Jörn-Marc Schmidt

Prof. Dr.techn.

List of Publications

Jörn-Marc Schmidt Leonie Bruckert. Post-Quanten-Kryptographie. *KES*, 34. Jahrgang, Nr. 1, Februar 2018.

Jörn-Marc Schmidt. Schlüsselaushandlung per PAKE-Protokoll. SICHERHEIT & DATENSCHUTZ (01/2017) ¨Blockchain, Kryptografie und Quantencomputer¨ in der iX (06/2017).

Jörn-Marc Schmidt. RFC 8125 - Requirements for Password-Authenticated Key Agreement (PAKE) Schemes. https://trac.tools.ietf.org/html/rfc8125, 2017.

Jörn-Marc Schmidt. Kryptographische und IT-Security-Perpektive auf Blockchain (Proof of Stake). Tangungsband TeleTrusT-Informationstag-Blockchain, 2017.

Michael Hutter and Jörn-Marc Schmidt. The temperature side channel and heating fault attacks. In *Smart Card Research and Advanced Applications*, Lecture Notes in Computer Science, pages 219–235. Springer, 2014.

Dusko Karaklajic, Jörn-Marc Schmidt, , and Ingrid Verbauwhede. Hardware designer's guide to fault attacks. *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, 2013.

Mario Kirschbaum, Thomas Plos, and Jörn-Marc Schmidt. On Secure Multi-Party Computation in Bandwidth-Limited Smart-Meter Systems. In *Availability, Reliability and Security, 2013. ARES '13. International Conference on*. IEEE Computer Society, September 2013.

Jörn-Marc Schmidt and Marcel Medwed. Countermeasures for symmetric key ciphers. In Marc Joye and Michael Tunstall, editors, *Fault Analysis in Cryptography*, chapter 5, pages 73 – 88. Springer, 2012.

Michael Hutter, Mario Kirschbaum, Thomas Plos, Jörn-Marc Schmidt, and Stefan Mangard. Exploiting the Difference of Side-Channel Leakages. In *Constructive Side-Channel Analysis and Secure Design – COSADE 2012, 3rd International Workshop, Darmstadt, Germany, May 3-4, 2012, Proceedings.*, 2012.

Benedikt Gierlichs, Jörn-Marc Schmidt, and Michael Tunstall. Infective computation and dummy rounds: Fault protection for block ciphers without check-before-output. In *LATINCRYPT*, pages 305–321, 2012.

Dusko Karaklajic, Junfeng Fan, Jörn-Marc Schmidt, and Ingrid Verbauwhede. Low-cost fault detection method for ECC using Montgomery powering ladder. In *Design, Automation and Test in Europe, DATE 2011, Grenoble, France, March 14-18, 2011*, pages 1016–1021. IEEE, 2011.

Mario Kirschbaum and Jörn-Marc Schmidt. Learning from Electromagnetic Emanations - A Case Study for iMDPL. In *Second International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2011), 24-25 February 2011, Darmstadt, Germany*, Workshop Proceedings COSADE 2011, pages 50–55, 2011.

Jörn-Marc Schmidt and Marcel Medwed. Fault Attacks on the Montgomery Powering Ladder. In Kyung Hyune Rhee and DaeHun Nyang, editors, *Information Security and Cryptology - ICISC 2010 - 13th International Conference, Seoul, Korea, December 1-3, 2010, Revised Selected Papers*, volume 6829 of *Lecture Notes in Computer Science*, pages 396–406. Springer, 2011.

Ingrid Verbauwhede, Dusko Karaklajic, and Jörn-Marc Schmidt. The Fault Attack Jungle - A Classification Model to Guide You. In Luca Breveglieri, Sylvain Guilley, Israel Koren, David Naccache, and Junko Takahashi, editors, *2011 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2011, Tokyo, Japan, September 29, 2011*, pages 3–8. IEEE, 2011.

Michael Hutter, Mario Kirschbaum, Thomas Plos, and Jörn-Marc Schmidt. Test Apparatus for Side-Channel Resistance Compliance Testing. In *Non-Invasive Attack Testing Workshop - NIAT, Nara, Japan, September 26-27, 2011.*, 2011.

Jörn-Marc Schmidt, Michael Tunstall, Roberto Maria Avanzi, Ilya Kizhvatov, Timo Kasper, and David Oswald. Combined Implementation Attack Resistant Exponentiation. In Michel Abdalla and Paulo S. L. M. Barreto, editors, *Progress in Cryptology - LATINCRYPT 2010, First International Conference on Cryptology and Information Security in Latin America, Puebla, Mexico, August 8-11, 2010, Proceedings*, volume 6212 of *Lecture Notes in Computer Science*, pages 305–322. Springer, 2010.

Marcel Medwed and Jörn-Marc Schmidt. A Continuous Fault Countermeasure for AES Providing a Constant Error Detection Rate. In Luca Breveglieri, Marc Joye, Israel Koren, David Naccache, and Ingrid Verbauwhede, editors, *Proceedings of the Seventh International Workshop, FDTC 2010, Santa Barbara, California, 21 August 2010*, volume 7. IEEE Computer Society, August 2010.

Stefan Tillich, Martin Feldhofer, Mario Kirschbaum, Thomas Plos, Jörn-Marc Schmidt, and Alexander Szekely. Hardware Implementations of the Round-Two SHA-3 Candidates: Comparison on a Common Ground. In *Proceedings of Austrochip 2010, October 6, 2010, Villach, Austria*, pages 43–48, October 2010. ISBN 978-3-200-01945-4.

Stefan Tillich, Martin Feldhofer, Mario Kirschbaum, Thomas Plos, Jörn-Marc Schmidt, and Alexander Szekely. Uniform Evaluation of Hardware Implementations of the Round-Two SHA-3 Candidates. August 2010.

Jean-Francois Gallais, Johann Großschädl, Neil Hanley, Markus Kasper, Marcel Medwed, Francesco Regazzoni, Jörn-Marc Schmidt, Stefan Tillich, and Marcin Wojcik. Hardware Trojans for Inducing or Amplifying Side-Channel Leakage of Cryptographic Software. In *Proceedings of 2nd International Conference on Trusted Systems, (INTRUST) 2010, Beijing, China, 13-15 December 2010*, 2010.

Jörn-Marc Schmidt, Thomas Plos, Mario Kirschbaum, Michael Hutter, Marcel Medwed, and Christoph Herbst. Side-Channel Leakage Across Borders. In Dieter Gollmann and Jean-Louis Lanet, editors, *Smart Card Research and Advanced Applications 9th IFIP WG 8.8/11.2 International Conference, CARDIS 2010,* *April 13-16, 2010, Passau, Germany, Proceedings*, Lecture Notes in Computer Science, pages 36–48. Springer, April 2010.

Michael Hutter, Jörn-Marc Schmidt, and Thomas Plos. Contact-Based Fault Injections and Power Analysis on RFID Tags. In *European Conference on Circuit Theory and Design 2009, EC-CTD*, 2009.

Marcel Medwed and Jörn-Marc Schmidt. Coding Schemes for Arithmetic and Logic Operations - How Robust Are They? In Heung Youl Youm and Moti Yung, editors, *10th International Workshop on Information Security Applications (WISA 2009), Busan, Korea, August 25-27, 2009*, pages 51–65, 2009.

Jörn-Marc Schmidt, Michael Hutter, and Thomas Plos. Optical Fault Attacks on AES: A Threat in Violet. In David Naccache and Elisabeth Oswald, editors, *Fault Diagnosis and Tolerance in Cryptography, Sixth International Workshop, FDTC 2009, Lausanne, Switzerland, September 6, 2009, Procceedings*, pages 13–22. IEEE-CS Press, September 2009.

Jörn-Marc Schmidt and Marcel Medwed. A Fault Attack on ECDSA. In David Naccache and Elisabeth Oswald, editors, *Fault Diagnosis and Tolerance in Cryptography, Sixth International Workshop, FDTC 2009, Lausanne, Switzerland, September 6, 2009, Procceedings*, pages 93–99. IEEE-CS Press, September 2009.

Stefan Tillich, Martin Feldhofer, Mario Kirschbaum, Thomas Plos, Jörn-Marc Schmidt, and Alexander Szekely. High-Speed Hardware Implementations of BLAKE, Blue Midnight Wish, CubeHash, ECHO, Fugue, Grøstl, Hamsi, JH, Keccak, Luffa, Shabal, SHAvite-3, SIMD, and Skein. Cryptology ePrint Archive, Report 2009/510, 2009.

Jörn-Marc Schmidt and Stefan Tillich. On the Security of Untrusted Memory. In *Availability, Reliability and Security, 2009. ARES '09. International Conference on*, pages 329–334. IEEE Computer Society, March 2009.

Michael Hutter, Jörn-Marc Schmidt, and Thomas Plos. RFID and its Vulnerability to Faults. In Elisabeth Oswald and Pankaj

Rohatgi, editors, *Cryptographic Hardware and Embedded Systems – CHES 2008, 10th International Workshop, Washington DC, USA, August 10-13, 2008, Proceedings*, volume 5154 of *Lecture Notes in Computer Science*, pages 363–379. Springer, August 2008.

Marcel Medwed and Jörn-Marc Schmidt. A Generic Fault Countermeasure Providing Data and Program Flow Integrity. In Luca Breveglieri, Shay Gueron, Israel Koren, David Naccache, and Jean-Pierre Seifert, editors, *Fault Diagnosis and Tolerance in Cryptography, Fifth International Workshop, FDTC 2008, Washington DC, USA, August 10, 2008, Proceedings*, pages 68–73. IEEE Computer Society, August 2008.

Jörn-Marc Schmidt. A Chemical Memory Snapshot. In Gilles Grimaud and François-Xavier Standaert, editors, *Proceedings of the Eight Smart Card Research and Advanced Application Conference, CARDIS '08, September 8-11, 2008, London, UK, Proceedings*, volume 5189 of *Lecture Notes in Computer Science*, pages 283–289. Springer, September 2008.

Jörn-Marc Schmidt and Christoph Herbst. A Practical Fault Attack on Square and Multiply. In Luca Breveglieri, Shay Gueron, Israel Koren, David Naccache, and Jean-Pierre Seifert, editors, *Fault Diagnosis and Tolerance in Cryptography, Fifth International Workshop, FDTC 2008, Washington DC, USA, August 10, 2008, Proceedings*, pages 53–58. IEEE Computer Society, August 2008.

Jörn-Marc Schmidt and Chong Hee Kim. A Probing Attack on AES. In Kyo-Il Chung, Moti Yung, and Kiwook Sohn, editors, *9th International Workshop on Information Security Applications (WISA 2008), Jeju Island, Korea, September 23-25, 2008, Proceedings*, volume 5379 of *Lecture Notes in Computer Science*, pages 256–265. Springer, September 2008.

Jörn-Marc Schmidt and Michael Hutter. Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results. In Karl Christian Posch and Johannes Wolkerstorfer, editors, *Proceedings of Austrochip 2007, October 11, 2007, Graz, Austria*, pages 61–67. Verlag der Technischen Universität Graz, October 2007. ISBN 978-3-902465-87-0.