



Daniel Kales

Curriculum Vitae

Education

- 2018–2022 **Doctoral programme in Computer Science**, *University of Technology, Graz*.
Thesis: Improving Modern Cryptographic Protocols using Domain-Specific Symmetric Primitives
Completed with distinction and *sub auspiciis* graduation.
Supervisor: Univ.-Prof. Christian Rechberger
- 2016–2017 **Masters of Information and Computer Engineering**, *University of Technology, Graz*.
Completed with distinction.
Major: Secure and Correct Systems
Minor: Embedded and Automotive Systems
- 2012–2016 **Bachelor of Information and Computer Engineering**, *University of Technology, Graz*.
Completed with distinction.
- 2006–2011 **Matura**, *Höhere Technische Bundeslehr- und Versuchsanstalt, Villach*.
Completed with distinction.

Experience

- 2022– **Co-Founder, Cryptographer, Technical Lead**, *TACEO GmbH, Graz, Austria*.
Conducting research in the area of post-quantum cryptography, zero-knowledge and privacy-preserving data analytics. Design and implementation of cryptographic software solutions.
- 2017–2022 **Scientific Project Staff/University Assistant**, *IAIK, TU Graz, Graz, Austria*.
Design and analysis of cryptographic primitives with focus on the area of multi-party computation and post-quantum signatures. Fast and secure implementation of cryptographic algorithms (e.g., PICNIC). Teaching master-level courses in the area of cryptography.

Internships

- 2019 **Internship**, *Microsoft Research, Redmond, WA, USA*, Mentor: Greg Zaverucha.
Working on improvements for the Picnic post-quantum signature scheme. This included protocol specific research as well as efforts to speed up the performance of the reference Picnic implementation. Other research in the area of post-quantum signatures lead to attacks on MQDSS, another post-quantum signature scheme.

Vocational

- 2016 **Summer Job as Software Engineer**, *IAIK, TU Graz, Graz, Austria*.
Refactoring of tool for differential cryptanalysis, Implementation of cryptographic attacks, C++.
- 2013–2015 **Summer Job as Software Engineer**, *B.A.P., Klagenfurt, Austria*.
Development of client/server-based hotel management software, C++/python.

Miscellaneous

2018–2022 **Lecturer (Applied Cryptography I & II, Modern Public Key Cryptography, Information Security, Privacy Enhancing Technologies)**, *University of Technology, Graz*.

2013–2017 **Teaching Assistant (Calculus I & II, Operating Systems, Secure Software Development)**, *University of Technology, Graz*.

Languages

German **Mother-tongue**

English **Advanced** *Con conversationally fluent, able to understand and create scientific documents*

Interests

- Member of TU Graz CTF team LosFuzzys (<https://hack.more.systems>)
- Bouldering, Running

Doctoral Thesis

Title *Improving Modern Cryptographic Protocols using Domain-Specific Symmetric Primitives*
Supervisor Univ.-Prof. Christian Rechberger

Abstract In this thesis, I explored several aspects of the security and efficiency of protocols using domain-specific symmetric primitives. One of the main explored applications is the long-term security of cryptographic primitives, where the security of many existing digital signature schemes is being threatened by quantum attacks. We investigated the security and efficiency of post-quantum signature schemes built solely using symmetric-key primitives. We show how to improve the performance of Picnic, one such scheme, further, investigate the security of alternative post-quantum signature designs and propose two new post-quantum signature designs that perform better than Picnic. Finally, we show that by combining generic multiparty computation with block ciphers specifically designed for this use case, we can create a protocol that is competitive with custom private set intersection protocols in the context of mobile contact discovery.

Masters Thesis

Title *Cryptanalysis of Tweakable Block Ciphers*
Supervisors Univ.-Prof. Christian Rechberger & Dipl.-Ing. Maria Eichlseder
Description In this thesis I used and expanded methods for differential cryptanalysis and applied them to different tweakable block ciphers, resulting in a new key-recovery attack on MANTIS-6.

Conference/Journal Publications

Note: The standard convention in this discipline is to list the authors in alphabetical order.

- [1] Carsten Baum, Cyprien Delpech de Saint Guilhem, Daniel Kales, Emmanuela Orsini, Peter Scholl, and Greg Zaverucha. “Banquet: Short and Fast Signatures from AES”. In: *Public Key Cryptography (1)*. Vol. 12710. LNCS. Springer, 2021, pp. 266–297.
- [2] Itai Dinur, Daniel Kales, Angela Promitzer, Sebastian Ramacher, and Christian Rechberger. “Linear Equivalence of Block Ciphers with Partial Non-Linear Layers: Application to LowMC”. In: *EUROCRYPT (1)*. Vol. 11476. LNCS. Springer, 2019, pp. 343–372.
- [3] Christoph Dobraunig, Maria Eichlseder, Daniel Kales, and Florian Mendel. “Practical Key-Recovery Attack on MANTIS5”. In: *IACR Trans. Symmetric Cryptol.* 2016.2 (2016), pp. 248–260.
- [4] Christoph Dobraunig, Daniel Kales, Christian Rechberger, Markus Schofnegger, and Greg Zaverucha. “Shorter Signatures Based on Tailor-Made Minimalist Symmetric-Key Crypto”. In: *CCS*. ACM, 2022, to appear.
- [5] Orr Dunkelman, Maria Eichlseder, Daniel Kales, Nathan Keller, Gaëtan Leurent, and Markus Schofnegger. “Practical Key Recovery Attacks on FlexAEAD”. In: *Designs, Codes and Cryptography (2022)*, to appear.
- [6] Maria Eichlseder and Daniel Kales. “Clustering Related-Tweak Characteristics: Application to MANTIS-6”. In: *IACR Trans. Symmetric Cryptol.* 2018.2 (2018), pp. 111–132.
- [7] Maria Eichlseder, Daniel Kales, and Markus Schofnegger. “Forgery Attacks on FlexAE and FlexAEAD”. In: *IMACC*. Vol. 11929. LNCS. Springer, 2019, pp. 200–214.
- [8] Lukas Helminger, Daniel Kales, Sebastian Ramacher, and Roman Walch. “Multi-party Revocation in Sovrin: Performance through Distributed Trust”. In: *CT-RSA*. Vol. 12704. LNCS. Springer, 2021, pp. 527–551.
- [9] Daniel Kales, Olamide Omolola, and Sebastian Ramacher. “Revisiting User Privacy for Certificate Transparency”. In: *EuroS&P*. IEEE, 2019, pp. 432–447.
- [10] Daniel Kales, Sebastian Ramacher, Christian Rechberger, Roman Walch, and Mario Werner. “Efficient FPGA Implementations of LowMC and Picnic”. In: *CT-RSA*. Vol. 12006. LNCS. Springer, 2020, pp. 417–441.
- [11] Daniel Kales, Christian Rechberger, Thomas Schneider, Matthias Senker, and Christian Weinert. “Mobile Private Contact Discovery at Scale”. In: *USENIX Security Symposium*. USENIX Association, 2019, pp. 1447–1464.
- [12] Daniel Kales and Greg Zaverucha. “An Attack on Some Signature Schemes Constructed from Five-Pass Identification Schemes”. In: *CANS*. Vol. 12579. LNCS. Springer, 2020, pp. 3–22.
- [13] Daniel Kales and Greg Zaverucha. “Improving the Performance of the Picnic Signature Scheme”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2020.4 (2020), pp. 154–188.
- [14] Deepika Natarajan, Anders Dalskov, Daniel Kales, and Shabnam Khanna. “PRIORIS: Enabling Secure Detection of Suicidal Ideation from Speech Using Homomorphic Encryption”. In: *Protecting Privacy through Homomorphic Encryption*. Springer, 2021, pp. 133–146.