany.
applied cryptography research and development
- 10/2015 - 01/2020 **Senior Cryptography/Security Engineer**, *Mozilla Germany*, Berlin, Germany.
NSS maintainer/developer (cryptography library), Formally verified cryptography using F*, Design & implementation of OS password storage integration for Firefox, Design & implementation of new extension signing mechanism, Design of authentication frameworks, Set up of NSS CI infrastructure, Fuzzing, Hardware-accelerated AES-GCM implementation
- 05/2015 - 07/2015 **Security Engineering Intern**, *Mozilla Inc*, San Francisco, USA.
Security Engineering, Implementing referrer policies (<https://www.w3.org/TR/referrer-policy/>)
- 11/2009 - 10/2012 **Software Developer**, *FlexSecure GmbH*, Darmstadt, DE.
Software development (PKI, JEE, Side channel resistant cryptography, Cryptographic protocols for German electronic identity cards, Smart card profiles), Software evaluation (Common Criteria).

Open Source & Research

- since 2018 **hacspe**c, *Formal specification language for specifications*.
Designing a new formal language for cryptography algorithms in specifications (<https://hacs-workshop.github.io/hacspe/>)
- since 2017 **HACL***, *Formally verified cryptographic library*.
Implementation of cryptographic primitives for HACL* (<https://github.com/project-everest/hacl-star>)
- 2009-2012 **FlexiProvider / Bouncy Castle**, *Java CSP*.
Implementation of cryptographic primitives for Java Cryptographic Providers FlexiProvider and BouncyCastle (<https://github.com/project-everest/hacl-star>)

Education

- 01/2013-02/2016 **PhD in Applied Cryptography**, *University of Surrey, Department of Computing*, Guildford, UK.
- 10/2010-10/2012 **M.Sc in Computer Science (with honours)**, *Technische Universität Darmstadt, Department of Computer Science*, Darmstadt, DE.

- 10/2010-10/2012 **M.Sc in IT-Security (with honours)**, *Technische Universität Darmstadt, Department of Computer Science*, Darmstadt, DE.
- 10/2007-09/2010 **B.Sc in Computer Science (with distinction)**, *Technische Universität Darmstadt, Department of Computer Science*, Darmstadt, DE.
- 08/2006-04/2007 **Community Service**, *University Hospital Rechts der Isar of the Technischen Universität München*, Munich, DE.
- 06/1998-05/2006 **Abitur (A-Level)**, *Gymnasium Marianum*, Warburg Westf., DE.

PhD thesis

Title Advancements in Password-based Cryptography [8]
Supervisor Dr. Mark Manulis

Languages

German Native Language
English Fluent

Programming

Languages C, C++, Rust, Python, Bash,
JavaScript, Java
Tools Docker, Git, Mercurial, AWS
Portfolio <https://github.com/franziskuskiefer>

Teaching & Community

Guest Lectures Lectures on secure content transfer on the internet and practical aspects of the web public key infrastructure at TU Berlin and TU Darmstadt
Thesis Supervision Beyond privacy-aware counting (Bachelor thesis at TU Berlin 2019)
Community Initiator and co-organiser of the Berlin Crypto meetup (<https://berlin-crypto.github.io>)

Talks

RWC 2018 HACLS* in Mozilla Firefox
ISC 2016 Universally Composable Two-Server PAKE
ISC 2015 Oblivious PAKE – Efficient Handling of Password Trials
ESORICS 2014 Zero-Knowledge Password Policy Checks and Verifier-based PAKE
ACNS 2014 Distributed Smooth Projective Hashing and Two-Server PAKE
CryptoForma 2014 Distributed Smooth Projective Hashing and Two-Server PAKE
MFS Seminar 2014 Password-based Authentication for Mobile Browsers
CryptoForma 2013 Oblivious PAKE – Efficient Handling of Password Trials
SAM 2012 Practical Security in E-Mail Applications

Other Interests

Music I play several instruments (drums, guitar, piano).
Outdoor I like hiking, climbing, and mountaineering.

Publications

- [1] Karthikeyan Bhargavan, Franziskus Kiefer, and Pierre-Yves Strub. hacspec: towards verifiable crypto standards. In *SSR 2018: Security Standardisation Research*, 2018.
- [2] Johannes Braun, Franziskus Kiefer, and Andreas Hülsing. Revocation and Non-repudiation: When the First Destroys the Latter. In *EuroPKI*, volume 8341 of *Lecture Notes in Computer Science*, pages 31–46. Springer-Verlag, 2013.
- [3] Johannes Buchmann, Johannes Braun, Moritz Horsch, Detlef Hühnlein, Franziskus Kiefer, Falko Strenzke, and Alexander Wiesmaier. Towards a mobile eCard Client. In *13. Kryptotag*, page 4, December 2010.
- [4] Changyu Dong and Franziskus Kiefer. Secure set-based policy checking and its application to password registration. In *Cryptology and Network Security - 14th International Conference, CANS 2015, Marrakesh, Morocco, December 10-12, 2015, Proceedings*, pages 59–74, 2015.
- [5] Nils Fleischhacker, Felix Günther, Franziskus Kiefer, Mark Manulis, and Bertram Poettering. Pseudorandom Signatures. Cryptology ePrint Archive, Report 2011/673, 2011. <http://eprint.iacr.org/>.
- [6] Nils Fleischhacker, Felix Günther, Franziskus Kiefer, Mark Manulis, and Bertram Poettering. Pseudorandom Signatures. In *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, ASIA CCS '13*, pages 107–118, New York, NY, USA, 2013. ACM.
- [7] Franziskus Kiefer. Effiziente Implementierung des PACE- und EAC Protokolls für mobile Geräte. Bachelor thesis, TU Darmstadt, July 2010.
- [8] Franziskus Kiefer. *Advancements in Password-based Cryptography*. PhD thesis, University of Surrey, 2016.
- [9] Franziskus Kiefer and Mark Manulis. Distributed smooth projective hashing and its application to two-server password authenticated key exchange. In *ACNS'14*, volume 8479 of *Lecture Notes in Computer Science*, pages 199–216. Springer-Verlag, 2014.
- [10] Franziskus Kiefer and Mark Manulis. Zero-knowledge password policy checks and verifier-based PAKE. In *ESORICS'14*, volume 8713 of *Lecture Notes in Computer Science*, pages 295–312. Springer-Verlag, 2014.
- [11] Franziskus Kiefer and Mark Manulis. Oblivious PAKE: efficient handling of password trials. In *Information Security - 18th International Conference, ISC 2015, Trondheim, Norway, September 9-11, 2015, Proceedings*, pages 191–208, 2015.
- [12] Franziskus Kiefer and Mark Manulis. Blind password registration for two-server password authenticated key exchange and secret sharing protocols. In *Information Security - 19th International Conference, ISC 2016, Honolulu, HI, USA, September 3-6, 2016, Proceedings*, pages 95–114, 2016.
- [13] Franziskus Kiefer and Mark Manulis. Blind password registration for verifier-based PAKE. In *Proceedings of the 3rd ACM International Workshop on ASIA*

Public-Key Cryptography, AsiaPKC@AsiaCCS, Xi'an, China, May 30 - June 03, 2016, pages 39–48, 2016.

- [14] Franziskus Kiefer and Mark Manulis. Universally composable two-server PAKE. In *Information Security - 19th International Conference, ISC 2016, Honolulu, HI, USA, September 3-6, 2016, Proceedings*, pages 147–166, 2016.
- [15] Franziskus Kiefer, Alexander Wiesmaier, and Christian Fritz. Practical Security in E-Mail Applications. In *The 2012 International Conference on Security and Management*, pages 138–144, July 2012.
- [16] Mark Manulis, Nils Fleischhacker, Felix Günther, Franziskus Kiefer, and Bertram Poettering. Group Signatures - Authentication with Privacy. German Information Security Agency (GISA), 2012. <https://www.bsi.bund.de/EN/>.
- [17] Mark Manulis, Douglas Stebila, Franziskus Kiefer, and Nick Denham. Secure modular password authentication for the web using channel bindings. *Int. J. Inf. Sec.*, 15(6):597–620, 2016.
- [18] Alex Wiesmaier, Moritz Horsch, Johannes Braun, Franziskus Kiefer, Detlef Hühnlein, Falko Strenzke, and Johannes Buchmann. An efficient mobile PACE implementation. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIA CCS '11*, pages 176–185, New York, NY, USA, 2011. ACM.