Securing Designs against Scan-Based Side-Channel Atta

IEEE Transactions on Dependable and Secure Computing

4, 325-336

DOI: 10.1109/tdsc.2007.70215

Citation Report

#	Article	IF	Citations
1	A physical unclonable function defined using power distribution system equivalent resistance variations. , 2009, , .		66
2	Third workshop on dependable and secure nanocomputing. , 2009, , .		0
3	Partial Scan Approach for Secret Information Protection. , 2009, , .		31
4	SS-KTC: A High-Testability Low-Overhead Scan Architecture with Multi-level Security Integration. , 2009, , .		31
5	Fourth workshop on dependable and secure nanocomputing. , 2010, , .		0
6	Scan-Based Side-Channel Attack against RSA Cryptosystems Using Scan Signatures. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93-A, 2481-2489.	0.3	65
7	Secure and testable scan design using extended de Bruijn graphs. , 2010, , .		24
8	SREEP: Shift Register Equivalents Enumeration and Synthesis Program for secure scan design. , 2010, , .		9
9	SSTKR: Secure and Testable Scan Design through Test Key Randomization. , 2011, , .		28
10	Security challenges during VLSI test. , 2011, , .		9
11	New security threats against chips containing scan chain structures. , 2011, , .		45
12	Scan Attacks and Countermeasures in Presence of Scan Response Compactors. , 2011, , .		32
13	Differential Behavior Equivalent Classes of Shift Register Equivalents for Secure and Testable Scan Design. IEICE Transactions on Information and Systems, 2011, E94-D, 1430-1439.	0.7	5
14	Scan Vulnerability in Elliptic Curve Cryptosystems. IPSJ Transactions on System LSI Design Methodology, 2011, 4, 47-59.	0.8	9
15	Balanced Secure Scan: Partial Scan Approach for Secret Information Protection. Journal of Electronic Testing: Theory and Applications (JETTA), 2011, 27, 99-108.	1.2	4
16	Secure scan design using shift register equivalents against differential behavior attack. , 2011, , .		7
17	STEP. , 2012, , .		0
18	PUF-based secure test wrapper design for cryptographic SoC testing. , 2012, , .		33

#	Article	IF	Citations
19	Functional test of small-delay faults using SAT and Craig interpolation. , 2012, , .		20
20	Differential Scan Attack on AES with X-tolerant and X-masked Test Response Compactor. , 2012, , .		20
21	Securing Access to Reconfigurable Scan Networks. , 2013, , .		22
22	Secure Scan Design with Dynamically Configurable Connection. , 2013, , .		23
23	Don't forget to lock your SIB: hiding instruments using P1687. , 2013, , .		51
24	Security Analysis of Industrial Test Compression Schemes. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2013, 32, 1966-1977.	2.7	33
25	Generalized Feed Forward Shift Registers and Their Application to Secure Scan Design. IEICE Transactions on Information and Systems, 2013, E96.D, 1125-1133.	0.7	4
26	Secure and Testable Scan Design Utilizing Shift Register Quasi-equivalents. IPSJ Transactions on System LSI Design Methodology, 2013, 6, 27-33.	0.8	2
27	Secure scan design using improved random order and its evaluations. , 2014, , .		4
28	Design-for-Security vs. Design-for-Testability: A Case Study on DFT Chain in Cryptographic Circuits. , 2014, , .		23
29	Access Port Protection for Reconfigurable Scan Networks. Journal of Electronic Testing: Theory and Applications (JETTA), 2014, 30, 711-723.	1.2	21
30	Design for security test on cryptographic ICs for design-time security evaluation. , 2014, , .		0
31	A Primer on Hardware Security: Models, Methods, and Metrics. Proceedings of the IEEE, 2014, 102, 1283-1295.	21.3	471
32	Test Versus Security: Past and Present. IEEE Transactions on Emerging Topics in Computing, 2014, 2, 50-62.	4.6	77
33	Board security enhancement using new locking SIB-based architectures. , 2014, , .		20
34	Strongly Secure Scan Design Using Generalized Feed Forward Shift Registers. IEICE Transactions on Information and Systems, 2015, E98.D, 1852-1855.	0.7	8
35	Introduction to Hardware Security. Electronics (Switzerland), 2015, 4, 763-784.	3.1	51
36	Fingerprint-Based Detection and Diagnosis of Malicious Programs in Hardware. IEEE Transactions on Reliability, 2015, 64, 1068-1077.	4.6	9

#	Article	IF	Citations
37	Fine-Grained Access Management in Reconfigurable Scan Networks. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34, 937-946.	2.7	55
38	A Low-Cost Unified Design Methodology for Secure Test and Intellectual Property Core Protection. IEEE Transactions on Reliability, 2015, 64, 1243-1253.	4.6	4
39	A secure architecture for the design for testability structures. , 2015, , .		3
40	Properties of Generalized Feedback Shift Registers for Secure Scan Design. IEICE Transactions on Information and Systems, 2016, E99.D, 1255-1258.	0.7	2
41	Securing test infrastructure of system-on-chips. , 2016, , .		4
42	Secure scan-based design using Blum Blum Shub algorithm. , 2016, , .		6
43	A Learning-Based Approach to Secure JTAG Against Unseen Scan-Based Attacks. , 2016, , .		3
44	A new countermeasure against scan-based side-channel attacks. , 2016, , .		17
45	Realization of SR-Equivalents Using Generalized Shift Registers for Secure Scan Design. IEICE Transactions on Information and Systems, 2016, E99.D, 2182-2185.	0.7	1
46	Using Scan Side Channel for Detecting IP Theft. , 2016, , .		2
47	Security Rule Check. , 2017, , 17-36.		4
48	VLSI Test and Hardware Security Background for Hardware Obfuscation. , 2017, , 33-68.		2
49	Why current secure scan designs fail and how to fix them?. The Integration VLSI Journal, 2017, 56, 105-114.	2.1	23
50	Introduction to Hardware Obfuscation: Motivation, Methods and Evaluation. , 2017, , 3-32.		16
51	Security vulnerability analysis of design-for-test exploits for asset protection in SoCs. , 2017, , .		29
52	Protection of Assets from Scan Chain Vulnerabilities Through Obfuscation. , 2017, , 135-158.		7
53	Dynamically obfuscated scan for protecting IPs against scan-based attacks throughout supply chain. , 2017, , .		5
54	Covert Timing Channels Exploiting Non-Uniform Memory Access based Architectures. , 2017, , .		23

#	Article	IF	Citations
55	Fast and automatic security test on cryptographic ICs against fault injection attacks based on design for security test. IET Information Security, 2017, 11, 312-318.	1.7	4
56	Using Scan Side Channel to Detect IP Theft. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2017, 25, 3268-3280.	3.1	9
57	Static and Dynamic Obfuscations of Scan Data Against Scan-Based Side-Channel Attacks. IEEE Transactions on Information Forensics and Security, 2017, 12, 363-376.	6.9	55
58	How to Secure Scan Design Against Scan-Based Side-Channel Attacks?. , 2017, , .		3
59	A secure test solution for sensor nodes containing crypto-cores. , 2017, , .		2
60	Increasing IJTAG bandwidth and managing security through parallel locking-SIBs. , 2017, , .		15
61	Cross-Level Detection Framework for Attacks on Cyber-Physical Systems. Journal of Hardware and Systems Security, 2017, 1, 356-369.	1.3	5
62	A secure scan chain test scheme exploiting retention loss of memristors. , 2017, , .		3
63	Revisit sequential logic obfuscation: Attacks and defenses. , 2017, , .		59
64	Trustworthy reconfigurable access to on-chip infrastructure. , 2017, , .		15
65	Potential Trigger Detection for Hardware Trojans. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2018, 37, 1384-1395.	2.7	13
66	Secure Scan and Test Using Obfuscation Throughout Supply Chain. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2018, 37, 1867-1880.	2.7	71
67	Hardware Protection via Logic Locking Test Points. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2018, 37, 3020-3030.	2.7	14
68	Pre-silicon Formal Verification of JTAG Instruction Opcodes for Security. , 2018, , .		3
69	Detecting and Resolving Security Violations in Reconfigurable Scan Networks. , 2018, , .		9
70	Vulnerability modelling of cryptoâ€chips against scanâ€based attacks. IET Information Security, 2018, 12, 543-550.	1.7	2
71	AES Design Improvements Towards Information Security Considering Scan Attack. , 2018, , .		11
72	On Securing Scan Design Through Test Vector Encryption. , 2018, , .		9

#	Article	IF	Citations
73	Device aging: A reliability and security concern. , 2018, , .		7
74	A Secure DFT Architecture Protecting Crypto Chips Against Scan-Based Attacks. IEEE Access, 2019, 7, 22206-22213.	4.2	15
75	Scan Chain Based Attacks and Countermeasures: A Survey. IEEE Access, 2019, 7, 85055-85065.	4.2	17
76	Securing Cryptographic Chips against Scan-Based Attacks in Wireless Sensor Network Applications. Sensors, 2019, 19, 4598.	3.8	5
77	ScanSAT: Unlocking Static and Dynamic Scan Obfuscation. IEEE Transactions on Emerging Topics in Computing, 2021, 9, 1867-1882.	4.6	22
78	Design for Test and Hardware Security Utilizing Retention Loss of Memristors. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27, 2536-2547.	3.1	4
79	Enhancing Sensor Network Security with Improved Internal Hardware Design. Sensors, 2019, 19, 1752.	3.8	12
80	ScanSAT. , 2019, , .		32
81	A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance. Future Generation Computer Systems, 2019, 97, 284-294.	7.5	56
82	Securing Designs of an Area Efficient BIST Technique in UART. , 2019, , .		0
83	Co-relation Scan Attack Analysis (COSAA) on AES: A Comprehensive Approach. , 2019, , .		3
84	Statistical security analysis of AES with Xâ€tolerant response compactor against all types of test infrastructure attacks with/without novel unified countermeasure. IET Circuits, Devices and Systems, 2019, 13, 1117-1124.	1.4	5
85	Preventing Scan Attack through Test Response Encryption. , 2019, , .		7
86	Test-Oriented Attacks. , 2019, , 219-243.		0
87	Revocable attribute-based encryption with decryption key exposure resistance and ciphertext delegation. Information Sciences, 2019, 479, 116-134.	6.9	64
88	IC Protection Against JTAG-Based Attacks. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2019, 38, 149-162.	2.7	16
89	Storage Based Built-In Test Pattern Generation Method for Close-to-Functional Broadside Tests. , 2020, , .		0
90	Reduced Fault Coverage as a Target for Design Scaffolding Security. , 2020, , .		0

#	Article	IF	Citations
91	A New Secure Scan Design with PUF-based Key for Authentication. , 2020, , .		4
92	A Dynamic-Key Based Secure Scan Architecture for Manufacturing and In-Field IC Testing. IEEE Transactions on Emerging Topics in Computing, 2022, 10, 373-385.	4.6	6
93	An Approach Towards Resisting Side-Channel Attacks for Secured Testing of Advanced Encryption Algorithm (AES) Cryptochip. , 2020, , .		5
94	A Guaranteed Secure Scan Design Based on Test Data Obfuscation by Cryptographic Hash. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2020, 39, 4524-4536.	2.7	16
95	Hardware Obfuscation and Logic Locking: A Tutorial Introduction. IEEE Design and Test, 2020, 37, 59-77.	1.2	7
96	A New PUF Based Lock and Key Solution for Secure In-Field Testing of Cryptographic Chips. IEEE Transactions on Emerging Topics in Computing, 2021, 9, 1095-1105.	4.6	25
97	From Cryptography to Logic Locking: A Survey on the Architecture Evolution of Secure Scan Chains. IEEE Access, 2021, 9, 73133-73151.	4.2	18
98	A Secure Scan Architecture Protecting Scan Test and Scan Dump Using Skew-Based Lock and Key. IEEE Access, 2021, 9, 102161-102176.	4.2	2
99	Ensuring Cryptography Chips Security by Preventing Scan-Based Side-Channel Attacks With Improved DFT Architecture. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022, 52, 2009-2023.	9.3	10
100	A Hybrid Protection Scheme for Reconfigurable Scan Networks. , 2021, , .		3
101	An Attack on Linear Scan Chains for Stream Ciphers and the Impossibility of Simple Countermeasures. Journal of Hardware and Systems Security, 0, , 1.	1.3	0
102	Defense-in-depth: A recipe for logic locking to prevail. The Integration VLSI Journal, 2020, 72, 39-57.	2.1	44
103	MAGLeak: A Learning-Based Side-Channel Attack for Password Recognition With Multiple Sensors in IIoT Environment. IEEE Transactions on Industrial Informatics, 2022, 18, 467-476.	11.3	19
105	Nanoscale Technologies: Prospect or Hazard to Dependable and Secure Computing?. Lecture Notes in Computer Science, 2007, , 3-6.	1.3	0
107	Scan-Based Side-Channel Attack on the RSA Cryptosystem. , 0, , .		0
108	Rapid and Proactive Approach on Exploration of Vulnerabilities in Cloud based Operating Systems. International Journal of Computer Applications, 2012, 42, 37-44.	0.2	23
109	An Efficient Technique to Protect AES Secret Key from Scan Test Channel Attacks. Journal of Semiconductor Technology and Science, 2012, 12, 286-292.	0.4	4
110	NIOS II Based Secure Test Wrapper Design for Testing Cryptographic Algorithms. International Journal of Reconfigurable and Embedded Systems (IJRES), 2015, 4, 185.	0.4	0

#	Article	IF	Citations
111	On Secure Data Flow in Reconfigurable Scan Networks. , 2019, , .		12
112	Hardware Trojans in Microcircuits. , 2020, , 277-452.		0
113	Preventing Scan-Based Side-Channel Attacks by Scan Obfuscating with a Configurable Shift Register. Security and Communication Networks, 2021, 2021, 1-9.	1.5	0
114	Is your secure test infrastructure secure enough? : Attacks based on delay test patterns using transient behavior analysis. , 2021, , .		1
115	Mist-Scan: A Secure Scan Chain Architecture to Resist Scan-Based Attacks in Cryptographic Chips. , 2020, , .		1
116	Secure Scan Design through Pseudo Fault Injection. , 2021, , .		0
117	SCAR: Security Compliance Analysis and Resynthesis of Reconfigurable Scan Networks. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2022, 41, 5644-5656.	2.7	2
118	Evaluating Security of New Locking SIB-based Architectures. , 2022, , .		3
119	PUF-based Secure Test Wrapper Design for Network-on-Chip. , 2022, , .		1
120	ICT for Acceptance of the Rights of Others in Cities: Promoting Social Justice, Inclusivity, and Stability Through the Use of Digital Technologies. , 2022, , 159-175.		0
121	New Approaches of Side-Channel Attacks Based on Chip Testing Methods. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2023, 42, 1411-1424.	2.7	2
122	On Attacking IJTAG Architecture based on Locking SIB with Security LFSR. , 2022, , .		1
123	Intrinsic-Transient PUF. , 2023, , 17-32.		0
124	Fault Injection Resistant Cryptographic Hardware. , 2023, , 333-346.		0
125	An obfuscation scheme of scan chain to protect the cryptographic chips. , 2022, , .		1
126	On Securing Cryptographic ICs against Scan-based Attacks: A Hamming Weight Distribution Perspective. ACM Journal on Emerging Technologies in Computing Systems, 2023, 19, 1-20.	2.3	2
127	A Novel Secure Scan Design Based on Delayed Physical Unclonable Function. Computers, Materials and Continua, 2023, 74, 6605-6622.	1.9	1
129	Logic locking for IP security: A comprehensive analysis on challenges, techniques, and trends. Computers and Security, 2023, 129, 103196.	6.0	2

#	Article	IF	Citations
130	Metrics for SoC Security Verification. , 2023, , 37-79.		0
131	A Low-overhead PUF-based Secure Scan Design. , 2023, , .		0
132	A secure scan architecture using parallel latch-based lock. The Integration VLSI Journal, 2023, 93, 102067.	2.1	0
133	An Adaptively Secure and Efficient Data Sharing System for Dynamic User Groups in Cloud. IEEE Transactions on Information Forensics and Security, 2023, 18, 5171-5185.	6.9	0
134	On Evaluating the Security of Dynamic Scan Obfuscation Scheme. , 2023, , .		0
135	Fundamentals of Logic Locking. , 2024, , 89-107.		0
136	Design-for-Testability and Its Impact on Logic Locking. , 2024, , 213-249.		0
137	A secure scan architecture using dynamic key to thwart scan-based side-channel attacks. Microelectronics Journal, 2024, 143, 106050.	2.0	0