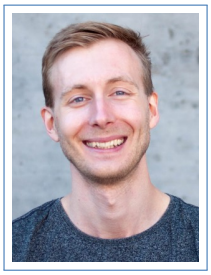

Daniel Kales

Curriculum Vitae

Education

2018– **Doctoral programme in Computer Science**, *University of Technology*, Graz.
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.

Experience

2017– **Scientific Project Staff**, *IAIK, TU Graz*, Graz, Austria.
Design and analysis of cryptographic primitives with focus on the area of multi-party computation. 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 improvements as well as efforts to speed up the performance of the Pinic implementation.

Vocational

2016 **Summer Job as Software Engineer**, *IAIK, TU Graz*, Graz, Austria.
Refactoring of tool for differential cryptanalysis, Implementation of cryptographic attacks, C++.

Miscellaneous

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

Technological skills

Coding C, C++, Rust, Assembly, Go, python, LaTeX
OS Linux, Microsoft Windows

Languages

German **Mother-tongue**
English **Advanced** *Conversationally fluent, able to understand and create scientific documents*

Interests

- Member of CTF team LosFuzzys (`https://hack.more.systems`)
- Bouldering, Running

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] 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. Lecture Notes in Computer Science. Springer, 2019, pp. 343–372.

[2] 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.

[3] Maria Eichlseder and Daniel Kales. "Clustering Related-Tweak Characteristics: Application to MANTIS-6". In: *IACR Trans. Symmetric Cryptol.* 2018.2 (2018), pp. 111–132.

[4] Maria Eichlseder, Daniel Kales, and Markus Schofnegger. "Forgery Attacks on FlexAE and FlexAEAD". In: *IMACC*. Vol. 11929. Lecture Notes in Computer Science. Springer, 2019, pp. 200–214.

[5] Daniel Kales, Olamide Omolola, and Sebastian Ramacher. "Revisiting User Privacy for Certificate Transparency". In: *EuroS&P*. IEEE, 2019, pp. 432–447.

[6] Daniel Kales, Sebastian Ramacher, Christian Rechberger, Roman Walch, and Mario Werner. "Efficient FPGA Implementations of LowMC and Picnic". In: *CT-RSA*. Vol. 12006. Lecture Notes in Computer Science. Springer, 2020, pp. 417–441.

[7] 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.

[8] Daniel Kales and Greg Zaverucha. "Improving the Performance of the Picnic Signature Scheme". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2020.4 (2020), to appear.