# Pei Luo

List of Publications by Year
in descending order



| | | | |
|---|---|---|---|
| 23 papers | 223 citations | 1684188 5 h-index | 1720034 7 g-index |
| 24 all docs | 24 docs citations | 24 times ranked | 168 citing authors |

| # | Article | IF | Citations |
|---|---|---|---|
| 1 | Side-channel power analysis of a GPU AES implementation. , 2015, , . | | 46 |
| 2 | A Statistical Model for Higher Order DPA on Masked Devices. Lecture Notes in Computer Science, 2014, , 147-169. | 1.3 | 33 |
| 3 | Algebraic Fault Analysis of SHA-3 Under Relaxed Fault Models. IEEE Transactions on Information Forensics and Security, 2018, 13, 1752-1761. | 6.9 | 16 |
| 4 | Power Analysis Attack of an AES GPU Implementation. Journal of Hardware and Systems Security, 2018, 2, 69-82. | 1.3 | 15 |
| 5 | Differential Fault Analysis of SHA3-224 and SHA3-256. , 2016, , . | | 14 |
| 6 | Side-channel analysis of MAC-Keccak hardware implementations. , 2015, , . | | 12 |
| 7 | Power analysis attack on hardware implementation of MAC-Keccak on FPGAs. , 2014, , . | | 10 |
| 8 | Side-channel power analysis of different protection schemes against fault attacks on AES. , 2014, , . | | 10 |
| 9 | Secure memories resistant to both random errors and fault injection attacks using nonlinear error correction codes. , 2013, , . | | 9 |
| 10 | Algebraic fault analysis of SHA-3. , 2017, , . | | 8 |
| 11 | Concurrent Error Detection for Reliable SHA-3 Design. , 2016, , . | | 7 |
| 12 | Differential Fault Analysis of SHA-3 Under Relaxed Fault Models. Journal of Hardware and Systems Security, 2017, 1, 156-172. | 1.3 | 7 |
| 13 | Hardware Implementation of Secure Shamir's Secret Sharing Scheme. , 2014, , . | | 6 |
| 14 | Towards secure cryptographic software implementation against side-channel power analysis attacks. , 2015, , . | | 6 |
| 15 | A Unified Metric for Quantifying Information Leakage of Cryptographic Devices Under Power Analysis Attacks. Lecture Notes in Computer Science, 2015, , 338-360. | 1.3 | 5 |
| 16 | A high reliable SOC on-board computer based on Leon3. , 2012, , . | | 4 |
| 17 | Balance power leakage to fight against side-channel analysis at gate level in FPGAs. , 2015, , . | | 4 |
| 18 | Scalable and efficient implementation of correlation power analysis using graphics processing units (GPUs). , 2014, , . | | 3 |

| # | Article | IF | Citations |
|---|---|---|---|
| 19 | Efficient 2nd-order power analysis on masked devices utilizing multiple leakage. , 2015, , . | | 3 |
| 20 | SEU mitigation strategies for SRAM-based FPGA. Proceedings of SPIE, 2011, , . | 0.8 | 2 |
| 21 | Efficient Nonprofiling 2nd-Order Power Analysis on Masked Devices Utilizing Multiple Leakage Points. IEEE Transactions on Dependable and Secure Computing, 2019, 16, 843-855. | 5.4 | 2 |
| 22 | Compiler-Assisted Threshold Implementation against Power Analysis Attacks. , 2017, , . | | 1 |
| 23 | Leakage evaluation on power balance countermeasure against side-channel attack on FPGAs. , 2015, , . | | 0 |