Nico Marcel Döttling

Schüren 34
66386 St. Ingbert, Germany
✉ *nico.doettling@gmail.com*

Personal Data

Date of Birth	November 2nd, 1982
Nationality	German
Family Status	married, 2 children

Work Experience

Current Position

since 08/2018 **Tenure-track Faculty**, *CISPA Helmholtz Center for Information Security*, Saarbrücken, Germany.

Prior Positions

10/2017–07/2018 **Assistant Professor (Juniorprofessor)**, *Friedrich-Alexander-University Erlangen-Nürnberg*, Germany.

04/2016–09/2017 **Postdoctoral Researcher and DAAD Fellow**, *University of California Berkeley*, USA.

06/2014–03/2016 **Postdoctoral Researcher**, *Cryptography Group at Department of Computer Science, Aarhus University*, Aarhus, Denmark.

09/2008–05/2014 **Research Assistant**, *Institute of Cryptography and Security, Karlsruhe Institute of Technology*, Karlsruhe, Germany.

01/2007–06/2007 **Internship**, *Siemens Energy & Automation*, Arlington (Texas), USA.

Education

10/2002–09/2008 **Undergraduate Studies in Computer Science**, *Karlsruhe University*, Karlsruhe.

26.06.2002 **Abitur (High School Diploma), Average Grade 1.1**, *Hohenlohegymnasium Öhringen*, Öhringen.

Theses

08.05.2014 **Dr. rer. nat. (PhD in Computer Science)**, *Institute of Theoretical Computer Science, Karlsruhe Institute of Technology*, Karlsruhe.
Title of the Thesis: Cryptography based on the Hardness of Decoding
Advisor: Jörn Müller-Quade
Co-referee: Daniel Wichs
Grade: very good with distinction
Available online at http://nbn-resolving.org/urn:nbn:de:swb:90-411105

09/2008 **Dipl.-Inform (MSc in Computer Science)**, *Institute of Algorithms and Cognitive Systems, Karlsruhe Institute of Technology*, Karlsruhe.
Title of the Thesis: Zur Sicherheit polynombasierter asymmetrischer kryptographischer Verfahren (On the Security of Polynomial-Based Asymmetric Encryption Schemes)
Advisors: Jörn Müller-Quade and Willi Geiselmann
Grade: very good

Awards

22.08.2017 **Best Paper Award at Crypto 2017 for the work *Identity-Based Encryption from the Diffie-Hellman Assumption*.**

01.03.2016 **Postdoctoral Fellowship at UC Berkeley sponsored by the German Academic Exchange Service (DAAD), €55418.**

24.11.2015 **Best Paper Award at ProvSec 2015 for the work *From Stateful Hardware to Resettable Hardware Using Symmetric Assumptions*.**

17.06.2015 **Biennial dissertation award for the best dissertation in computer science at the Karlsruhe Institute of Technology in the years 2014 and 2015 by the Erika and Dr. Wolfgang Eichelbeger foundation.**

Grants

01.01.2020 **Helmholtz Pilot Project Trusted-Federated Data Analytics, Co-PI.**

2016 **DAAD Postdoctoral Grant: *Strong Cryptography from Weak Assumptions***, *04/2016-03/2017*, €55418.

2011 **KASTEL Center of Competence for IT-security**, *Coauthor of Grant Application*, KIT.

2010–2013 **IBM CAS Project HomER**, *Coauthor of Grant Application and Project-Conduct*, KIT.

Program Committees

- CRYPTO 2017, 2019
- EUROCRYPT 2016, 2018
- ASIACRYPT 2015, 2016, 2017, 2018
- TCC 2015, 2016b, 2019, 2020
- PKC 2017, 2018, 2019
- ProvSec 2014, 2016
- ICITS 2016

Invited Talks / Keynotes

26.09.2019 **Quantum Computing and Cryptography**, *DPG Fall Meeting*.

18.07.2019 **CASA Distinguished Lecture, Ruhr University Bochum**, *Trapdoor Hash Functions and their Applications*.

02.12.2017 **Keynote at 16th International Conference on Cryptology and Network Security (CANS 2017), Hong Kong**, *Identity-Based Encryption from Standard Assumptions (or the unexpected virtue of garbled circuits)*.

26.09.2016 **Workshop on Mathematics of Information - Theoretic Cryptography, NUS Singapore**, *Information theoretic continuously non-malleable codes in the constant split-state model*.

24.04.2015 **RISC Seminar on Secret Sharing and Multiparty Computation, CWI Amsterdam**, *Linear Secret Sharing Schemes from Error Correcting Codes and Universal Hash Functions*.

22.11.2013 **IBM Academic Lab Days, IBM R&D Böblingen**, *Sicherheit durch Kryptographie?*.

14.05.2013 **Podiumsdiskussion Cyberwar, Universität Göttingen**.

Grant Evaluation

Evaluator for Israel Science Foundation, *2016, 2020*.

Evaluator for the European Research Council, *2020*.

Teaching Experience

2020 **Cryptography**, *Core Lecture*, CISPA/UdS.

2019 **Cryptography**, *Core Lecture*, CISPA/UdS.

2018 **Advanced Public Key Encryption**, *Advanced Lecture*, CISPA/UdS.

2018 **Signals and Codes**, *Advanced Lecture*, FAU Erlangen-Nürnberg.

2017 **Computer Science for Engineers**, *Core Lecture*, FAU Erlangen-Nürnberg.

2015 **Coding Theory**, *Advanced Lecture*, Aarhus University.

2010–2013 **Selected Areas of Cryptography**, *Advanced Lecture*, Karlsruhe Institute of Technology.

2010–2014 **Coding Theory (Signale und Codes)**, *Advanced Lecture*, Karlsruhe Institute of Technology.

Supervised Theses

2020 **Ring Signatures for cryptographically secure online-voting**, *Jeanette (Stella) Wohnig*, Master-Thesis, CISPA.

2020 **Maliciously Circuit-Private Rate-1 FHE**, *Jesko Dujmovic*, Master-Thesis, CISPA.

2011 **Obtaining an efficient, universally composable obfuscation-scheme**, *Tobias Nilges*, Master-Thesis, KIT, co-supervised.

2011 **Eine optimierte Implementierung von Gentrys vollhomomorphem Verschlüsselungsverfahren**, *Diploma-Thesis, Tobias Beck*, KIT, co-supervised.

2010 **Automatische Erzeugung von geschützten, selbstentschlüsselnden Programmen unter Linux**, *Jan Stijohann*, Diploma-Thesis, KIT, co-supervised.

Publications

Conference Papers

[1] Sri Aravinda Krishnan Thyagarajan, Adithya Bhat, Giulio Malavolta, Nico Döttling, Aniket Kate, and Dominique Schröder. Verifiable timed signatures made practical. In *CCS 2020: ACM Conference on Computer and Communications Security* , 2020.

[2] Zvika Brakerski, Nico Döttling, Sanjam Garg, and Giulio Malavolta. Candidate io from homomorphic encryption schemes. In *EUROCRYPT (1)*, volume 12105 of *Lecture Notes in Computer Science*, pages 79–109. Springer, 2020.

[3] Zvika Brakerski and Nico Döttling. Hardness of LWE on general entropic distributions. In *EUROCRYPT (2)*, volume 12106 of *Lecture Notes in Computer Science*, pages 551–575. Springer, 2020.

[4] Nico Döttling, Sanjam Garg, Mohammad Hajiabadi, Daniel Masny, and Daniel Wichs. Two-round oblivious transfer from CDH or LPN. In *EUROCRYPT (2)*, volume 12106 of *Lecture Notes in Computer Science*, pages 768–797. Springer, 2020.

[5] Nico Döttling, Sanjam Garg, Giulio Malavolta, and Prashant Nalini Vasudevan. Tight verifiable delay functions. In *SCN 2020 : 12th Conference on Security and Cryptography for Networks* , 2020.

[6] Dominic Deuber, Nico Döttling, Bernardo Magri, Giulio Malavolta, and Sri Aravinda Krishnan Thyagarajan. Minting mechanisms for (pos) blockchains. In *ACNS 2020: Applied Cryptography and Network Security* , 2020.

[7] Zvika Brakerski, Nico Döttling, Sanjam Garg, and Giulio Malavolta. Leveraging linear decryption: Rate-1 fully-homomorphic encryption and time-lock puzzles. In *TCC*, 2019.

[8] Nico Döttling, Sanjam Garg, Mohammad Hajiabadi, Kevin Liu, and Giulio Malavolta. Rate-1 trapdoor functions from the diffie-hellman problem. In *ASIACRYPT*, 2019.

[9] Ignacio Cascudo, Ivan Damgård, Bernardo David, Nico Döttling, Rafael Dowsley, and Irene Giacomelli. Efficient uc commitment extension with homomorphism for free (and applications). In *ASIACRYPT*, 2019.

[10] Nico Döttling, Sanjam Garg, Vipul Goyal, and Giulio Malavolta. Laconic conditional disclosure of secrets and applications. In *FOCS*, 2019.

[11] Nico Döttling, Sanjam Garg, Yuval Ishai, Giulio Malavolta, Tamer Mour, and Rafail Ostrovsky. Trapdoor hash functions and their applications. In *CRYPTO*, Lecture Notes in Computer Science, 2019.

[12] Michael Backes, Nico Döttling, Lucjan Hanzlik, Kamil Kluczniak, and Jonas Schneider. Ring signatures: Logarithmic-size, no setup - from standard assumptions. In *EUROCRYPT*, Lecture Notes in Computer Science, 2019.

[13] Divesh Aggarwal, Nico Döttling, Maciej Obremski Jesper Buus Nielsen, and Erick Purwanto. Continuous non-malleable codes in the 8-split-state model. In *EUROCRYPT*, Lecture Notes in Computer Science. Springer, 2019.

[14] Nico Döttling, Russell Lai, and Giulio Malavolta. Incremental proofs of sequential work. In *EUROCRYPT*, Lecture Notes in Computer Science. Springer, 2019.

[15] Nico Döttling, Sanjam Garg, Divya Gupta, Peihan Miao, and Pratyay Mukherjee. Obfuscation from low noise multilinear maps. In *INDOCRYPT*, volume 11356 of *Lecture Notes in Computer Science*, pages 329–352. Springer, 2018.

[16] Zvika Brakerski and Nico Döttling. Two-message statistically sender-private OT from LWE. In *TCC (2)*, volume 11240 of *Lecture Notes in Computer Science*, pages 370–390. Springer, 2018.

[17] Nico Döttling, Sanjam Garg, Mohammad Hajiabadi, and Daniel Masny. New constructions of identity-based and key-dependent message secure encryption schemes. In *PKC*, Lecture Notes in Computer Science. Springer, 2018.

[18] Nico Döttling and Sanjam Garg. From selective IBE to full IBE and selective HIBE. In *TCC (1)*, volume 10677 of *Lecture Notes in Computer Science*, pages 372–408. Springer, 2017.

[19] Ronald Cramer, Ivan Damgård, Nico Döttling, Irene Giacomelli, and Chaoping Xing. Linear-time non-malleable codes in the bit-wise independent tampering model. In *ICITS*, volume 10681 of *Lecture Notes in Computer Science*, pages 1–25. Springer, 2017.

[20] Nico Döttling, Satrajit Ghosh, Jesper Buus Nielsen, Tobias Nilges, and Roberto Trifiletti. Tinyole: Efficient actively secure two-party computation from oblivious linear function evaluation. In *ACM CCS 2017*, 2017.

[21] Nico Döttling and Sanjam Garg. Identity-based encryption from the diffie-hellman assumption. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, pages 537–569, 2017. **Best Paper Award**.

[22] Chongwon Cho, Nico Döttling, Sanjam Garg, Divya Gupta, Peihan Miao, and Antigoni Polychroniadou. Laconic oblivious transfer and its applications. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II*, pages 33–65, 2017.

[23] Daniel Apon, Nico Döttling, Sanjam Garg, and Pratyay Mukherjee. Cryptanalysis of indistinguishability obfuscations of circuits over GGH13. In *44th International Colloquium on Automata, Languages, and Programming, ICALP 2017, July 10-14, 2017, Warsaw, Poland*, pages 38:1–38:16, 2017.

[24] Brandon Broadnax, Nico Döttling, Gunnar Hartung, Jörn Müller-Quade, and Matthias Nagel. Concurrently composable security with shielded super-polynomial simulators. In *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International*

Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part I, pages 351–381, 2017.

[25] Nico Döttling, Nils Fleischhacker, Johannes Krupp, and Dominique Schröder. Two-message, oblivious evaluation of cryptographic functionalities. In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part III*, pages 619–648, 2016.

[26] Ignacio Cascudo, Ivan Damgård, Bernardo David, Nico Döttling, and Jesper Buus Nielsen. Rate-1, linear time and additively homomorphic UC commitments. In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part III*, pages 179–207, 2016.

[27] Nico Döttling, Daniel Kraschewski, Jörn Müller-Quade, and Tobias Nilges. From stateful hardware to resettable hardware using symmetric assumptions. In *Provable Security - 9th International Conference, ProvSec 2015, Kanazawa, Japan, November 24-26, 2015, Proceedings*, pages 23–42, 2015. **Best Paper Award**.

[28] Nico Döttling and Dominique Schröder. Efficient pseudorandom functions via on-the-fly adaptation. In *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, pages 329–350, 2015.

[29] Ronald Cramer, Ivan Bjerre Damgård, Nico Döttling, Serge Fehr, and Gabriele Spini. Linear secret sharing schemes from error correcting codes and universal hash functions. In *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II*, pages 313–336, 2015.

[30] Nico Döttling, Daniel Kraschewski, Jörn Müller-Quade, and Tobias Nilges. General statistically secure computation with bounded-resettable hardware tokens. In *Theory of Cryptography - 12th Theory of Cryptography Conference, TCC 2015, Warsaw, Poland, March 23-25, 2015, Proceedings, Part I*, pages 319–344, 2015.

[31] Nico Döttling. Low noise LPN: KDM secure public key encryption and sample amplification. In *Public-Key Cryptography - PKC 2015 - 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, March 30 - April 1, 2015, Proceedings*, pages 604–626, 2015.

[32] Nico Döttling and Jörn Müller-Quade. Lossy codes and a new variant of the learning-with-errors problem. In *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, pages 18–34, 2013.

[33] Nico Döttling, Thilo Mie, Jörn Müller-Quade, and Tobias Nilges. Implementing resettable uc-functionalities with untrusted tamper-proof hardware-tokens. In *Theory of Cryptography - 10th Theory of Cryptography Conference, TCC 2013, Tokyo, Japan, March 3-6, 2013. Proceedings*, pages 642–661, 2013.

[34] Nico Döttling, Jörn Müller-Quade, and Anderson C. A. Nascimento. IND-CCA secure cryptography based on a variant of the LPN problem. In *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, pages 485–503, 2012.

[35] Nico Döttling, Daniel Kraschewski, and Jörn Müller-Quade. Statistically secure linear-rate dimension extension for oblivious affine function evaluation. In *Information Theoretic Security - 6th International Conference, ICITS 2012, Montreal, QC, Canada, August 15-17, 2012. Proceedings*, pages 111–128, 2012.

[36] Nico Döttling, Daniel Kraschewski, and Jörn Müller-Quade. Efficient reductions for non-signaling cryptographic primitives. In *Information Theoretic Security - 5th International Conference, ICITS 2011, Amsterdam, The Netherlands, May 21-24, 2011. Proceedings*, pages 120–137, 2011.

[37] Nico Döttling, Daniel Kraschewski, and Jörn Müller-Quade. Unconditional and composable security using a single stateful tamper-proof hardware token. In *Theory of Cryptography - 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, March 28-30, 2011. Proceedings*, pages 164–181, 2011.

[38] Nico Döttling, Dejan E. Lazich, Jörn Müller-Quade, and Antonio Sobreira de Almeida. Vulnerabilities of wireless key exchange based on channel reciprocity. In *Information Security Applications - 11th International Workshop, WISA 2010, Jeju Island, Korea, August 24-26, 2010, Revised Selected Papers*, pages 206–220, 2010.

[39] Nico Döttling, Dejan E. Lazich, Jörn Müller-Quade, and Antonio Sobreira de Almeida. Wireless key exchange using the gnu radio platform. In *European Reconfigurable Radio Technology Workshop, ERRT*, 2010.

Journal Papers

[1] Nico Döttling, Rafael Dowsley, Jörn Müller-Quade, and Anderson C. A. Nascimento. A CCA2 secure variant of the mceliece cryptosystem. *IEEE Trans. Information Theory*, 58(10):6672–6680, 2012.

[2] Nico Döttling. Low noise LPN: key dependent message secure public key encryption an sample amplification. *IET Information Security*, 10(6):372–385, 2016.

Preprint

[1] Nico Döttling, Thilo Mie, Jörn Müller-Quade, and Tobias Nilges. Basing obfuscation on simple tamper-proof hardware assumptions. *IACR Cryptology ePrint Archive*, 2011:675, 2011.