

Stefan Mangard - Full List of Publications

Peer-Reviewed Conference and Journal Publications

- [154] E. Andreeva, S. Mangard, R. Nagpal, A. Roy, and S. Trevisani. “Power Analysis and Countermeasures on the MiMC Block Cipher”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst. (to appear)* 2026.4 (2026).
- [153] F. Draschbacher, L. Maar, L. Schumm, R. Denifl, L. Treffner, and S. Mangard. “Clone2Pwn: A Systematic Security Analysis of Data Migration Tools in the Android Ecosystem”. In: *Computer Security - ESORICS 2026 - 31st European Symposium on Research in Computer Security, 2026, Proceedings (to appear)*. Lecture Notes in Computer Science. Springer, 2026.
- [152] E. M. García, L. Maar, M. Unterguggenberger, and S. Mangard. “Fence2Pwn: KFENCE-Enabled Kernel Exploitation Bypassing Slab Hardening and Memory Tagging”. In: *35th USENIX Security Symposium, USENIX Security 2026, Baltimore, MD, USA, August 12-14, 2026 (to appear)*. Ed. by E. Redmiles and B. Stock. USENIX Association, 2026. URL: <https://www.usenix.org/conference/usenixsecurity26/presentation/garcia>.
- [151] E. M. García, L. Maar, M. Unterguggenberger, M. Oberhuber, and S. Mangard. “LeakyTree: Cross-VM Bit-by-Bit Deduplicated Page Leakage via Linux Kernel Samepage Merging Internals”. In: *Proceedings of the 2026 ACM SIGSAC Conference on Computer and Communications Security, CCS 2026 (to appear)*. ACM, 2026.
- [150] M. Oberhuber, M. Unterguggenberger, M. Wistauder, A. Kogler, R. Nagpal, and S. Mangard. “PowerHook: Enabling Software-Based Power Side Channels Against AMD SEV Technologies via Transient-Execution Replay”. In: *20th USENIX WOOT Conference on Offensive Technologies, WOOT 2026, Baltimore, MD, USA, August 10-11, 2026*. Ed. by A. Bianchi and J. Classen. USENIX Association, 2026, pp. 211–228. URL: <https://www.usenix.org/conference/woot26/presentation/oberhuber>.
- [149] L. Schumm, L. Lamster, E. Kraft, M. Medwed, and S. Mangard. “Implicit Control-Flow Integrity: Efficient Runtime Security for Embedded Devices”. In: *Annual Computer Security Applications Conference, ACSAC 2026 (to appear)*. ACM, 2026.
- [148] M. Waser, P. Gollob, M. Unterguggenberger, and S. Mangard. “CAGE-V: Confidential Computing Architecture supporting Guest Enclaves for RISC-V”. In: *Proceedings of the ACM Asia Conference on Computer and Communications Security, ASIA CCS 2026, Bangalore, India, June 1-5, 2026*. Ed. by M. Agrawal, I. Molloy, V. Pandit, D. Mukhopadhyay, and K. Paterson. ACM, 2026, pp. 577–590. DOI: [10.1145/3779208.3807479](https://doi.org/10.1145/3779208.3807479).
- [147] F. Draschbacher, L. Maar, M. Oberhuber, and S. Mangard. “ChoiceJacking: Compromising Mobile Devices through Malicious Chargers like a Decade ago”. In: *34th USENIX Security Symposium, USENIX Security 2025, Seattle, WA, USA, August 13-15, 2025*. Ed. by L. Bauer and G. Pellegrino. USENIX Association, 2025, pp. 4363–4379. URL: <https://www.usenix.org/conference/usenixsecurity25/presentation/draschbacher>.

- [146] L. Lamster, F. Rauscher, M. Unterguggenberger, and S. Mangard. “WaitWatcher and WaitGuard: Detecting Flush-Based Cache Side-Channels Through Spurious Wakeups”. In: *Computer Security - ESORICS 2025 - 30th European Symposium on Research in Computer Security, Toulouse, France, September 22-24, 2025, Proceedings, Part III*. Ed. by V. Nicomette, A. Benzekri, N. Boulahia-Cuppens, and J. Vaidya. Vol. 16055. Lecture Notes in Computer Science. Springer, 2025, pp. 303–322. DOI: [10.1007/978-3-032-07894-0_16](https://doi.org/10.1007/978-3-032-07894-0_16).
- [145] L. Lamster, M. Unterguggenberger, M. Waser, D. Schrammel, and S. Mangard. “FatPTE - Expanding Page Table Entries for Security”. In: *Availability, Reliability and Security - 20th International Conference, ARES 2025, Ghent, Belgium, August 11-14, 2025, Proceedings, Part II*. Ed. by M. D. Preda, S. Schrittwieser, V. Naessens, and B. D. Sutter. Vol. 15993. Lecture Notes in Computer Science. Springer, 2025, pp. 127–148. DOI: [10.1007/978-3-032-00627-1_7](https://doi.org/10.1007/978-3-032-00627-1_7).
- [144] L. Maar, F. Draschbacher, L. Schumm, E. M. García, and S. Mangard. “The Doom of Device Drivers: Your Android Device (Most Likely) has N-Day Kernel Vulnerabilities”. In: *34th USENIX Security Symposium, USENIX Security 2025, Seattle, WA, USA, August 13-15, 2025*. Ed. by L. Bauer and G. Pellegrino. USENIX Association, 2025, pp. 4205–4224. URL: <https://www.usenix.org/conference/usenixsecurity25/presentation/maar-doom>.
- [143] L. Maar, L. Giner, D. Gruss, and S. Mangard. “When Good Kernel Defenses Go Bad: Reliable and Stable Kernel Exploits via Defense-Amplified TLB Side-Channel Leaks”. In: *34th USENIX Security Symposium, USENIX Security 2025, Seattle, WA, USA, August 13-15, 2025*. Ed. by L. Bauer and G. Pellegrino. USENIX Association, 2025, pp. 7447–7465. URL: <https://www.usenix.org/conference/usenixsecurity25/presentation/maar-kernel>.
- [142] L. Maar, J. Juffinger, T. Steinbauer, D. Gruss, and S. Mangard. “KernelSnitch: Side Channel-Attacks on Kernel Data Structures”. In: *32nd Annual Network and Distributed System Security Symposium, NDSS 2025, San Diego, California, USA, February 24-28, 2025*. The Internet Society, 2025. URL: <https://www.ndss-symposium.org/ndss-paper/kernelSnitch-side-channel-attacks-on-kernel-data-structures/>.
- [141] R. Nagpal, V. Hadzic, R. Primas, and S. Mangard. “Efficient SPA Countermeasures Using Redundant Number Representation with Application to ML-KEM”. In: *Selected Areas in Cryptography - SAC 2025 - 32nd International Conference, Toronto, ON, Canada, August 13-15, 2025, Revised Selected Papers*. Ed. by C. Boura, A. Mashatan, and A. Miri. Vol. 16207. Lecture Notes in Computer Science. Springer, 2025, pp. 753–780. DOI: [10.1007/978-3-032-10536-3_28](https://doi.org/10.1007/978-3-032-10536-3_28).
- [140] M. Oberhuber, M. Unterguggenberger, L. Maar, A. Kogler, and S. Mangard. “Power-Related Side-Channel Attacks using the Android Sensor Framework”. In: *32nd Annual Network and Distributed System Security Symposium, NDSS 2025, San Diego, California, USA, February 24-28, 2025*. The Internet Society, 2025. URL: <https://www.ndss-symposium.org/ndss-paper/power-related-side-channel-attacks-using-the-android-sensor-framework/>.
- [139] M. Unterguggenberger, L. Lamster, M. Oberhuber, S. Scherer, and S. Mangard. “Code Encryption with Intel TME-MK for Control-Flow Enforcement”. In: *Computer Security - ESORICS 2025 - 30th European*

Symposium on Research in Computer Security, Toulouse, France, September 22-24, 2025, Proceedings, Part II. Ed. by V. Nicomette, A. Benzekri, N. Boulahia-Cuppens, and J. Vaidya. Vol. 16054. Lecture Notes in Computer Science. Springer, 2025, pp. 359–378. DOI: [10.1007/978-3-032-07891-9_19](https://doi.org/10.1007/978-3-032-07891-9_19).

- [138] M. Unterguggenberger, L. Lamster, D. Schrammel, M. Schwarzl, and S. Mangard. “TME-Box: Scalable In-Process Isolation through Intel TME-MK Memory Encryption”. In: *32nd Annual Network and Distributed System Security Symposium, NDSS 2025, San Diego, California, USA, February 24-28, 2025*. The Internet Society, 2025. URL: <https://www.ndss-symposium.org/ndss-paper/tme-box-scalable-in-process-isolation-through-intel-tme-mk-memory-encryption/>.
- [137] M. Unterguggenberger, D. Schrammel, L. Maar, L. Lamster, V. Hadzic, and S. Mangard. “Cryptographic Least Privilege Enforcement for Scalable Memory Isolation”. In: *IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2025, San Jose, CA, USA, May 5-8, 2025*. IEEE, 2025, pp. 312–323. DOI: [10.1109/HOST64725.2025.11050045](https://doi.org/10.1109/HOST64725.2025.11050045).
- [136] M. Waser, L. Lamster, D. Schrammel, M. Unterguggenberger, and S. Mangard. “CHERI UNCHAINED: Generic Instruction and Register Control for CHERI Capabilities”. In: *Availability, Reliability and Security - 20th International Conference, ARES 2025, Ghent, Belgium, August 11-14, 2025, Proceedings, Part II*. Ed. by M. D. Preda, S. Schrittwieser, V. Naessens, and B. D. Sutter. Vol. 15993. Lecture Notes in Computer Science. Springer, 2025, pp. 149–170. DOI: [10.1007/978-3-032-00627-1_8](https://doi.org/10.1007/978-3-032-00627-1_8).
- [135] M. Waser, D. Schrammel, R. Schilling, and S. Mangard. “FAULTLESS: Flexible and Transparent Fault Protection for Superscalar RISC-V Processors”. In: *Detection of Intrusions and Malware, and Vulnerability Assessment - 22nd International Conference, DIMVA 2025, Graz, Austria, July 9-11, 2025, Proceedings, Part II*. Ed. by M. Egele, V. Moonsamy, D. Gruss, and M. Carminati. Vol. 15748. Lecture Notes in Computer Science. Springer, 2025, pp. 297–315. DOI: [10.1007/978-3-031-97623-0_18](https://doi.org/10.1007/978-3-031-97623-0_18).
- [134] G. Cassiers, B. Gigerl, S. Mangard, C. Momin, and R. Nagpal. “Compress: Generate Small and Fast Masked Pipelined Circuits”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2024.3 (2024), pp. 500–529. DOI: [10.46586/TCHES.V2024.I3.500-529](https://doi.org/10.46586/TCHES.V2024.I3.500-529).
- [133] B. Gigerl, F. Klug, S. Mangard, F. Mendel, and R. Primas. “Smooth Passage with the Guards: Second-Order Hardware Masking of the AES with Low Randomness and Low Latency”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2024.1 (2024), pp. 309–335. DOI: [10.46586/TCHES.V2024.I1.309-335](https://doi.org/10.46586/TCHES.V2024.I1.309-335).
- [132] B. Gigerl, K. Pretterhofer, and S. Mangard. “Security Aspects of Masking on FPGAs”. In: *IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2024, Tysons Corner, VA, USA, May 6-9, 2024*. IEEE, 2024, pp. 199–210. DOI: [10.1109/HOST55342.2024.10545383](https://doi.org/10.1109/HOST55342.2024.10545383).
- [131] V. Hadzic, G. Cassiers, R. Primas, S. Mangard, and R. Bloem. “Quantile: Quantifying Information Leakage”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2024.1 (2024), pp. 433–456. DOI: [10.46586/TCHES.V2024.I1.433-456](https://doi.org/10.46586/TCHES.V2024.I1.433-456).
- [130] L. Lamster, M. Unterguggenberger, D. Schrammel, and S. Mangard. “Voodoo: Memory Tagging, Authenticated Encryption, and Error Correction through MAGIC”. In: *33rd USENIX Security Symposium, USENIX Security 2024, Philadelphia, PA, USA, August 14-16, 2024*. Ed. by D. Balzarotti and W. Xu. USENIX As-

sociation, 2024. URL: <https://www.usenix.org/conference/usenixsecurity24/presentation/lamster>.

- [129] L. Maar, F. Draschbacher, L. Lamster, and S. Mangard. “Defects-in-Depth: Analyzing the Integration of Effective Defenses against One-Day Exploits in Android Kernels”. In: *33rd USENIX Security Symposium, USENIX Security 2024, Philadelphia, PA, USA, August 14-16, 2024*. Ed. by D. Balzarotti and W. Xu. USENIX Association, 2024. URL: <https://www.usenix.org/conference/usenixsecurity24/presentation/maar-defects>.
- [128] L. Maar, S. Gast, M. Unterguggenberger, M. Oberhuber, and S. Mangard. “SLUBStick: Arbitrary Memory Writes through Practical Software Cross-Cache Attacks within the Linux Kernel”. In: *33rd USENIX Security Symposium, USENIX Security 2024, Philadelphia, PA, USA, August 14-16, 2024*. Ed. by D. Balzarotti and W. Xu. USENIX Association, 2024. URL: <https://www.usenix.org/conference/usenixsecurity24/presentation/maar-slubstick>.
- [127] L. Maar, P. Nasahl, and S. Mangard. “Beyond the Edges of Kernel Control-Flow Hijacking Protection with HEK-CFI”. In: *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security, ASIA CCS 2024, Singapore, July 1-5, 2024*. Ed. by J. Zhou, T. Q. S. Quek, D. Gao, and A. A. Cárdenas. ACM, 2024. DOI: [10.1145/3634737.3661135](https://doi.org/10.1145/3634737.3661135).
- [126] R. Nagpal, G. Cassiers, R. Primas, C. Knoll, F. Pernkopf, and S. Mangard. “On Loopy Belief Propagation for SASCAs: An Analysis and Empirical Study of the Inference Problem”. In: *IACR Commun. Cryptol.* 1.4 (2024), p. 15. DOI: [10.62056/AYL8KSDJA](https://doi.org/10.62056/AYL8KSDJA).
- [125] D. Schrammel, M. Unterguggenberger, L. Lamster, S. Sultana, K. Grewal, M. LeMay, D. M. Durham, and S. Mangard. “Memory Tagging using Cryptographic Integrity on Commodity x86 CPUs”. In: *9th IEEE European Symposium on Security and Privacy, EuroS&P 2024, Vienna, Austria, July 8-12, 2024*. IEEE, 2024, pp. 311–326. DOI: [10.1109/EUROSP60621.2024.00024](https://doi.org/10.1109/EUROSP60621.2024.00024).
- [124] S. Tollec, V. Hadzic, P. Nasahl, M. Asavoe, R. Bloem, D. Couroussé, K. Heydemann, M. Jan, and S. Mangard. “Fault-Resistant Partitioning of Secure CPUs for System Co-Verification against Faults”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2024.4 (2024), pp. 179–204. DOI: [10.46586/TCHES.V2024.I4.179-204](https://doi.org/10.46586/TCHES.V2024.I4.179-204).
- [123] T. Wedenig, R. Nagpal, G. Cassiers, S. Mangard, and R. Peharz. “Exact Soft Analytical Side-Channel Attacks using Tractable Circuits”. In: *Forty-first International Conference on Machine Learning, ICML 2024, Vienna, Austria, July 21-27, 2024*. Ed. by R. Salakhutdinov, Z. Kolter, K. A. Heller, A. Weller, N. Oliver, J. Scarlett, and F. Berkenkamp. Vol. 235. Proceedings of Machine Learning Research. PMLR / OpenReview.net, 2024, pp. 52472–52483. URL: <https://proceedings.mlr.press/v235/wedenig24a.html>.
- [122] B. Gigerl, R. Primas, and S. Mangard. “Formal Verification of Arithmetic Masking in Hardware and Software”. In: *Applied Cryptography and Network Security - 21st International Conference, ACNS 2023, Kyoto, Japan, June 19-22, 2023, Proceedings, Part I*. Ed. by M. Tibouchi and X. Wang. Vol. 13905. Lecture Notes in Computer Science. Springer, 2023, pp. 3–32. DOI: [10.1007/978-3-031-33488-7_1](https://doi.org/10.1007/978-3-031-33488-7_1).

- [121] B. Gigerl, R. Primas, and S. Mangard. “Secure Context Switching of Masked Software Implementations”. In: *Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security, ASIA CCS 2023, Melbourne, VIC, Australia, July 10-14, 2023*. Ed. by J. K. Liu, Y. Xiang, S. Nepal, and G. Tsudik. ACM, 2023, pp. 980–992. DOI: [10.1145/3579856.3595798](https://doi.org/10.1145/3579856.3595798).
- [120] L. Giner, S. Steinegger, A. Purnal, M. Eichlseder, T. Unterluggauer, S. Mangard, and D. Gruss. “Scatter and Split Securely: Defeating Cache Contention and Occupancy Attacks”. In: *44th IEEE Symposium on Security and Privacy, SP 2023, San Francisco, CA, USA, May 21-25, 2023*. IEEE, 2023, pp. 2273–2287. DOI: [10.1109/SP46215.2023.10179440](https://doi.org/10.1109/SP46215.2023.10179440).
- [119] A. Kogler, J. Juffinger, L. Giner, L. Gerlach, M. Schwarzl, M. Schwarz, D. Gruss, and S. Mangard. “Collide+Power: Leaking Inaccessible Data with Software-based Power Side Channels”. In: *32nd USENIX Security Symposium, USENIX Security 2023, Anaheim, CA, USA, August 9-11, 2023*. Ed. by J. A. Calandrino and C. Troncoso. USENIX Association, 2023, pp. 7285–7302. URL: <https://www.usenix.org/conference/usenixsecurity23/presentation/kogler>.
- [118] L. Lamster, M. Unterguggenberger, D. Schrammel, and S. Mangard. “HashTag: Hash-based Integrity Protection for Tagged Architectures”. In: *32nd USENIX Security Symposium, USENIX Security 2023, Anaheim, CA, USA, August 9-11, 2023*. Ed. by J. A. Calandrino and C. Troncoso. USENIX Association, 2023, pp. 2797–2814. URL: <https://www.usenix.org/conference/usenixsecurity23/presentation/lamster>.
- [117] L. Maar, M. Schwarzl, F. Rauscher, D. Gruss, and S. Mangard. “DOPE: DOnain Protection Enforcement with PKS”. In: *Annual Computer Security Applications Conference, ACSAC 2023, Austin, TX, USA, December 4-8, 2023*. ACM, 2023, pp. 662–676. DOI: [10.1145/3627106.3627113](https://doi.org/10.1145/3627106.3627113).
- [116] P. Nasahl and S. Mangard. “SCRAMBLE-CFI: Mitigating Fault-Induced Control-Flow Attacks on OpenTitan”. In: *Proceedings of the Great Lakes Symposium on VLSI 2023, GLSVLSI 2023, Knoxville, TN, USA, June 5-7, 2023*. Ed. by H. Thapliyal, R. F. DeMara, I. Partin-Vaisband, and S. Katkoori. ACM, 2023, pp. 45–50. DOI: [10.1145/3583781.3590221](https://doi.org/10.1145/3583781.3590221).
- [115] P. Nasahl, S. Sultana, H. Liljestrand, K. Grewal, M. LeMay, D. M. Durham, D. Schrammel, and S. Mangard. “EC-CFI: Control-Flow Integrity via Code Encryption Counteracting Fault Attacks”. In: *IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2023, San Jose, CA, USA, May 1-4, 2023*. IEEE, 2023, pp. 24–35. DOI: [10.1109/HOST55118.2023.10132915](https://doi.org/10.1109/HOST55118.2023.10132915).
- [114] P. Nasahl, M. Unterguggenberger, R. Nagpal, R. Schilling, D. Schrammel, and S. Mangard. “SCFI: State Machine Control-Flow Hardening Against Fault Attacks”. In: *Design, Automation & Test in Europe Conference & Exhibition, DATE 2023, Antwerp, Belgium, April 17-19, 2023*. IEEE, 2023, pp. 1–6. DOI: [10.23919/DATE56975.2023.10137038](https://doi.org/10.23919/DATE56975.2023.10137038).
- [113] D. Schrammel, S. Sultana, K. Grewal, M. LeMay, D. M. Durham, M. Unterguggenberger, P. Nasahl, and S. Mangard. “MEMES: Memory Encryption-Based Memory Safety on Commodity Hardware”. In: *Proceedings of the 20th International Conference on Security and Cryptography, SECRIPT 2023, Rome, Italy, July 10-12, 2023*. Ed. by S. D. C. di Vimercati and P. Samarati. SCITEPRESS, 2023, pp. 25–36. DOI: [10.5220/0012050300003555](https://doi.org/10.5220/0012050300003555).

- [112] D. Schrammel, M. Waser, L. Lamster, M. Unterguggenberger, and S. Mangard. “SPEAR-V: Secure and Practical Enclave Architecture for RISC-V”. In: *Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security, ASIA CCS 2023, Melbourne, VIC, Australia, July 10-14, 2023*. Ed. by J. K. Liu, Y. Xiang, S. Nepal, and G. Tsodik. ACM, 2023, pp. 457–468. DOI: [10.1145/3579856.3595784](https://doi.org/10.1145/3579856.3595784).
- [111] M. Unterguggenberger, D. Schrammel, L. Lamster, P. Nasahl, and S. Mangard. “Cryptographically Enforced Memory Safety”. In: *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, CCS 2023, Copenhagen, Denmark, November 26-30, 2023*. Ed. by W. Meng, C. D. Jensen, C. Cremers, and E. Kirda. ACM, 2023, pp. 889–903. DOI: [10.1145/3576915.3623138](https://doi.org/10.1145/3576915.3623138).
- [110] M. Unterguggenberger, D. Schrammel, P. Nasahl, R. Schilling, L. Lamster, and S. Mangard. “Multi-Tag: A Hardware-Software Co-Design for Memory Safety based on Multi-Granular Memory Tagging”. In: *Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security, ASIA CCS 2023, Melbourne, VIC, Australia, July 10-14, 2023*. Ed. by J. K. Liu, Y. Xiang, S. Nepal, and G. Tsodik. ACM, 2023, pp. 177–189. DOI: [10.1145/3579856.3590331](https://doi.org/10.1145/3579856.3590331).
- [109] R. Bloem, B. Gigerl, M. Gourjon, V. Hadzic, S. Mangard, and R. Primas. “Power Contracts: Provably Complete Power Leakage Models for Processors”. In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022*. Ed. by H. Yin, A. Stavrou, C. Cremers, and E. Shi. ACM, 2022, pp. 381–395. DOI: [10.1145/3548606.3560600](https://doi.org/10.1145/3548606.3560600).
- [108] R. Nagpal, B. Gigerl, R. Primas, and S. Mangard. “Riding the Waves Towards Generic Single-Cycle Masking in Hardware”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2022.4 (2022), pp. 693–717. DOI: [10.46586/TCHES.V2022.I4.693-717](https://doi.org/10.46586/TCHES.V2022.I4.693-717).
- [107] P. Nasahl, M. Osorio, P. Vogel, M. Schaffner, T. Trippel, D. Rizzo, and S. Mangard. “SYNFI: Pre-Silicon Fault Analysis of an Open-Source Secure Element”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2022.4 (2022), pp. 56–87. DOI: [10.46586/TCHES.V2022.I4.56-87](https://doi.org/10.46586/TCHES.V2022.I4.56-87).
- [106] R. Schilling, P. Nasahl, and S. Mangard. “FIPAC: Thwarting Fault- and Software-Induced Control-Flow Attacks with ARM Pointer Authentication”. In: *Constructive Side-Channel Analysis and Secure Design - 13th International Workshop, COSADE 2022, Leuven, Belgium, April 11-12, 2022, Proceedings*. Ed. by J. Balasch and C. O’Flynn. Vol. 13211. Lecture Notes in Computer Science. Springer, 2022, pp. 100–124. DOI: [10.1007/978-3-030-99766-3_5](https://doi.org/10.1007/978-3-030-99766-3_5).
- [105] R. Schilling, P. Nasahl, M. Unterguggenberger, and S. Mangard. “SFP: Providing System Call Flow Protection against Software and Fault Attacks”. In: *Proceedings of the 11th International Workshop on Hardware and Architectural Support for Security and Privacy, HASP 2022, Chicago, IL, USA, 1 October 2022*. ACM, 2022, pp. 18–26. DOI: [10.1145/3569562.3569565](https://doi.org/10.1145/3569562.3569565).
- [104] D. Schrammel, S. Weiser, R. Sadek, and S. Mangard. “Jenny: Securing Syscalls for PKU-based Memory Isolation Systems”. In: *31st USENIX Security Symposium, USENIX Security 2022, Boston, MA, USA, August 10-12, 2022*. Ed. by K. R. B. Butler and K. Thomas. USENIX Association, 2022, pp. 936–952. URL: <https://www.usenix.org/conference/usenixsecurity22/presentation/schrammel>.

- [103] B. Gigerl, V. Hadzic, R. Primas, S. Mangard, and R. Bloem. “Coco: Co-Design and Co-Verification of Masked Software Implementations on CPUs”. In: *30th USENIX Security Symposium, USENIX Security 2021, August 11-13, 2021*. Ed. by M. D. Bailey and R. Greenstadt. USENIX Association, 2021, pp. 1469–1486. URL: <https://www.usenix.org/conference/usenixsecurity21/presentation/gigerl>.
- [102] B. Gigerl, R. Primas, and S. Mangard. “Secure and Efficient Software Masking on Superscalar Pipelined Processors”. In: *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part II*. Ed. by M. Tibouchi and H. Wang. Vol. 13091. Lecture Notes in Computer Science. Springer, 2021, pp. 3–32. DOI: [10.1007/978-3-030-92075-3_1](https://doi.org/10.1007/978-3-030-92075-3_1).
- [101] P. Nasahl, R. Schilling, and S. Mangard. “Protecting Indirect Branches Against Fault Attacks Using ARM Pointer Authentication”. In: *IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2021, Tysons Corner, VA, USA, December 12-15, 2021*. IEEE, 2021, pp. 68–79. DOI: [10.1109/HOST49136.2021.9702268](https://doi.org/10.1109/HOST49136.2021.9702268).
- [100] P. Nasahl, R. Schilling, M. Werner, J. Hoogerbrugge, M. Medwed, and S. Mangard. “CrypTag: Thwarting Physical and Logical Memory Vulnerabilities using Cryptographically Colored Memory”. In: *ASIA CCS ’21: ACM Asia Conference on Computer and Communications Security, Virtual Event, Hong Kong, June 7-11, 2021*. Ed. by J. Cao, M. H. Au, Z. Lin, and M. Yung. ACM, 2021, pp. 200–212. DOI: [10.1145/3433210.3453684](https://doi.org/10.1145/3433210.3453684).
- [99] P. Nasahl, R. Schilling, M. Werner, and S. Mangard. “HECTOR-V: A Heterogeneous CPU Architecture for a Secure RISC-V Execution Environment”. In: *ASIA CCS ’21: ACM Asia Conference on Computer and Communications Security, Virtual Event, Hong Kong, June 7-11, 2021*. Ed. by J. Cao, M. H. Au, Z. Lin, and M. Yung. ACM, 2021, pp. 187–199. DOI: [10.1145/3433210.3453112](https://doi.org/10.1145/3433210.3453112).
- [98] R. Schilling, P. Nasahl, S. Weiglhofer, and S. Mangard. “SecWalk: Protecting Page Table Walks Against Fault Attacks”. In: *IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2021, Tysons Corner, VA, USA, December 12-15, 2021*. IEEE, 2021, pp. 56–67. DOI: [10.1109/HOST49136.2021.9702269](https://doi.org/10.1109/HOST49136.2021.9702269).
- [97] S. Steinegger, D. Schrammel, S. Weiser, P. Nasahl, and S. Mangard. “SERVAS! Secure Enclaves via RISC-V Authenticryption Shield”. In: *Computer Security - ESORICS 2021 - 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4-8, 2021, Proceedings, Part II*. Ed. by E. Bertino, H. Schulmann, and M. Waidner. Vol. 12973. Lecture Notes in Computer Science. Springer, 2021, pp. 370–391. DOI: [10.1007/978-3-030-88428-4_19](https://doi.org/10.1007/978-3-030-88428-4_19).
- [96] C. Dobraunig, M. Eichlseder, S. Mangard, F. Mendel, B. Mennink, R. Primas, and T. Unterluggauer. “ISAP v2.0”. In: *IACR Trans. Symmetric Cryptol.* 2020.S1 (2020), pp. 390–416. DOI: [10.13154/TOSC.V2020.IS1.390-416](https://doi.org/10.13154/TOSC.V2020.IS1.390-416).
- [95] P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom. “Spectre attacks: exploiting speculative execution”. In: *Commun. ACM* 63.7 (2020), pp. 93–101. DOI: [10.1145/3399742](https://doi.org/10.1145/3399742).

- [94] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, J. Horn, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, M. Hamburg, and R. Strackx. “Meltdown: reading kernel memory from user space”. In: *Commun. ACM* 63.6 (2020), pp. 46–56. DOI: [10.1145/3357033](https://doi.org/10.1145/3357033).
- [93] D. Schrammel, S. Weiser, S. Steinegger, M. Schwarzl, M. Schwarz, S. Mangard, and D. Gruss. “Donky: Domain Keys - Efficient In-Process Isolation for RISC-V and x86”. In: *29th USENIX Security Symposium, USENIX Security 2020, August 12-14, 2020*. Ed. by S. Capkun and F. Roesner. USENIX Association, 2020, pp. 1677–1694. URL: <https://www.usenix.org/conference/usenixsecurity20/presentation/schrammel>.
- [92] M. Schwarz, S. Weiser, D. Gruss, C. Maurice, and S. Mangard. “Malware Guard Extension: abusing Intel SGX to conceal cache attacks”. In: *Cybersecur.* 3.1 (2020), p. 2. DOI: [10.1186/S42400-019-0042-Y](https://doi.org/10.1186/S42400-019-0042-Y).
- [91] H. Groß, K. Stoffelen, L. D. Meyer, M. Krenn, and S. Mangard. “First-Order Masking with Only Two Random Bits”. In: *Proceedings of ACM Workshop on Theory of Implementation Security, TIS@CCS 2019, London, UK, November 11, 2019*. Ed. by B. Bilgin, S. Petkova-Nikova, and V. Rijmen. ACM, 2019, pp. 10–23. DOI: [10.1145/3338467.3358950](https://doi.org/10.1145/3338467.3358950).
- [90] A. F. Karl, R. Schilling, R. Bloem, and S. Mangard. “Small Faults Grow Up - Verification of Error Masking Robustness in Arithmetically Encoded Programs”. In: *Verification, Model Checking, and Abstract Interpretation - 20th International Conference, VMCAI 2019, Cascais, Portugal, January 13-15, 2019, Proceedings*. Ed. by C. Enea and R. Piskac. Vol. 11388. Lecture Notes in Computer Science. Springer, 2019, pp. 183–204. DOI: [10.1007/978-3-030-11245-5_9](https://doi.org/10.1007/978-3-030-11245-5_9).
- [89] P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom. “Spectre Attacks: Exploiting Speculative Execution”. In: *2019 IEEE Symposium on Security and Privacy, SP 2019, San Francisco, CA, USA, May 19-23, 2019*. IEEE, 2019, pp. 1–19. DOI: [10.1109/SP.2019.00002](https://doi.org/10.1109/SP.2019.00002).
- [88] T. Unterluggauer, M. Werner, and S. Mangard. “MEAS: memory encryption and authentication secure against side-channel attacks”. In: *J. Cryptogr. Eng.* 9.2 (2019), pp. 137–158. DOI: [10.1007/S13389-018-0180-2](https://doi.org/10.1007/S13389-018-0180-2).
- [87] S. Weiser, M. Werner, F. Brasser, M. Malenko, S. Mangard, and A. Sadeghi. “TIMBER-V: Tag-Isolated Memory Bringing Fine-grained Enclaves to RISC-V”. In: *26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019*. The Internet Society, 2019. URL: <https://www.ndss-symposium.org/ndss-paper/timber-v-tag-isolate-d-memory-bringing-fine-grained-enclaves-to-risc-v/>.
- [86] M. Werner, R. Schilling, T. Unterluggauer, and S. Mangard. “Protecting RISC-V Processors against Physical Attacks”. In: *Design, Automation & Test in Europe Conference & Exhibition, DATE 2019, Florence, Italy, March 25-29, 2019*. Ed. by J. Teich and F. Fummi. IEEE, 2019, pp. 1136–1141. DOI: [10.23919/DATE.2019.8714811](https://doi.org/10.23919/DATE.2019.8714811).
- [85] M. Werner, T. Unterluggauer, L. Giner, M. Schwarz, D. Gruss, and S. Mangard. “ScatterCache: Thwarting Cache Attacks via Cache Set Randomization”. In: *28th USENIX Security Symposium, USENIX Security 2019, Santa Clara, CA, USA, August 14-16, 2019*. Ed. by N. Heninger and P. Traynor. USENIX Association,

2019, pp. 675–692. URL: <https://www.usenix.org/conference/usenixsecurity19/presentation/werner>.

- [84] R. Bloem, H. Groß, R. Iusupov, B. Könighofer, S. Mangard, and J. Winter. “Formal Verification of Masked Hardware Implementations in the Presence of Glitches”. In: *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*. Ed. by J. B. Nielsen and V. Rijmen. Vol. 10821. Lecture Notes in Computer Science. Springer, 2018, pp. 321–353. DOI: [10.1007/978-3-319-78375-8_11](https://doi.org/10.1007/978-3-319-78375-8_11).
- [83] C. Dobraunig, M. Eichlseder, H. Groß, S. Mangard, F. Mendel, and R. Primas. “Statistical Ineffective Fault Attacks on Masked AES with Fault Countermeasures”. In: *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part II*. Ed. by T. Peyrin and S. D. Galbraith. Vol. 11273. Lecture Notes in Computer Science. Springer, 2018, pp. 315–342. DOI: [10.1007/978-3-030-03329-3_11](https://doi.org/10.1007/978-3-030-03329-3_11).
- [82] C. Dobraunig, M. Eichlseder, T. Korak, S. Mangard, F. Mendel, and R. Primas. “SIFA: Exploiting Ineffective Fault Inductions on Symmetric Cryptography”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2018.3 (2018), pp. 547–572. DOI: [10.13154/TCHES.V2018.I3.547-572](https://doi.org/10.13154/TCHES.V2018.I3.547-572).
- [81] C. Dobraunig, S. Mangard, F. Mendel, and R. Primas. “Fault Attacks on Nonce-Based Authenticated Encryption: Application to Keyak and Ketje”. In: *Selected Areas in Cryptography - SAC 2018 - 25th International Conference, Calgary, AB, Canada, August 15-17, 2018, Revised Selected Papers*. Ed. by C. Cid and M. J. J. Jr. Vol. 11349. Lecture Notes in Computer Science. Springer, 2018, pp. 257–277. DOI: [10.1007/978-3-030-10970-7_12](https://doi.org/10.1007/978-3-030-10970-7_12).
- [80] H. Groß and S. Mangard. “A unified masking approach”. In: *J. Cryptogr. Eng.* 8.2 (2018), pp. 109–124. DOI: [10.1007/S13389-018-0184-Y](https://doi.org/10.1007/S13389-018-0184-Y).
- [79] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, and M. Hamburg. “Meltdown: Reading Kernel Memory from User Space”. In: *27th USENIX Security Symposium, USENIX Security 2018, Baltimore, MD, USA, August 15-17, 2018*. Ed. by W. Enck and A. P. Felt. USENIX Association, 2018, pp. 973–990. URL: <https://www.usenix.org/conference/usenixsecurity18/presentation/lipp>.
- [78] R. Schilling, T. Unterluggauer, S. Mangard, F. K. Gürkaynak, M. Muehlberghuber, and L. Benini. “High speed ASIC implementations of leakage-resilient cryptography”. In: *2018 Design, Automation & Test in Europe Conference & Exhibition, DATE 2018, Dresden, Germany, March 19-23, 2018*. Ed. by J. Madsen and A. K. Coskun. IEEE, 2018, pp. 1259–1264. DOI: [10.23919/DATE.2018.8342208](https://doi.org/10.23919/DATE.2018.8342208).
- [77] R. Schilling, M. Werner, and S. Mangard. “Securing conditional branches in the presence of fault attacks”. In: *2018 Design, Automation & Test in Europe Conference & Exhibition, DATE 2018, Dresden, Germany, March 19-23, 2018*. Ed. by J. Madsen and A. K. Coskun. IEEE, 2018, pp. 1586–1591. DOI: [10.23919/DATE.2018.8342268](https://doi.org/10.23919/DATE.2018.8342268).

- [76] R. Schilling, M. Werner, P. Nasahl, and S. Mangard. “Pointing in the Right Direction - Securing Memory Accesses in a Faulty World”. In: *Proceedings of the 34th Annual Computer Security Applications Conference, ACSAC 2018, San Juan, PR, USA, December 03-07, 2018*. ACM, 2018, pp. 595–604. DOI: [10.1145/3274694.3274728](https://doi.org/10.1145/3274694.3274728).
- [75] M. Schwarz, D. Gruss, M. Lipp, C. Maurice, T. Schuster, A. Fogh, and S. Mangard. “Automated Detection, Exploitation, and Elimination of Double-Fetch Bugs using Modern CPU Features”. In: *Proceedings of the 2018 on Asia Conference on Computer and Communications Security, AsiaCCS 2018, Incheon, Republic of Korea, June 04-08, 2018*. Ed. by J. Kim, G. Ahn, S. Kim, Y. Kim, J. López, and T. Kim. ACM, 2018, pp. 587–600. DOI: [10.1145/3196494.3196508](https://doi.org/10.1145/3196494.3196508).
- [74] M. Schwarz, M. Lipp, D. Gruss, S. Weiser, C. Maurice, R. Spreitzer, and S. Mangard. “KeyDrown: Eliminating Software-Based Keystroke Timing Side-Channel Attacks”. In: *25th Annual Network and Distributed System Security Symposium, NDSS 2018, San Diego, California, USA, February 18-21, 2018*. The Internet Society, 2018. URL: https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018%5C_04B-1%5C_Schwarz%5C_paper.pdf.
- [73] R. Spreitzer, F. Kirchengast, D. Gruss, and S. Mangard. “ProcHarvester: Fully Automated Analysis of Procs Side-Channel Leaks on Android”. In: *Proceedings of the 2018 on Asia Conference on Computer and Communications Security, AsiaCCS 2018, Incheon, Republic of Korea, June 04-08, 2018*. Ed. by J. Kim, G. Ahn, S. Kim, Y. Kim, J. López, and T. Kim. ACM, 2018, pp. 749–763. DOI: [10.1145/3196494.3196510](https://doi.org/10.1145/3196494.3196510).
- [72] R. Spreitzer, V. Moonsamy, T. Korak, and S. Mangard. “Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices”. In: *IEEE Commun. Surv. Tutorials* 20.1 (2018), pp. 465–488. DOI: [10.1109/COMST.2017.2779824](https://doi.org/10.1109/COMST.2017.2779824).
- [71] R. Spreitzer, G. Palfinger, and S. Mangard. “SCAnDroid: Automated Side-Channel Analysis of Android APIs”. In: *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks, WiSec 2018, Stockholm, Sweden, June 18-20, 2018*. Ed. by P. Papadimitratos, K. R. B. Butler, and C. Pöpper. ACM, 2018, pp. 224–235. DOI: [10.1145/3212480.3212506](https://doi.org/10.1145/3212480.3212506).
- [70] S. Weiser, A. Zankl, R. Spreitzer, K. Miller, S. Mangard, and G. Sigl. “DATA - Differential Address Trace Analysis”. In: *28. Krypto-Tag, Kirchheim bei München, Germany, June 7-8, 2018*. Ed. by D. Loebenberger and M. Nüsken. Gesellschaft für Informatik e.V. / FG KRYPTO, 2018. DOI: [10.18420/CDM-2018-28-14](https://doi.org/10.18420/CDM-2018-28-14).
- [69] S. Weiser, A. Zankl, R. Spreitzer, K. Miller, S. Mangard, and G. Sigl. “DATA - Differential Address Trace Analysis: Finding Address-based Side-Channels in Binaries”. In: *27th USENIX Security Symposium, USENIX Security 2018, Baltimore, MD, USA, August 15-17, 2018*. Ed. by W. Enck and A. P. Felt. USENIX Association, 2018, pp. 603–620. URL: <https://www.usenix.org/conference/usenixsecurity18/presentation/weiser>.
- [68] M. Werner, T. Unterluggauer, D. Schaffenrath, and S. Mangard. “Sponge-Based Control-Flow Protection for IoT Devices”. In: *2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018, London, United Kingdom, April 24-26, 2018*. IEEE, 2018, pp. 214–226. DOI: [10.1109/EUROSP.2018.00023](https://doi.org/10.1109/EUROSP.2018.00023).

- [67] F. Conti, R. Schilling, P. D. Schiavone, A. Pullini, D. Rossi, F. K. Gürkaynak, M. Muehlberghuber, M. Gautschi, I. Loi, G. Haugou, S. Mangard, and L. Benini. “An IoT Endpoint System-on-Chip for Secure and Energy-Efficient Near-Sensor Analytics”. In: *IEEE Trans. Circuits Syst. I Regul. Pap.* 64-I.9 (2017), pp. 2481–2494. DOI: [10.1109/TCSI.2017.2698019](https://doi.org/10.1109/TCSI.2017.2698019).
- [66] C. Dobraunig, M. Eichlseder, S. Mangard, F. Mendel, and T. Unterluggauer. “ISAP - Towards Side-Channel Secure Authenticated Encryption”. In: *IACR Trans. Symmetric Cryptol.* 2017.1 (2017), pp. 80–105. DOI: [10.13154/TOSC.V2017.I1.80-105](https://doi.org/10.13154/TOSC.V2017.I1.80-105).
- [65] H. Groß and S. Mangard. “Reconciling d+1 Masking in Hardware and Software”. In: *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*. Ed. by W. Fischer and N. Homma. Vol. 10529. Lecture Notes in Computer Science. Springer, 2017, pp. 115–136. DOI: [10.1007/978-3-319-66787-4_6](https://doi.org/10.1007/978-3-319-66787-4_6).
- [64] H. Groß, S. Mangard, and T. Korak. “An Efficient Side-Channel Protected AES Implementation with Arbitrary Protection Order”. In: *Topics in Cryptology - CT-RSA 2017 - The Cryptographers’ Track at the RSA Conference 2017, San Francisco, CA, USA, February 14-17, 2017, Proceedings*. Ed. by H. Handschuh. Vol. 10159. Lecture Notes in Computer Science. Springer, 2017, pp. 95–112. DOI: [10.1007/978-3-319-52153-4_6](https://doi.org/10.1007/978-3-319-52153-4_6).
- [63] H. Groß, D. Schaffenrath, and S. Mangard. “Higher-Order Side-Channel Protected Implementations of KECCAK”. In: *Euromicro Conference on Digital System Design, DSD 2017, Vienna, Austria, August 30 - Sept. 1, 2017*. Ed. by H. Kubátová, M. Novotný, and A. Skavhaug. IEEE Computer Society, 2017, pp. 205–212. DOI: [10.1109/DSD.2017.21](https://doi.org/10.1109/DSD.2017.21).
- [62] B. Großwindhager, A. Rupp, M. Tappler, M. Tranninger, S. Weiser, B. K. Aichernig, C. A. Boano, M. Horn, G. Kubin, S. Mangard, M. Steinberger, and K. Römer. “Dependable Internet of Things for Networked Cars”. In: *Int. J. Comput.* 16 (2017), pp. 226–237. DOI: [10.47839/IJC.16.4.911](https://doi.org/10.47839/IJC.16.4.911).
- [61] D. Gruss, M. Lipp, M. Schwarz, R. Fellner, C. Maurice, and S. Mangard. “KASLR is Dead: Long Live KASLR”. In: *Engineering Secure Software and Systems - 9th International Symposium, ESSoS 2017, Bonn, Germany, July 3-5, 2017, Proceedings*. Ed. by E. Bodden, M. Payer, and E. Athanasopoulos. Vol. 10379. Lecture Notes in Computer Science. Springer, 2017, pp. 161–176. DOI: [10.1007/978-3-319-62105-0_11](https://doi.org/10.1007/978-3-319-62105-0_11).
- [60] F. K. Gürkaynak, R. Schilling, M. Muehlberghuber, F. Conti, S. Mangard, and L. Benini. “Multi-core data analytics SoC with a flexible 1.76 Gbit/s AES-XTS cryptographic accelerator in 65 nm CMOS”. In: *Proceedings of the Fourth Workshop on Cryptography and Security in Computing Systems, CS2@HiPEAC 2017, Stockholm, Sweden, January 24, 2017*. Ed. by M. Brorsson, Z. Lu, G. Agosta, A. Barengi, and G. Pelosi. ACM, 2017, pp. 19–24. DOI: [10.1145/3031836.3031840](https://doi.org/10.1145/3031836.3031840).
- [59] M. Lipp, D. Gruss, M. Schwarz, D. Bidner, C. Maurice, and S. Mangard. “Practical Keystroke Timing Attacks in Sandboxed JavaScript”. In: *Computer Security - ESORICS 2017 - 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part II*. Ed. by S. N. Foley, D. Gollmann, and E. Sneekenes. Vol. 10493. Lecture Notes in Computer Science. Springer, 2017, pp. 191–209. DOI: [10.1007/978-3-319-66399-9_11](https://doi.org/10.1007/978-3-319-66399-9_11).

- [58] C. Maurice, M. Weber, M. Schwarz, L. Giner, D. Gruss, C. A. Boano, S. Mangard, and K. Römer. “Hello from the Other Side: SSH over Robust Cache Covert Channels in the Cloud”. In: *24th Annual Network and Distributed System Security Symposium, NDSS 2017, San Diego, California, USA, February 26 - March 1, 2017*. The Internet Society, 2017. URL: <https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/hello-other-side-ssh-over-robust-cache-covert-channels-cloud/>.
- [57] R. Primas, P. Pessl, and S. Mangard. “Single-Trace Side-Channel Attacks on Masked Lattice-Based Encryption”. In: *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*. Ed. by W. Fischer and N. Homma. Vol. 10529. Lecture Notes in Computer Science. Springer, 2017, pp. 513–533. DOI: [10.1007/978-3-319-66787-4_25](https://doi.org/10.1007/978-3-319-66787-4_25).
- [56] M. Schwarz, C. Maurice, D. Gruss, and S. Mangard. “Fantastic Timers and Where to Find Them: High-Resolution Microarchitectural Attacks in JavaScript”. In: *Financial Cryptography and Data Security - 21st International Conference, FC 2017, Sliema, Malta, April 3-7, 2017, Revised Selected Papers*. Ed. by A. Kiayias. Vol. 10322. Lecture Notes in Computer Science. Springer, 2017, pp. 247–267. DOI: [10.1007/978-3-319-70972-7_13](https://doi.org/10.1007/978-3-319-70972-7_13).
- [55] M. Schwarz, S. Weiser, D. Gruss, C. Maurice, and S. Mangard. “Malware Guard Extension: Using SGX to Conceal Cache Attacks”. In: *Detection of Intrusions and Malware, and Vulnerability Assessment - 14th International Conference, DIMVA 2017, Bonn, Germany, July 6-7, 2017, Proceedings*. Ed. by M. Polychronakis and M. Meier. Vol. 10327. Lecture Notes in Computer Science. Springer, 2017, pp. 3–24. DOI: [10.1007/978-3-319-60876-1_1](https://doi.org/10.1007/978-3-319-60876-1_1).
- [54] T. Unterluggauer, T. Korak, S. Mangard, R. Schilling, L. Benini, F. K. Gürkaynak, and M. Muehlberghuber. “Leakage Bounds for Gaussian Side Channels”. In: *Smart Card Research and Advanced Applications - 16th International Conference, CARDIS 2017, Lugano, Switzerland, November 13-15, 2017, Revised Selected Papers*. Ed. by T. Eisenbarth and Y. Tegliah. Vol. 10728. Lecture Notes in Computer Science. Springer, 2017, pp. 88–104. DOI: [10.1007/978-3-319-75208-2_6](https://doi.org/10.1007/978-3-319-75208-2_6).
- [53] T. Unterluggauer, M. Werner, and S. Mangard. “Securing Memory Encryption and Authentication Against Side-Channel Attacks Using Unprotected Primitives”. In: *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, AsiaCCS 2017, Abu Dhabi, United Arab Emirates, April 2-6, 2017*. Ed. by R. Karri, O. Sinanoglu, A. Sadeghi, and X. Yi. ACM, 2017, pp. 690–702. DOI: [10.1145/3052973.3052985](https://doi.org/10.1145/3052973.3052985).
- [52] T. Unterluggauer, M. Werner, and S. Mangard. “Side-channel plaintext-recovery attacks on leakage-resilient encryption”. In: *Design, Automation & Test in Europe Conference & Exhibition, DATE 2017, Lausanne, Switzerland, March 27-31, 2017*. Ed. by D. Atienza and G. D. Natale. IEEE, 2017, pp. 1318–1323. DOI: [10.23919/DATE.2017.7927197](https://doi.org/10.23919/DATE.2017.7927197).
- [51] M. Werner, T. Unterluggauer, R. Schilling, D. Schaffenrath, and S. Mangard. “Transparent memory encryption and authentication”. In: *27th International Conference on Field Programmable Logic and Applications, FPL 2017, Ghent, Belgium, September 4-8, 2017*. Ed. by M. D. Santambrogio, D. Göhringer, D. Stroobandt, N. Mentens, and J. Nurmi. IEEE, 2017, pp. 1–6. DOI: [10.23919/FPL.2017.8056797](https://doi.org/10.23919/FPL.2017.8056797).

- [50] H. Groß, M. Jelinek, S. Mangard, T. Unterluggauer, and M. Werner. “Concealing Secrets in Embedded Processors Designs”. In: *Smart Card Research and Advanced Applications - 15th International Conference, CARDIS 2016, Cannes, France, November 7-9, 2016, Revised Selected Papers*. Ed. by K. Lemke-Rust and M. Tunstall. Vol. 10146. Lecture Notes in Computer Science. Springer, 2016, pp. 89–104. DOI: [10.1007/978-3-319-54669-8_6](https://doi.org/10.1007/978-3-319-54669-8_6).
- [49] H. Groß, S. Mangard, and T. Korak. “Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order”. In: *Proceedings of the ACM Workshop on Theory of Implementation Security, TIS@CCS 2016 Vienna, Austria, October, 2016*. Ed. by B. Bilgin, S. Nikova, and V. Rijmen. ACM, 2016, p. 3. DOI: [10.1145/2996366.2996426](https://doi.org/10.1145/2996366.2996426).
- [48] D. Gruss, C. Maurice, A. Fogh, M. Lipp, and S. Mangard. “Prefetch Side-Channel Attacks: Bypassing SMAP and Kernel ASLR”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*. Ed. by E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi. ACM, 2016, pp. 368–379. DOI: [10.1145/2976749.2978356](https://doi.org/10.1145/2976749.2978356).
- [47] D. Gruss, C. Maurice, and S. Mangard. “Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript”. In: *Detection of Intrusions and Malware, and Vulnerability Assessment - 13th International Conference, DIMVA 2016, San Sebastián, Spain, July 7-8, 2016, Proceedings*. Ed. by J. Caballero, U. Zurutuza, and R. J. Rodríguez. Vol. 9721. Lecture Notes in Computer Science. Springer, 2016, pp. 300–321. DOI: [10.1007/978-3-319-40667-1_15](https://doi.org/10.1007/978-3-319-40667-1_15).
- [46] D. Gruss, C. Maurice, K. Wagner, and S. Mangard. “Flush+Flush: A Fast and Stealthy Cache Attack”. In: *Detection of Intrusions and Malware, and Vulnerability Assessment - 13th International Conference, DIMVA 2016, San Sebastián, Spain, July 7-8, 2016, Proceedings*. Ed. by J. Caballero, U. Zurutuza, and R. J. Rodríguez. Vol. 9721. Lecture Notes in Computer Science. Springer, 2016, pp. 279–299. DOI: [10.1007/978-3-319-40667-1_14](https://doi.org/10.1007/978-3-319-40667-1_14).
- [45] M. Lipp, D. Gruss, R. Spreitzer, C. Maurice, and S. Mangard. “ARMageddon: Cache Attacks on Mobile Devices”. In: *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016*. Ed. by T. Holz and S. Savage. USENIX Association, 2016, pp. 549–564. URL: <https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/lipp>.
- [44] P. Pessl, D. Gruss, C. Maurice, M. Schwarz, and S. Mangard. “DRAMA: Exploiting DRAM Addressing for Cross-CPU Attacks”. In: *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016*. Ed. by T. Holz and S. Savage. USENIX Association, 2016, pp. 565–581. URL: <https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/pessl>.
- [43] P. Pessl and S. Mangard. “Enhancing Side-Channel Analysis of Binary-Field Multiplication with Bit Reliability”. In: *Topics in Cryptology - CT-RSA 2016 - The Cryptographers’ Track at the RSA Conference 2016, San Francisco, CA, USA, February 29 - March 4, 2016, Proceedings*. Ed. by K. Sako. Vol. 9610. Lecture Notes in Computer Science. Springer, 2016, pp. 255–270. DOI: [10.1007/978-3-319-29485-8_15](https://doi.org/10.1007/978-3-319-29485-8_15).
- [42] R. Spreitzer, S. Griesmayr, T. Korak, and S. Mangard. “Exploiting Data-Usage Statistics for Website Fingerprinting Attacks on Android”. In: *Proceedings of the 9th ACM Conference on Security & Privacy in*

Wireless and Mobile Networks, WISEC 2016, Darmstadt, Germany, July 18-22, 2016. Ed. by M. Hollick, P. Papadimitratos, and W. Enck. ACM, 2016, pp. 49–60. DOI: [10.1145/2939918.2939922](https://doi.org/10.1145/2939918.2939922).

- [41] T. Unterluggauer and S. Mangard. “Exploiting the Physical Disparity: Side-Channel Attacks on Memory Encryption”. In: *Constructive Side-Channel Analysis and Secure Design - 7th International Workshop, COSADE 2016, Graz, Austria, April 14-15, 2016, Revised Selected Papers*. Ed. by F. Standaert and E. Oswald. Vol. 9689. Lecture Notes in Computer Science. Springer, 2016, pp. 3–18. DOI: [10.1007/978-3-319-43283-0_1](https://doi.org/10.1007/978-3-319-43283-0_1).
- [40] C. Dobraunig, F. Koeune, S. Mangard, F. Mendel, and F. Standaert. “Towards Fresh and Hybrid Re-Keying Schemes with Beyond Birthday Security”. In: *Smart Card Research and Advanced Applications - 14th International Conference, CARDIS 2015, Bochum, Germany, November 4-6, 2015. Revised Selected Papers*. Ed. by N. Homma and M. Medwed. Vol. 9514. Lecture Notes in Computer Science. Springer, 2015, pp. 225–241. DOI: [10.1007/978-3-319-31271-2_14](https://doi.org/10.1007/978-3-319-31271-2_14).
- [39] D. Gruss, D. Bidner, and S. Mangard. “Practical Memory Deduplication Attacks in Sandboxed Javascript”. In: *Computer Security - ESORICS 2015 - 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part I*. Ed. by G. Pernul, P. Y. A. Ryan, and E. R. Weippl. Vol. 9326. Lecture Notes in Computer Science. Springer, 2015, pp. 108–122. DOI: [10.1007/978-3-319-24174-6_6](https://doi.org/10.1007/978-3-319-24174-6_6).
- [38] D. Gruss, R. Spreitzer, and S. Mangard. “Cache Template Attacks: Automating Attacks on Inclusive Last-Level Caches”. In: *24th USENIX Security Symposium, USENIX Security 15, Washington, D.C., USA, August 12-14, 2015*. Ed. by J. Jung and T. Holz. USENIX Association, 2015, pp. 897–912. URL: <https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/gruss>.
- [37] S. Mangard. “Fault Attacks at the System Level - The Challenge of Securing Application Software”. In: *2015 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2015, Saint Malo, France, September 13, 2015*. Ed. by N. Homma and V. Lomné. IEEE Computer Society, 2015, p. 1. DOI: [10.1109/FDTC.2015.23](https://doi.org/10.1109/FDTC.2015.23).
- [36] M. Werner, E. Wenger, and S. Mangard. “Protecting the Control Flow of Embedded Processors against Fault Attacks”. In: *Smart Card Research and Advanced Applications - 14th International Conference, CARDIS 2015, Bochum, Germany, November 4-6, 2015. Revised Selected Papers*. Ed. by N. Homma and M. Medwed. Vol. 9514. Lecture Notes in Computer Science. Springer, 2015, pp. 161–176. DOI: [10.1007/978-3-319-31271-2_10](https://doi.org/10.1007/978-3-319-31271-2_10).
- [35] S. Belaïd, F. D. Santis, J. Heyszl, S. Mangard, M. Medwed, J. Schmidt, F. Standaert, and S. Tillich. “Towards fresh re-keying with leakage-resilient PRFs: cipher design principles and analysis”. In: *J. Cryptogr. Eng.* 4.3 (2014), pp. 157–171. DOI: [10.1007/S13389-014-0079-5](https://doi.org/10.1007/S13389-014-0079-5).
- [34] C. Dobraunig, M. Eichlseder, S. Mangard, and F. Mendel. “On the Security of Fresh Re-keying to Counteract Side-Channel and Fault Attacks”. In: *Smart Card Research and Advanced Applications - 13th International Conference, CARDIS 2014, Paris, France, November 5-7, 2014. Revised Selected Papers*. Ed. by M. Joye

- and A. Moradi. Vol. 8968. Lecture Notes in Computer Science. Springer, 2014, pp. 233–244. DOI: [10.1007/978-3-319-16763-3_14](https://doi.org/10.1007/978-3-319-16763-3_14).
- [33] J. Heyszl, A. Ibing, S. Mangard, F. D. Santis, and G. Sigl. “Clustering Algorithms for Non-profiled Single-Execution Attacks on Exponentiations”. In: *Smart Card Research and Advanced Applications - 12th International Conference, CARDIS 2013, Berlin, Germany, November 27-29, 2013. Revised Selected Papers*. Ed. by A. Francillon and P. Rohatgi. Vol. 8419. Lecture Notes in Computer Science. Springer, 2013, pp. 79–93. DOI: [10.1007/978-3-319-08302-5_6](https://doi.org/10.1007/978-3-319-08302-5_6).
 - [32] S. Mangard. “Keeping Secrets on Low-Cost Chips”. In: *IEEE Secur. Priv.* 11.4 (2013), pp. 75–77. DOI: [10.1109/MSP.2013.88](https://doi.org/10.1109/MSP.2013.88).
 - [31] F. D. Santis, M. Kasper, S. Mangard, G. Sigl, O. Stein, and M. Stöttinger. “On the Relationship between Correlation Power Analysis and the Stochastic Approach: An ASIC Designer Perspective”. In: *Progress in Cryptology - INDOCRYPT 2013 - 14th International Conference on Cryptology in India, Mumbai, India, December 7-10, 2013. Proceedings*. Ed. by G. Paul and S. Vaudenay. Vol. 8250. Lecture Notes in Computer Science. Springer, 2013, pp. 215–226. DOI: [10.1007/978-3-319-03515-4_14](https://doi.org/10.1007/978-3-319-03515-4_14).
 - [30] J. Heyszl, S. Mangard, B. Heinz, F. Stumpf, and G. Sigl. “Localized Electromagnetic Analysis of Cryptographic Implementations”. In: *Topics in Cryptology - CT-RSA 2012 - The Cryptographers’ Track at the RSA Conference 2012, San Francisco, CA, USA, February 27 - March 2, 2012. Proceedings*. Ed. by O. Dunkelman. Vol. 7178. Lecture Notes in Computer Science. Springer, 2012, pp. 231–244. DOI: [10.1007/978-3-642-27954-6_15](https://doi.org/10.1007/978-3-642-27954-6_15).
 - [29] M. Hutter, M. Kirschbaum, T. Plos, J. Schmidt, and S. Mangard. “Exploiting the Difference of Side-Channel Leakages”. In: *Constructive Side-Channel Analysis and Secure Design - Third International Workshop, COSADE 2012, Darmstadt, Germany, May 3-4, 2012. Proceedings*. Ed. by W. Schindler and S. A. Huss. Vol. 7275. Lecture Notes in Computer Science. Springer, 2012, pp. 1–16. DOI: [10.1007/978-3-642-29912-4_1](https://doi.org/10.1007/978-3-642-29912-4_1).
 - [28] S. Mangard. “Die physikalische Sicherheit eingebetteter Systeme”. In: *Datenschutz und Datensicherheit* 36.12 (2012), pp. 867–871. DOI: [10.1007/S11623-012-0292-2](https://doi.org/10.1007/S11623-012-0292-2).
 - [27] S. Mangard, E. Oswald, and F. Standaert. “One for all - all for one: unifying standard differential power analysis attacks”. In: *IET Inf. Secur.* 5.2 (2011), pp. 100–110. DOI: [10.1049/IET-IFS.2010.0096](https://doi.org/10.1049/IET-IFS.2010.0096).
 - [26] M. Medwed and S. Mangard. “Arithmetic logic units with high error detection rates to counteract fault attacks”. In: *Design, Automation and Test in Europe, DATE 2011, Grenoble, France, March 14-18, 2011*. IEEE, 2011, pp. 1644–1649. DOI: [10.1109/DATE.2011.5763261](https://doi.org/10.1109/DATE.2011.5763261).
 - [25] B. M. Gammel and S. Mangard. “On the Duality of Probing and Fault Attacks”. In: *J. Electron. Test.* 26.4 (2010), pp. 483–493. DOI: [10.1007/S10836-010-5160-0](https://doi.org/10.1007/S10836-010-5160-0).
 - [24] F. Standaert, N. Veyrat-Charvillon, E. Oswald, B. Gierlichs, M. Medwed, M. Kasper, and S. Mangard. “The World Is Not Enough: Another Look on Second-Order DPA”. In: *Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Secu-*

- ity, Singapore, December 5-9, 2010. *Proceedings*. Ed. by M. Abe. Vol. 6477. Lecture Notes in Computer Science. Springer, 2010, pp. 112–129. DOI: [10.1007/978-3-642-17373-8_7](https://doi.org/10.1007/978-3-642-17373-8_7).
- [23] T. Popp, M. Kirschbaum, and S. Mangard. “Practical Attacks on Masked Hardware”. In: *Topics in Cryptology - CT-RSA 2009, The Cryptographers’ Track at the RSA Conference 2009, San Francisco, CA, USA, April 20-24, 2009. Proceedings*. Ed. by M. Fischlin. Vol. 5473. Lecture Notes in Computer Science. Springer, 2009, pp. 211–225. DOI: [10.1007/978-3-642-00862-7_14](https://doi.org/10.1007/978-3-642-00862-7_14).
- [22] M. Hutter, S. Mangard, and M. Feldhofer. “Power and EM Attacks on Passive 13.56 MHz RFID Devices”. In: *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*. Ed. by P. Paillier and I. Verbauwhede. Vol. 4727. Lecture Notes in Computer Science. Springer, 2007, pp. 320–333. DOI: [10.1007/978-3-540-74735-2_22](https://doi.org/10.1007/978-3-540-74735-2_22).
- [21] E. Oswald and S. Mangard. “Template Attacks on Masking - Resistance Is Futile”. In: *Topics in Cryptology - CT-RSA 2007, The Cryptographers’ Track at the RSA Conference 2007, San Francisco, CA, USA, February 5-9, 2007, Proceedings*. Ed. by M. Abe. Vol. 4377. Lecture Notes in Computer Science. Springer, 2007, pp. 243–256. DOI: [10.1007/11967668_16](https://doi.org/10.1007/11967668_16).
- [20] T. Popp, M. Kirschbaum, T. Zeffere, and S. Mangard. “Evaluation of the Masked Logic Style MDPL on a Prototype Chip”. In: *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*. Ed. by P. Paillier and I. Verbauwhede. Vol. 4727. Lecture Notes in Computer Science. Springer, 2007, pp. 81–94. DOI: [10.1007/978-3-540-74735-2_6](https://doi.org/10.1007/978-3-540-74735-2_6).
- [19] T. Popp, S. Mangard, and E. Oswald. “Power Analysis Attacks and Countermeasures”. In: *IEEE Des. Test Comput.* 24.6 (2007), pp. 535–543. DOI: [10.1109/MDT.2007.200](https://doi.org/10.1109/MDT.2007.200).
- [18] S. Ravi and S. Mangard. “Tutorial T1: Designing Secure SoCs”. In: *20th International Conference on VLSI Design (VLSI Design 2007), Sixth International Conference on Embedded Systems (ICES 2007), 6-10 January 2007, Bangalore, India*. IEEE Computer Society, 2007, p. 3. DOI: [10.1109/VLSID.2007.165](https://doi.org/10.1109/VLSID.2007.165).
- [17] S. Tillich, C. Herbst, and S. Mangard. “Protecting AES Software Implementations on 32-Bit Processors Against Power Analysis”. In: *Applied Cryptography and Network Security, 5th International Conference, ACNS 2007, Zhuhai, China, June 5-8, 2007, Proceedings*. Ed. by J. Katz and M. Yung. Vol. 4521. Lecture Notes in Computer Science. Springer, 2007, pp. 141–157. DOI: [10.1007/978-3-540-72738-5_10](https://doi.org/10.1007/978-3-540-72738-5_10).
- [16] M. J. Aigner, S. Mangard, F. Menichelli, R. Menicocci, M. Olivieri, T. Popp, G. Scotti, and A. Trifiletti. “Side channel analysis resistant design flow”. In: *International Symposium on Circuits and Systems (ISCAS 2006), 21-24 May 2006, Island of Kos, Greece*. IEEE, 2006. DOI: [10.1109/ISCAS.2006.1693233](https://doi.org/10.1109/ISCAS.2006.1693233).
- [15] C. Herbst, E. Oswald, and S. Mangard. “An AES Smart Card Implementation Resistant to Power Analysis Attacks”. In: *Applied Cryptography and Network Security, 4th International Conference, ACNS 2006, Singapore, June 6-9, 2006, Proceedings*. Ed. by J. Zhou, M. Yung, and F. Bao. Vol. 3989. Lecture Notes in Computer Science. Springer, 2006, pp. 239–252. DOI: [10.1007/11767480_16](https://doi.org/10.1007/11767480_16).
- [14] S. Mangard and K. Schramm. “Pinpointing the Side-Channel Leakage of Masked AES Hardware Implementations”. In: *Cryptographic Hardware and Embedded Systems - CHES 2006, 8th International Workshop,*

- Yokohama, Japan, October 10-13, 2006, Proceedings*. Ed. by L. Goubin and M. Matsui. Vol. 4249. Lecture Notes in Computer Science. Springer, 2006, pp. 76–90. DOI: [10.1007/11894063_7](https://doi.org/10.1007/11894063_7).
- [13] E. Oswald, S. Mangard, C. Herbst, and S. Tillich. “Practical Second-Order DPA Attacks for Masked Smart Card Implementations of Block Ciphers”. In: *Topics in Cryptology - CT-RSA 2006, The Cryptographers’ Track at the RSA Conference 2006, San Jose, CA, USA, February 13-17, 2006, Proceedings*. Ed. by D. Pointcheval. Vol. 3860. Lecture Notes in Computer Science. Springer, 2006, pp. 192–207. DOI: [10.1007/11605805_13](https://doi.org/10.1007/11605805_13).
 - [12] T. Popp and S. Mangard. “Implementation aspects of the DPA-resistant logic style MDPL”. In: *International Symposium on Circuits and Systems (ISCAS 2006), 21-24 May 2006, Island of Kos, Greece*. IEEE, 2006. DOI: [10.1109/ISCAS.2006.1693234](https://doi.org/10.1109/ISCAS.2006.1693234).
 - [11] H. Yoo, C. Herbst, S. Mangard, E. Oswald, and S. Moon. “Investigations of Power Analysis Attacks and Countermeasures for ARIA”. In: *Information Security Applications, 7th International Workshop, WISA 2006, Jeju Island, Korea, August 28-30, 2006, Revised Selected Papers*. Ed. by J. Lee, O. Yi, and M. Yung. Vol. 4298. Lecture Notes in Computer Science. Springer, 2006, pp. 160–172. DOI: [10.1007/978-3-540-71093-6_13](https://doi.org/10.1007/978-3-540-71093-6_13).
 - [10] M. J. Aigner, S. Mangard, R. Menicocci, M. Olivieri, G. Scotti, and A. Trifiletti. “A novel CMOS logic style with data independent power consumption”. In: *International Symposium on Circuits and Systems (ISCAS 2005), 23-26 May 2005, Kobe, Japan*. IEEE, 2005, pp. 1066–1069. DOI: [10.1109/ISCAS.2005.1464776](https://doi.org/10.1109/ISCAS.2005.1464776).
 - [9] S. Mangard, T. Popp, and B. M. Gammel. “Side-Channel Leakage of Masked CMOS Gates”. In: *Topics in Cryptology - CT-RSA 2005, The Cryptographers’ Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005, Proceedings*. Ed. by A. Menezes. Vol. 3376. Lecture Notes in Computer Science. Springer, 2005, pp. 351–365. DOI: [10.1007/978-3-540-30574-3_24](https://doi.org/10.1007/978-3-540-30574-3_24).
 - [8] S. Mangard, N. Pramstaller, and E. Oswald. “Successfully Attacking Masked AES Hardware Implementations”. In: *Cryptographic Hardware and Embedded Systems - CHES 2005, 7th International Workshop, Edinburgh, UK, August 29 - September 1, 2005, Proceedings*. Ed. by J. R. Rao and B. Sunar. Vol. 3659. Lecture Notes in Computer Science. Springer, 2005, pp. 157–171. DOI: [10.1007/11545262_12](https://doi.org/10.1007/11545262_12).
 - [7] E. Oswald, S. Mangard, N. Pramstaller, and V. Rijmen. “A Side-Channel Analysis Resistant Description of the AES S-Box”. In: *Fast Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers*. Ed. by H. Gilbert and H. Handschuh. Vol. 3557. Lecture Notes in Computer Science. Springer, 2005, pp. 413–423. DOI: [10.1007/11502760_28](https://doi.org/10.1007/11502760_28).
 - [6] T. Popp and S. Mangard. “Masked Dual-Rail Pre-charge Logic: DPA-Resistance Without Routing Constraints”. In: *Cryptographic Hardware and Embedded Systems - CHES 2005, 7th International Workshop, Edinburgh, UK, August 29 - September 1, 2005, Proceedings*. Ed. by J. R. Rao and B. Sunar. Vol. 3659. Lecture Notes in Computer Science. Springer, 2005, pp. 172–186. DOI: [10.1007/11545262_13](https://doi.org/10.1007/11545262_13).
 - [5] S. Mangard. “Hardware Countermeasures against DPA ? A Statistical Analysis of Their Effectiveness”. In: *Topics in Cryptology - CT-RSA 2004, The Cryptographers’ Track at the RSA Conference 2004, San*

Francisco, CA, USA, February 23-27, 2004, *Proceedings*. Ed. by T. Okamoto. Vol. 2964. Lecture Notes in Computer Science. Springer, 2004, pp. 222–235. DOI: [10.1007/978-3-540-24660-2_18](https://doi.org/10.1007/978-3-540-24660-2_18).

- [4] N. Pramstaller, S. Mangard, S. Dominikus, and J. Wolkerstorfer. “Efficient AES Implementations on ASICs and FPGAs”. In: *Advanced Encryption Standard - AES, 4th International Conference, AES 2004, Bonn, Germany, May 10-12, 2004, Revised Selected and Invited Papers*. Ed. by H. Dobbertin, V. Rijmen, and A. Sowa. Vol. 3373. Lecture Notes in Computer Science. Springer, 2004, pp. 98–112. DOI: [10.1007/11506447_9](https://doi.org/10.1007/11506447_9).
- [3] S. Mangard, M. J. Aigner, and S. Dominikus. “A Highly Regular and Scalable AES Hardware Architecture”. In: *IEEE Trans. Computers* 52.4 (2003), pp. 483–491. DOI: [10.1109/TC.2003.1190589](https://doi.org/10.1109/TC.2003.1190589).
- [2] S. Mangard. “A Simple Power-Analysis (SPA) Attack on Implementations of the AES Key Expansion”. In: *Information Security and Cryptology - ICISC 2002, 5th International Conference Seoul, Korea, November 28-29, 2002, Revised Papers*. Ed. by P. J. Lee and C. H. Lim. Vol. 2587. Lecture Notes in Computer Science. Springer, 2002, pp. 343–358. DOI: [10.1007/3-540-36552-4_24](https://doi.org/10.1007/3-540-36552-4_24).
- [1] G. Ateniese and S. Mangard. “A new approach to DNS security (DNSSEC)”. In: *CCS 2001, Proceedings of the 8th ACM Conference on Computer and Communications Security, Philadelphia, Pennsylvania, USA, November 6-8, 2001*. Ed. by M. K. Reiter and P. Samarati. ACM, 2001, pp. 86–95. DOI: [10.1145/501983.501996](https://doi.org/10.1145/501983.501996).

Editorships

- [8] M. Tempelmeier, F. D. Santis, S. Bhasin, and S. Mangard. “Special Issue on Open Hardware for Embedded System Security and Cryptography”. In: *ACM Trans. Embed. Comput. Syst.* 24.5 (2025), 64:1–64:3. DOI: [10.1145/3747326](https://doi.org/10.1145/3747326).
- [7] E. R. Weippl, S. Katzenbeisser, M. Payer, S. Mangard, E. Androulaki, and M. K. Reiter, eds. *Proceedings of the 2016 ACM on Cloud Computing Security Workshop, CCSW 2016, Vienna, Austria, October 28, 2016*. ACM, 2016. DOI: [10.1145/2996429](https://doi.org/10.1145/2996429).
- [6] E. R. Weippl, S. Katzenbeisser, M. Payer, S. Mangard, A. A. Cárdenas, and R. B. Bobba, eds. *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy, CPS-SPC@CCS 2016, Vienna, Austria, October 28, 2016*. ACM, 2016. DOI: [10.1145/2994487](https://doi.org/10.1145/2994487).
- [5] E. R. Weippl, S. Katzenbeisser, M. Payer, S. Mangard, X. Fan, and T. Güneysu, eds. *Proceedings of the 6th International Workshop on Trustworthy Embedded Devices, TrustED@CCS 16, Vienna, Austria, October 28, 2016*. ACM, 2016. DOI: [10.1145/2995289](https://doi.org/10.1145/2995289).
- [4] S. Mangard and A. Y. Poschmann, eds. *Constructive Side-Channel Analysis and Secure Design - 6th International Workshop, COSADE 2015, Berlin, Germany, April 13-14, 2015. Revised Selected Papers*. Vol. 9064. Lecture Notes in Computer Science. Springer, 2015. DOI: [10.1007/978-3-319-21476-4](https://doi.org/10.1007/978-3-319-21476-4).
- [3] S. Mangard and P. Schaumont, eds. *Radio Frequency Identification. Security and Privacy Issues - 11th International Workshop, RFIDsec 2015, New York, NY, USA, June 23-24, 2015, Revised Selected Papers*. Vol. 9440. Lecture Notes in Computer Science. Springer, 2015. DOI: [10.1007/978-3-319-24837-0](https://doi.org/10.1007/978-3-319-24837-0).

- [2] S. Mangard, ed. *Smart Card Research and Advanced Applications - 11th International Conference, CARDIS 2012, Graz, Austria, November 28-30, 2012, Revised Selected Papers*. Vol. 7771. Lecture Notes in Computer Science. Springer, 2013. DOI: [10.1007/978-3-642-37288-9](https://doi.org/10.1007/978-3-642-37288-9).
- [1] S. Mangard and F. Standaert, eds. *Cryptographic Hardware and Embedded Systems, CHES 2010, 12th International Workshop, Santa Barbara, CA, USA, August 17-20, 2010. Proceedings*. Vol. 6225. Lecture Notes in Computer Science. Springer, 2010. DOI: [10.1007/978-3-642-15031-9](https://doi.org/10.1007/978-3-642-15031-9).

Books and Book Chapters

- [2] E. Oswald and S. Mangard. “Counteracting Power Analysis Attacks by Masking”. In: *Secure Integrated Circuits and Systems*. Ed. by I. M. R. Verbauwhede. Integrated Circuits and Systems. Springer, 2010, pp. 159–178. DOI: [10.1007/978-0-387-71829-3_9](https://doi.org/10.1007/978-0-387-71829-3_9).
- [1] S. Mangard, E. Oswald, and T. Popp. *Power Analysis Attacks - Revealing the Secrets of Smart Cards*. Springer, 2007. URL: <https://link.springer.com/book/10.1007/978-0-387-38162-6>.

Patents

- [11] B. Gammel, S. Mangard, and S. Sonnekalb. “Program-instruction-controlled instruction flow supervision”. Patent US 10,867,028 B2. Infineon Technologies AG. Filed 2019-11-08, priority date 2011-03-07. Dec. 2020. URL: [https://ppubs.uspto.gov/pubwebapp/external.html?q=\(10867028\).pn](https://ppubs.uspto.gov/pubwebapp/external.html?q=(10867028).pn).
- [10] B. Gammel, S. Mangard, and S. Sonnekalb. “Apparatus and method for detecting integrity violation”. Patent US 10,514,892 B2. Infineon Technologies AG. Filed 2013-07-26, priority date 2013-07-26. Dec. 2019. URL: [https://ppubs.uspto.gov/pubwebapp/external.html?q=\(10514892\).pn](https://ppubs.uspto.gov/pubwebapp/external.html?q=(10514892).pn).
- [9] B. Gammel, T. Felicijan, S. Mangard, and W. Mergler. “Randomized memory access”. Patent US 9,916,261 B2. Infineon Technologies AG. Filed 2014-05-19, priority date 2014-05-19. Mar. 2018. URL: [https://ppubs.uspto.gov/pubwebapp/external.html?q=\(9916261\).pn](https://ppubs.uspto.gov/pubwebapp/external.html?q=(9916261).pn).
- [8] B. Gammel and S. Mangard. “Signature update by code transformation”. Patent FR 2973130 B1. Infineon Technologies AG. Filed 2012-03-16, priority date 2011-03-23. Apr. 2018. URL: <https://worldwide.espacenet.com/patent/search?q=pn%3DFR2973130>.
- [7] B. Gammel, W. Fischer, and S. Mangard. “Generating a session key for authentication and secure data transfer”. Patent US 9,509,508 B2. Infineon Technologies AG. Filed 2013-11-07, priority date 2009-06-10. Nov. 2016. URL: [https://ppubs.uspto.gov/pubwebapp/external.html?q=\(9509508\).pn](https://ppubs.uspto.gov/pubwebapp/external.html?q=(9509508).pn).
- [6] B. Gammel and S. Mangard. “Method and device for processing data”. Patent FR 2991071 B1. Infineon Technologies AG. Filed 2013-05-17, priority date 2012-05-22. May 2016. URL: <https://worldwide.espacenet.com/patent/search?q=pn%3DFR2991071>.

- [5] B. Gammel, T. Felicijan, and S. Mangard. “Computational system”. Patent US 9,195,857 B2. Infineon Technologies AG. Filed 2013-09-30, priority date 2013-09-30. Nov. 2015. URL: [https://ppubs.uspto.gov/pubwebapp/external.html?q=\(9195857\).pn](https://ppubs.uspto.gov/pubwebapp/external.html?q=(9195857).pn).
- [4] B. Gammel and S. Mangard. “Masked nonlinear feedback shift register”. Patent US 8,983,068 B2. Infineon Technologies AG. Filed 2013-03-06, priority date 2013-03-06. Mar. 2015. URL: [https://ppubs.uspto.gov/pubwebapp/external.html?q=\(8983068\).pn](https://ppubs.uspto.gov/pubwebapp/external.html?q=(8983068).pn).
- [3] S. Sonneckal and S. Mangard. “Apparatus comprising a pair of an alarm condition generator and an associated alarm sensor”. Patent US 8,981,932 B2. Infineon Technologies AG. Filed 2013-04-15, priority date 2013-04-15. Mar. 2015. URL: [https://ppubs.uspto.gov/pubwebapp/external.html?q=\(8981932\).pn](https://ppubs.uspto.gov/pubwebapp/external.html?q=(8981932).pn).
- [2] S. Mangard. “Instruction encryption/decryption arrangement and method with iterative encryption/decryption key update”. Patent US 8,745,408 B2. Infineon Technologies AG. Filed 2011-04-08, priority date 2011-04-08. June 2014. URL: [https://ppubs.uspto.gov/pubwebapp/external.html?q=\(8745408\).pn](https://ppubs.uspto.gov/pubwebapp/external.html?q=(8745408).pn).
- [1] S. Mangard, B. Gammel, and J. Duve. “Distributed compiling process with instruction signature support”. Patent US 8,694,977 B2. Infineon Technologies AG. Filed 2011-07-15, priority date 2011-07-15. Apr. 2014. URL: [https://ppubs.uspto.gov/pubwebapp/external.html?q=\(8694977\).pn](https://ppubs.uspto.gov/pubwebapp/external.html?q=(8694977).pn).

Preprints and Other Publications

- [61] E. Andreeva, S. Mangard, R. Nagpal, A. Roy, and S. Trevisani. “Power Analysis and Countermeasures on the MiMC Block Cipher”. In: *IACR Cryptol. ePrint Arch.* 2026 (2026), p. 1562. URL: <https://eprint.iacr.org/2026/1562>.
- [60] R. Nagpal, V. Hadzic, R. Primas, and S. Mangard. “Efficient SPA Countermeasures using Redundant Number Representation with Application to ML-KEM”. In: *IACR Cryptol. ePrint Arch.* 2025 (2025), p. 679. URL: <https://eprint.iacr.org/2025/679>.
- [59] T. Wedenig, R. Nagpal, G. Cassiers, S. Mangard, and R. Peharz. “Exact Soft Analytical Side-Channel Attacks using Tractable Circuits”. In: *CoRR* abs/2501.13748 (2025). DOI: [10.48550/ARXIV.2501.13748](https://doi.org/10.48550/ARXIV.2501.13748).
- [58] S. Tolle, V. Hadzic, P. Nasahl, M. Asavae, R. Bloem, D. Couroussé, K. Heydemann, M. Jan, and S. Mangard. “Fault-Resistant Partitioning of Secure CPUs for System Co-Verification against Faults”. In: *IACR Cryptol. ePrint Arch.* 2024 (2024), p. 247. URL: <https://eprint.iacr.org/2024/247>.
- [57] M. Unterguggenberger, L. Lamster, D. Schrammel, M. Schwarzl, and S. Mangard. “TME-Box: Scalable In-Process Isolation through Intel TME-MK Memory Encryption”. In: *CoRR* abs/2407.10740 (2024). DOI: [10.48550/ARXIV.2407.10740](https://doi.org/10.48550/ARXIV.2407.10740).
- [56] G. Cassiers, B. Gigerl, S. Mangard, C. Momin, and R. Nagpal. “Compress: Reducing Area and Latency of Masked Pipelined Circuits”. In: *IACR Cryptol. ePrint Arch.* 2023 (2023), p. 1600. URL: <https://eprint.iacr.org/2023/1600>.

- [55] B. Gigerl, R. Primas, and S. Mangard. “Secure Context Switching of Masked Software Implementations”. In: *IACR Cryptol. ePrint Arch.* 2023 (2023), p. 677. URL: <https://eprint.iacr.org/2023/677>.
- [54] P. Nasahl and S. Mangard. “SCRAMBLE-CFI: Mitigating Fault-Induced Control-Flow Attacks on OpenTitan”. In: *CoRR* abs/2303.03711 (2023). DOI: [10.48550/ARXIV.2303.03711](https://doi.org/10.48550/ARXIV.2303.03711).
- [53] P. Nasahl, S. Sultana, H. Liljestrand, K. Grewal, M. LeMay, D. M. Durham, D. Schrammel, and S. Mangard. “EC-CFI: Control-Flow Integrity via Code Encryption Counteracting Fault Attacks”. In: *CoRR* abs/2301.13760 (2023). DOI: [10.48550/ARXIV.2301.13760](https://doi.org/10.48550/ARXIV.2301.13760).
- [52] R. Schilling, P. Nasahl, M. Unterguggenberger, and S. Mangard. “SFP: Providing System Call Flow Protection against Software and Fault Attacks”. In: *CoRR* abs/2301.02915 (2023). DOI: [10.48550/ARXIV.2301.02915](https://doi.org/10.48550/ARXIV.2301.02915).
- [51] R. Bloem, B. Gigerl, M. Gourjon, V. Hadzic, S. Mangard, and R. Primas. “Power Contracts: Provably Complete Power Leakage Models for Processors”. In: *IACR Cryptol. ePrint Arch.* 2022 (2022), p. 565. URL: <https://eprint.iacr.org/2022/565>.
- [50] B. Gigerl, R. Primas, and S. Mangard. “Formal Verification of Arithmetic Masking in Hardware and Software”. In: *IACR Cryptol. ePrint Arch.* 2022 (2022), p. 849. URL: <https://eprint.iacr.org/2022/849>.
- [49] R. Nagpal, B. Gigerl, R. Primas, and S. Mangard. “Riding the Waves Towards Generic Single-Cycle Masking in Hardware”. In: *IACR Cryptol. ePrint Arch.* 2022 (2022), p. 505. URL: <https://eprint.iacr.org/2022/505>.
- [48] P. Nasahl, M. Osorio, P. Vogel, M. Schaffner, T. Trippel, D. Rizzo, and S. Mangard. “SYNFI: Pre-Silicon Fault Analysis of an Open-Source Secure Element”. In: *CoRR* abs/2205.04775 (2022). DOI: [10.48550/ARXIV.2205.04775](https://doi.org/10.48550/ARXIV.2205.04775).
- [47] P. Nasahl, M. Unterguggenberger, R. Nagpal, R. Schilling, D. Schrammel, and S. Mangard. “SCFI: State Machine Control-Flow Hardening Against Fault Attacks”. In: *CoRR* abs/2208.01356 (2022). DOI: [10.48550/ARXIV.2208.01356](https://doi.org/10.48550/ARXIV.2208.01356).
- [46] B. Gigerl, R. Primas, and S. Mangard. “Secure and Efficient Software Masking on Superscalar Pipelined Processors”. In: *IACR Cryptol. ePrint Arch.* 2021 (2021), p. 1110. URL: <https://eprint.iacr.org/2021/1110>.
- [45] R. Schilling, P. Nasahl, and S. Mangard. “FIPAC: Thwarting Fault- and Software-Induced Control-Flow Attacks with ARM Pointer Authentication”. In: *CoRR* abs/2104.14993 (2021). URL: <https://arxiv.org/abs/2104.14993>.
- [44] S. Steinegger, D. Schrammel, S. Weiser, P. Nasahl, and S. Mangard. “SERVAS! Secure Enclaves via RISC-V Authenticryption Shield”. In: *CoRR* abs/2105.03395 (2021). URL: <https://arxiv.org/abs/2105.03395>.

- [43] B. Gigerl, V. Hadzic, R. Primas, S. Mangard, and R. Bloem. “Coco: Co-Design and Co-Verification of Masked Software Implementations on CPUs”. In: *IACR Cryptol. ePrint Arch.* 2020 (2020), p. 1294. URL: <https://eprint.iacr.org/2020/1294>.
- [42] P. Nasahl, R. Schilling, M. Werner, J. Hoogerbrugge, M. Medwed, and S. Mangard. “CrypTag: Thwarting Physical and Logical Memory Vulnerabilities using Cryptographically Colored Memory”. In: *CoRR* abs/2012.06761 (2020). URL: <https://arxiv.org/abs/2012.06761>.
- [41] P. Nasahl, R. Schilling, M. Werner, and S. Mangard. “HECTOR-V: A Heterogeneous CPU Architecture for a Secure RISC-V Execution Environment”. In: *CoRR* abs/2009.05262 (2020). URL: <https://arxiv.org/abs/2009.05262>.
- [40] R. Bloem, H. Groß, R. Iusupov, M. Krenn, and S. Mangard. “Sharing Independence & Relabeling: Efficient Formal Verification of Higher-Order Masking”. In: *IACR Cryptol. ePrint Arch.* 2018 (2018), p. 1031. URL: <https://eprint.iacr.org/2018/1031>.
- [39] C. Dobraunig, M. Eichlseder, H. Groß, S. Mangard, F. Mendel, and R. Primas. “Statistical Ineffective Fault Attacks on Masked AES with Fault Countermeasures”. In: *IACR Cryptol. ePrint Arch.* 2018 (2018), p. 357. URL: <https://eprint.iacr.org/2018/357>.
- [38] C. Dobraunig, M. Eichlseder, T. Korak, S. Mangard, F. Mendel, and R. Primas. “Exploiting Ineffective Fault Inductions on Symmetric Cryptography”. In: *IACR Cryptol. ePrint Arch.* 2018 (2018), p. 71. URL: <http://eprint.iacr.org/2018/071>.
- [37] C. Dobraunig, S. Mangard, F. Mendel, and R. Primas. “Fault Attacks on Nonce-based Authenticated Encryption: Application to Keyak and Ketje”. In: *IACR Cryptol. ePrint Arch.* 2018 (2018), p. 852. URL: <https://eprint.iacr.org/2018/852>.
- [36] H. Groß, L. D. Meyer, M. Krenn, and S. Mangard. “Masking the AES with Only Two Random Bits”. In: *IACR Cryptol. ePrint Arch.* 2018 (2018), p. 1007. URL: <https://eprint.iacr.org/2018/1007>.
- [35] P. Kocher, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom. “Spectre Attacks: Exploiting Speculative Execution”. In: *CoRR* abs/1801.01203 (2018). URL: <http://arxiv.org/abs/1801.01203>.
- [34] P. Kocher, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom. “Spectre Attacks: Exploiting Speculative Execution”. In: *meltdownattack.com* (2018). URL: <https://spectreattack.com/spectre.pdf>.
- [33] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, and M. Hamburg. “Meltdown”. In: *CoRR* abs/1801.01207 (2018). URL: <http://arxiv.org/abs/1801.01207>.
- [32] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, and M. Hamburg. “Meltdown”. In: *meltdownattack.com* (2018). URL: <https://meltdownattack.com/meltdown.pdf>.

- [31] R. Schilling, M. Werner, and S. Mangard. “Securing Conditional Branches in the Presence of Fault Attacks”. In: *CoRR* abs/1803.08359 (2018). URL: <http://arxiv.org/abs/1803.08359>.
- [30] R. Schilling, M. Werner, P. Nasahl, and S. Mangard. “Pointing in the Right Direction - Securing Memory Accesses in a Faulty World”. In: *CoRR* abs/1809.08811 (2018). URL: <http://arxiv.org/abs/1809.08811>.
- [29] M. Werner, T. Unterluggauer, D. Schaffenrath, and S. Mangard. “Sponge-Based Control-Flow Protection for IoT Devices”. In: *CoRR* abs/1802.06691 (2018). URL: <http://arxiv.org/abs/1802.06691>.
- [28] R. Bloem, H. Groß, R. Iusupov, B. Könighofer, S. Mangard, and J. Winter. “Formal Verification of Masked Hardware Implementations in the Presence of Glitches”. In: *IACR Cryptol. ePrint Arch.* 2017 (2017), p. 897. URL: <http://eprint.iacr.org/2017/897>.
- [27] H. Groß and S. Mangard. “Reconciling d+1Masking in Hardware and Software”. In: *IACR Cryptol. ePrint Arch.* 2017 (2017), p. 103. URL: <http://eprint.iacr.org/2017/103>.
- [26] H. Groß, D. Schaffenrath, and S. Mangard. “Higher-Order Side-Channel Protected Implementations of Keccak”. In: *IACR Cryptol. ePrint Arch.* 2017 (2017), p. 395. URL: <http://eprint.iacr.org/2017/395>.
- [25] R. Primas, P. Pessl, and S. Mangard. “Single-Trace Side-Channel Attacks on Masked Lattice-Based Encryption”. In: *IACR Cryptol. ePrint Arch.* 2017 (2017), p. 594. URL: <http://eprint.iacr.org/2017/594>.
- [24] M. Schwarz, D. Gruss, M. Lipp, C. Maurice, T. Schuster, A. Fogh, and S. Mangard. “Automated Detection, Exploitation, and Elimination of Double-Fetch Bugs using Modern CPU Features”. In: *CoRR* abs/1711.01254 (2017). URL: <http://arxiv.org/abs/1711.01254>.
- [23] M. Schwarz, M. Lipp, D. Gruss, S. Weiser, C. Maurice, R. Spreitzer, and S. Mangard. “KeyDrown: Eliminating Keystroke Timing Side-Channel Attacks”. In: *CoRR* abs/1706.06381 (2017). URL: <http://arxiv.org/abs/1706.06381>.
- [22] M. Schwarz, S. Weiser, D. Gruss, C. Maurice, and S. Mangard. “Malware Guard Extension: Using SGX to Conceal Cache Attacks”. In: *CoRR* abs/1702.08719 (2017). URL: <http://arxiv.org/abs/1702.08719>.
- [21] T. Unterluggauer, T. Korak, S. Mangard, R. Schilling, L. Benini, F. K. Gürkaynak, and M. Muehlberghuber. “Leakage Bounds for Gaussian Side Channels”. In: *IACR Cryptol. ePrint Arch.* 2017 (2017), p. 992. URL: <http://eprint.iacr.org/2017/992>.
- [20] T. Unterluggauer, M. Werner, and S. Mangard. “Securing Memory Encryption and Authentication Against Side-Channel Attacks Using Unprotected Primitives”. In: *IACR Cryptol. ePrint Arch.* 2017 (2017), p. 663. URL: <http://eprint.iacr.org/2017/663>.
- [19] M. Werner, T. Unterluggauer, R. Schilling, D. Schaffenrath, and S. Mangard. “Transparent Memory Encryption and Authentication”. In: *IACR Cryptol. ePrint Arch.* 2017 (2017), p. 674. URL: <http://eprint.iacr.org/2017/674>.

- [18] F. Conti, R. Schilling, P. D. Schiavone, A. Pullini, D. Rossi, F. K. Gürkaynak, M. Muehlberghuber, M. Gautschi, I. Loi, G. Haugou, S. Mangard, and L. Benini. “An IoT Endpoint System-on-Chip for Secure and Energy-Efficient Near-Sensor Analytics”. In: *CoRR* abs/1612.05974 (2016). URL: <http://arxiv.org/abs/1612.05974>.
- [17] C. Dobraunig, M. Eichlseder, S. Mangard, F. Mendel, and T. Unterluggauer. “ISAP - Authenticated Encryption Inherently Secure Against Passive Side-Channel Attacks”. In: *IACR Cryptol. ePrint Arch.* 2016 (2016), p. 952. URL: <http://eprint.iacr.org/2016/952>.
- [16] H. Groß, M. Jelinek, S. Mangard, T. Unterluggauer, and M. Werner. “Concealing Secrets in Embedded Processors Designs”. In: *IACR Cryptol. ePrint Arch.* 2016 (2016), p. 935. URL: <http://eprint.iacr.org/2016/935>.
- [15] H. Groß, S. Mangard, and T. Korak. “Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order”. In: *IACR Cryptol. ePrint Arch.* 2016 (2016), p. 486. URL: <http://eprint.iacr.org/2016/486>.
- [14] R. Spreitzer, V. Moonsamy, T. Korak, and S. Mangard. “SoK: Systematic Classification of Side-Channel Attacks on Mobile Devices”. In: *CoRR* abs/1611.03748 (2016). URL: <http://arxiv.org/abs/1611.03748>.
- [13] T. Unterluggauer and S. Mangard. “Exploiting the Physical Disparity: Side-Channel Attacks on Memory Encryption”. In: *IACR Cryptol. ePrint Arch.* 2016 (2016), p. 473. URL: <http://eprint.iacr.org/2016/473>.
- [12] T. Unterluggauer, M. Werner, and S. Mangard. “Side-Channel Plaintext-Recovery Attacks on Leakage-Resilient Encryption”. In: *IACR Cryptol. ePrint Arch.* 2016 (2016), p. 1074. URL: <http://eprint.iacr.org/2016/1074>.
- [11] C. Dobraunig, M. Eichlseder, S. Mangard, and F. Mendel. “On the Security of Fresh Re-keying to Counteract Side-Channel and Fault Attacks”. In: *IACR Cryptol. ePrint Arch.* 2015 (2015), p. 33. URL: <http://eprint.iacr.org/2015/033>.
- [10] D. Gruss, C. Maurice, and S. Mangard. “Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript”. In: *CoRR* abs/1507.06955 (2015). URL: <http://arxiv.org/abs/1507.06955>.
- [9] M. Lipp, D. Gruss, R. Spreitzer, and S. Mangard. “ARMageddon: Last-Level Cache Attacks on Mobile Devices”. In: *CoRR* abs/1511.04897 (2015). URL: <http://arxiv.org/abs/1511.04897>.
- [8] P. Pessl, D. Gruss, C. Maurice, and S. Mangard. “Reverse Engineering Intel DRAM Addressing and Exploitation”. In: *CoRR* abs/1511.08756 (2015). URL: <http://arxiv.org/abs/1511.08756>.
- [7] S. Belaïd, F. D. Santis, J. Heyszl, S. Mangard, M. Medwed, J. Schmidt, F. Standaert, and S. Tillich. “Towards Fresh Re-Keying with Leakage-Resilient PRFs: Cipher Design Principles and Analysis”. In: *IACR Cryptol. ePrint Arch.* 2013 (2013), p. 305. URL: <http://eprint.iacr.org/2013/305>.

- [6] J. Heyszl, A. Ibing, S. Mangard, F. D. Santis, and G. Sigl. “Clustering Algorithms for Non-Profiled Single-Execution Attacks on Exponentiations”. In: *IACR Cryptol. ePrint Arch.* 2013 (2013), p. 438. URL: <http://eprint.iacr.org/2013/438>.
- [5] F. Standaert, N. Veyrat-Charvillon, E. Oswald, B. Gierlichs, M. Medwed, M. Kasper, and S. Mangard. “The World is Not Enough: Another Look on Second-Order DPA”. In: *IACR Cryptol. ePrint Arch.* 2010 (2010), p. 180. URL: <http://eprint.iacr.org/2010/180>.
- [4] B. M. Gammel and S. Mangard. “On the Duality of Probing and Fault Attacks”. In: *CoRR* abs/0907.4273 (2009). URL: <http://arxiv.org/abs/0907.4273>.
- [3] B. M. Gammel and S. Mangard. “On the Duality of Probing and Fault Attacks”. In: *IACR Cryptol. ePrint Arch.* 2009 (2009), p. 352. URL: <http://eprint.iacr.org/2009/352>.
- [2] S. Mangard, E. Oswald, and F. Standaert. “One for All - All for One: Unifying Standard DPA Attacks”. In: *IACR Cryptol. ePrint Arch.* 2009 (2009), p. 449. URL: <http://eprint.iacr.org/2009/449>.
- [1] E. Oswald, S. Mangard, and N. Pramstaller. “Secure and Efficient Masking of AES - A Mission Impossible?”. In: *IACR Cryptol. ePrint Arch.* 2004 (2004), p. 134. URL: <http://eprint.iacr.org/2004/134>.