# Qiaoyan Yu

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/5857044/publications.pdf

Version: 2024-02-01

| | | | |
|---|---|---|---|
| 56<br>papers | 543<br>citations | 1163117<br>8<br>h-index | 996975<br>15<br>g-index |
| 57<br>all docs | 57<br>docs citations | 57<br>times ranked | 361<br>citing authors |

| # | Article | IF | Citations |
|---|---|---|---|
| 1 | Novel Dynamic State-Deflection Method for Gate-Level Design Obfuscation. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2018, 37, 273-285. | 2.7 | 51 |
| 2 | Hardware security assurance in emerging IoT applications. , 2016, , . |  | 42 |
| 3 | A hardened network-on-chip design using runtime hardware Trojan mitigation methods. The Integration VLSI Journal, 2017, 56, 15-31. | 2.1 | 35 |
| 4 | Hardware Security Threats and Potential Countermeasures in Emerging 3D ICs. , 2016, , . |  | 33 |
| 5 | Assessing CPA resistance of AES with different fault tolerance mechanisms. , 2016, , . |  | 31 |
| 6 | Exploiting error control approaches for Hardware Trojans on Network-on-Chip links. , 2013, , . |  | 28 |
| 7 | A Comprehensive FPGA-Based Assessment on Fault-Resistant AES against Correlation Power Analysis Attack. Journal of Electronic Testing: Theory and Applications (JETTA), 2016, 32, 611-624. | 1.2 | 26 |
| 8 | Thwarting Security Threats From Malicious FPGA Tools With Novel FPGA-Oriented Moving Target Defense. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27, 665-678. | 3.1 | 25 |
| 9 | Dual-Layer Adaptive Error Control for Network-on-Chip Links. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2012, 20, 1304-1317. | 3.1 | 21 |
| 10 | Transistor-level camouflaged logic locking method for monolithic 3D IC security. , 2016, , . |  | 19 |
| 11 | Security Threats and Countermeasures in Three-Dimensional Integrated Circuits. , 2017, , . |  | 14 |
| 12 | Hardware-Efficient Logic Camouflaging for Monolithic 3-D ICs. IEEE Transactions on Circuits and Systems II: Express Briefs, 2018, 65, 799-803. | 3.0 | 14 |
| 13 | Transient and Permanent Error Control for High-End Multiprocessor Systems-on-Chip. , 2012, , . |  | 13 |
| 14 | Exploiting hardware obfuscation methods to prevent and detect hardware Trojans. , 2017, , . |  | 13 |
| 15 | Strengthening SIMON Implementation Against Intelligent Fault Attacks. IEEE Embedded Systems Letters, 2015, 7, 113-116. | 1.9 | 12 |
| 16 | Exploiting PDN noise to thwart correlation power analysis attacks in 3D ICs. , 2018, , . |  | 12 |
| 17 | DSD: A Dynamic State-Deflection Method for Gate-Level Netlist Obfuscation. , 2016, , . |  | 10 |
| 18 | Security Threats and Countermeasures for Approximate Arithmetic Computing. , 2020, , . |  | 10 |

| # | Article | IF | Citations |
|---|---|---|---|
| 19 | Improving power analysis attack resistance using intrinsic noise in 3D ICs. The Integration VLSI Journal, 2020, 73, 30-42. | 2.1 | 9 |
| 20 | Boosting SMT solver performance on mixed-bitwise-arithmetic expressions. , 2021, , . | | 9 |
| 21 | New Security Threats on FPGAs: From FPGA Design Tools Perspective. , 2021, , . | | 9 |
| 22 | IntelliCAN: Attack-resilient Controller Area Network (CAN) for secure automobiles. , 2015, , . | | 8 |
| 23 | New Replay Attacks on ZigBee Devices for Internet-of-Things (IoT) Applications. , 2020, , . | | 8 |
| 24 | A low-cost masquerade and replay attack detection method for CAN in automobiles. , 2017, , . | | 7 |
| 25 | Securing FPGA-based obsolete component replacement for legacy systems. , 2018, , . | | 7 |
| 26 | Modeling Hardware Trojans in 3D ICs. , 2019, , . | | 7 |
| 27 | Security Threat Analyses and Attack Models for Approximate Computing Systems. ACM Transactions on Design Automation of Electronic Systems, 2021, 26, 1-31. | 2.6 | 7 |
| 28 | Analysis of Attack Surfaces and Practical Attack Examples in Open Source FPGA CAD Tools. , 2021, , . | | 7 |
| 29 | Efficient Hardware Trojan Detection with Differential Cascade Voltage Switch Logic. VLSI Design, 2014, 2014, 1-11. | 0.5 | 5 |
| 30 | Invariance Checking Based Trojan Detection Method for Three-Dimensional Integrated Circuits. , 2020, , . | | 5 |
| 31 | Fine-grained splitting methods to address permanent errors in Network-on-Chip links. , 2012, , . | | 4 |
| 32 | A 0.1-pJ/b and ACF &lt;0.04 Multiple-Valued PUF for Chip Identification Using Bit-Line Sharing Strategy in 65-nm CMOS. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27, 1043-1052. | 3.1 | 4 |
| 33 | An Attack Analysis Framework for LoRaWAN applied Advanced Manufacturing. , 2021, , . | | 4 |
| 34 | A new fault injection method for evaluation of combining SEU and SET effects on circuit reliability. , 2014, , . | | 3 |
| 35 | Securing Approximate Computing Systems via Obfuscating Approximate-Precise Boundary. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2023, 42, 27-40. | 2.7 | 3 |
| 36 | Hardware Security in Sensor and its Networks. Frontiers in Sensors, 2022, 3, . | 3.3 | 3 |

| # | Article | IF | Citations |
|---|---|---|---|
| 37 | Transient error management for partially adaptive router in network-on-chip (NoC). , 2012, , . | | 2 |
| 38 | Systematic analyses for latching probability of single-event transients. , 2014, , . | | 2 |
| 39 | Fault-tolerant methods for a new lightweight cipher SIMON. , 2015, , . | | 2 |
| 40 | Investigation of single-event upsets in dynamic logic based flip-flops. , 2015, , . | | 2 |
| 41 | Investigating Reliability and Security of Integrated Circuits and Systems. , 2018, , . | | 2 |
| 42 | ADobf: Obfuscated Detection Method against Analog Trojans on I<sup>2</sup>C Master-Slave Interface. , 2020, , . | | 2 |
| 43 | Comprehensive Analysis on Hardware Trojans in 3D ICs: Characterization and Experimental Impact Assessment. SN Computer Science, 2020, 1, 1. | 3.6 | 2 |
| 44 | Collaborative error control method for sequential logic circuits. , 2013, , . | | 1 |
| 45 | A novel energy-efficient serializer design method for gigascale systems. , 2013, , . | | 1 |
| 46 | A novel signaling technique for high-speed wireline backplane transceiver: Four phase-shifted sinusoid symbol (PSS-4). , 2014, , . | | 1 |
| 47 | Towards Energy-Efficient and Secure Computing Systems. Journal of Low Power Electronics and Applications, 2018, 8, 48. | 2.0 | 1 |
| 48 | An Orthogonal Algorithm for Key Management in Hardware Obfuscation. , 2019, , . | | 1 |
| 49 | Hardware Obfuscation Methods for Hardware Trojan Prevention and Detection. , 2018, , 291-325. | | 1 |
| 50 | Advanced VLSI Architecture Design for Emerging Digital Systems. VLSI Design, 2014, 2014, 1-2. | 0.5 | 0 |
| 51 | A New Analytical Model of SET Latching Probability for Circuits Experiencing Single- or Multiple-Cycle Single-Event Transients. Journal of Electronic Testing: Theory and Applications (JETTA), 2014, 30, 595-609. | 1.2 | 0 |
| 52 | A Survey on Energy Efficiency Techniques for Secure Computing Systems. , 2018, , . | | 0 |
| 53 | Exploiting Principle of Moving Target Defense to Secure FPGA Systems. , 2018, , . | | 0 |
| 54 | SRASA: a Generalized Theoretical Framework for Security and Reliability Analysis in Computing Systems. Journal of Hardware and Systems Security, 2019, 3, 200-218. | 1.3 | 0 |

| # | Article | IF | Citations |
|---|---|---|---|
| 55 | Guest Editor's Introduction: Special Section on Reliability-Aware Design and Analysis Methods for Digital Systems: From Gate to System Level. IEEE Transactions on Emerging Topics in Computing, 2020, 8, 561-563. | 4.6 | 0 |
| 56 | FTAI: Frequency-based Trojan-Activity Identification Method for 3D Integrated Circuits. , 2020, , . | | 0 |