

Publikationen

- (2020): Lightweight edge authentication for software defined networks. In: Computing (Special Issue), no. 8 August 2020. DOI: 10.1007/s00607-020-00835-4.
- (2019): Delegation of Authentication to the Data Plane in Software Defined Networks. In: Proceedings of the 18th IEEE International Conference on Ubiquitous Computing and Communications (IUCC 2019) [October 21-23, 2019, Shenyang, China]. DOI: 10.1109/IUCC/DSCI/SmartCNS.2019.00038.
- (2019): On the Energy Consumption of Quantum-resistant Cryptographic Software Implementations Suitable for Wireless Sensor Networks. In: Proceedings of the 16th International Joint Conference on e-Business and Telecommunications (July 26-28, 2019; Prague, Czech Republic), vol. Vol. 2 (SECRYPT 2019 : 16th International Conference on Security and Cryptography). DOI: 10.5220/0007835600720083.
- (2019): Comparison of Energy-Efficient Key Management Protocols for Wireless Sensor Networks. In: Proceedings of the 2019 International Electronics Communication Conference (IECC '19) [July 7-9, 2019; Okinawa, Japan]. DOI: 10.1145/3343147.3343156.
- (2019): Hacking an optics manufacturing machine: You don't see it coming?!. In: Proceedings of SPIE 11171 (Sixth European Seminar on Precision Optics Manufacturing, 1117101 [9-10 April 2019, Teisnach]), Bellingham, WA, USA. DOI: 10.1117/12.2526691.
- (2019): A Lightweight Quantum-Safe Security Concept for Wireless Sensor Network Communication. In: Proceedings of the IEEE Annual International Conference on Pervasive Computing and Communications Workshops (March 11-15, 2019; Kyoto, Japan). DOI: 10.1109/PERCOMW.2019.8730749.
- (2019): A Resource-Preserving Self-Regulating Uncoupled MAC Algorithm to be Applied in Incident Detection. In: Computers & Security, vol. 85, no. August, pp. 270-285. DOI: 10.1016/j.cose.2019.05.010.
- (2018): A Practical Introduction to Cryptographic Engineering. [Invited Talk;eingeladen von Dalibor Fiala (PhD)].
- (2018): A Vendor-Neutral Unified Core for Cryptographic Operations in $GF(p)$ and $GF(2^m)$ Based on Montgomery Arithmetic (Article ID 4983404). In: Security and Communication Networks, no. 9, pp. 1-18. DOI: 10.1155/2018/4983404.
- (2018): Incident Reaction Based on Intrusion Detections' Alert Analysis. In: Proceedings of the 23rd International Conference on Applied Electronics (AE) 2018 (University of West Bohemia, Pilsen, Czech Republic; September 11-12, 2018). DOI: 10.23919/AE.2018.8501419.
- (2017): Experimental assessment of FIRO- and GARO-based noise sources for digital TRNG designs on FPGAs. In: Proceedings of the 22nd International Conference on Applied Electronics (AE 2017) [Sep 5-7, 2017;University of West Bohemia, Pilsen, Czech Republic]. DOI: 10.23919/AE.2017.8053618.
- (2017): Assessment simulation model for uncoupled message authentication. In: Proceedings of the 22nd International Conference on Applied Electronics (AE 2017) [Sep 5-7, 2017;University of West Bohemia, Pilsen, Czech Republic]. DOI: 10.23919/AE.2017.8053580.
- (2016): Embedded Plug-In Devices to Secure Industrial Network Communications. In: IEEE Proceedings of the 21st International Conference on Applied Electronics (Sept 6-7 2016, Pilsen, Czech Republic).
- (2014): Embedded Trusted Computing on ARM-based Systems. In: Security Forum 2014, Hagenberg im Mühlkreis, Österreich.

- (2014): Resilience in Embedded Industrial Networks. In: Trusted Computing Group Members Meeting 2014, Barcelona, Spanien.
- (2014): Trusted Computing Concepts for Resilient Embedded Networks. International Workshop on Engineering Cyber Security and Resilience. In: 2014 ASE Bigdata/SocialCom/Cybersecurity Conference, Stanford, CA, USA.
- (2013): Enhanced Embedded Device Security by Combining Hardware-Based Trust Mechanisms. Poster-Session. In: ACM Conference on Computer and Communications Security, Berlin.
- (2013): On the Implementation of an Efficient Multiplier Logic for FPGA-based Cryptographic Applications. In: IEEE Applied Electronics International Conference, Pilsen, Tschechische Republik.
- (2013): On the Implementation of a Lightweight Generic FPGA ECC Crypto-Core over GF(p). In: IEEE Applied Electronics International Conference, Pilsen, Tschechische Republik.
- (2012): Reconfigurable Trust for Embedded Computing Platforms. In: IEEE Applied Electronics International Conference, Pilsen, Tschechische Republik.
- (2012): The Establishment of High Degrees of Trust in a Linux Environment. In: Embedded World International Conference 2012, Nürnberg.
- (2011): Utilizing a State-of-the-art Trust Anchor in Order to Increase the Trustworthiness of Embedded Platforms. In: Embedded World International Conference 2011, Nürnberg.
- (2011): Trustworthy Building Blocks for a More Secure Embedded Computing Environment. In: Applied Electronics International Conference, Pilsen, Tschechische Republik.
- (2010): The Benefits of Combining Trusted Computing with Virtualization Techniques. In: IEEE International Conference on Applied Electronics 2010, Pilsen, Tschechische Republik.
- (2010): The Benefits of Combining Trusted Computing with Virtualization Techniques. In: Applied Electronics International Conference, Pilsen, Tschechische Republik.