List of Publications

by Michael Muehlberghuber

March 22, 2015

Book Chapters

[1] M. Muehlberghuber, C. Keller, F. K. Gürkaynak, and N. Felber, "FPGA-Based High-Speed Authenticated Encryption System," in *VLSI-SoC: From Algorithms to Circuits and System-on-Chip Design*, ser. IFIP Advances in Information and Communication Technology, A. Burg, A. Coşkun, M. Guthaus, S. Katkoori, and R. Reis, Eds. Springer Berlin Heidelberg, 2013, vol. 418, pp. 1–20, http://dx.doi.org/10.1007/978-3-642-45073-0_1.

Peer-Reviewed Conference Proceedings

[1] M. Muehlberghuber, T. Korak, P. Dunst, and M. Hutter, "Zorro - A Masked Keccak Hardware Implementation for Authenticated Encryption," in *6th International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE'15)*, 2015, Note: to be published.

[2] O. Söll, T. Korak, M. Muehlberghuber, and M. Hutter, "EM-Based Detection of Hardware Trojans on FPGAs," in *7th IEEE International Symposium on Hardware-Oriented Security and Trust (HOST'14)*, May 2014, pp. 84–87, http://dx.doi.org/10.1109/HST.2014.6855574.

[3] M. Gautschi, M. Muehlberghuber, A. Traber, S. Stucki, M. Baer, R. Andri, L. Benini, B. Muheim, and H. Kaeslin, "SIR10US: A Tightly Coupled Elliptic-Curve Cryptography Co-Processor for the OpenRISC," in *25th IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP'14)*, June 2014, pp. 25–29, http://dx.doi.org/10.1109/ASAP.2014.6868626.

[4] C. Nagl, M. Muehlberghuber, and F. K. Gürkaynak, "Evaluation of the Back-End Design Overhead for ASIC Implementations of Large-Operand Multipliers Targeting Resource-Constrained Environments," in *22nd Austrian Workshop on Microelectronics (Austrochip'14)*, Oct. 2014, pp. 1–6, http://dx.doi.org/10.1109/Austrochip.2014.6946314.

[5] M. Muehlberghuber, F. K. Gürkaynak, T. Korak, P. Dunst, and M. Hutter, "Red Team vs. Blue Team Hardware Trojan Analysis: Detection of a Hardware Trojan on an Actual ASIC," in *2nd International Workshop on Hardware and Architectural Support for Security and Privacy (HASP'13)*. New York, NY, USA: ACM, 2013, pp. 1:1–1:8, http://dx.doi.org/10.1145/2487726.2487727.

[6] M. Muehlberghuber, C. Keller, N. Felber, and C. Pendl, "100 Gbit/s Authenticated Encryption Based on Quantum Key Distribution," in *20th IEEE/IFIP International Conference on VLSI and System-on-Chip (VLSI-SoC'12)*, Oct. 2012, pp. 123–128, http://dx.doi.org/10.1109/VLSI-SoC.2012.6379017.

[7] M. Pelnar, M. Muehlberghuber, and M. Hutter, "Putting together What Fits together - GrÆStl," in *11th International Conference on Smart Card Research and Advanced Applications (CARDIS'12)*, ser. Lecture Notes in Computer Science, S. Mangard, Ed. Springer Berlin Heidelberg, 2013, vol. 7771, pp. 173–187, http://dx.doi.org/10.1007/978-3-642-37288-9_12.

[8] S. Tillich, M. Feldhofer, W. Issovits, T. Kern, H. Kureck, M. Mühlberghuber, G. Neubauer, A. Reiter, A. Köfler, and M. Mayrhofer, "Compact Hardware Implementations of the SHA-3 Candidates ARIRANG, BLAKE, Grøstl, and Skein," *IACR ePrint Report*, 2009, http://eprint.iacr.org/2009/349.

Other Contributions (incl. Not-Security Related)

[1] H. Zbinden, N. Walenta, O. Guinnard, R. Houlmann, C. L. C. Wen, B. Korzh, T. Lunghi, N. Gisin, A. Burg, J. Constantin, M. Legré, P. Trinkler, D. Caselunghe, N. Kulesza, G. Trolliet, F. Vannel, P. Junod, O. Auberson, Y. Graf, G. Curchod, G. Habegger, E. Messerli, C. Portmann, L. Henzen, C. Keller, C. Pendl, M. Mühlberghuber, C. Roth, N. Felber, F. Gürkaynak, D. Schöni, and B. Muheim, "Continuous QKD and high speed data encryption," pp. 88 990P–88 990P–4, 2013, http://dx.doi.org/10.1117/12.2032731.

[2] L. Bai, P. Maechler, M. Muehlberghuber, and H. Kaeslin, "High-Speed Compressed Sensing Reconstruction on FPGA Using OMP and AMP," in *19th IEEE International Conference on Electronics, Circuits and Systems (ICECS'12)*, Dec. 2012, pp. 53–56, http://dx.doi.org/10.1109/ICECS.2012.6463559.