Mitsuru Shiozaki

List of Publications by Year
in descending order

22	140	1937685 4	1588992 8
papers	citations	h-index	g-index

22	22	22	123
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Simple electromagnetic analysis attack based on geometric leak on ASIC implementation of ring-oscillator PUF. Journal of Cryptographic Engineering, 2021, 11, 201-212.	1.8	0
2	Model Reverse-Engineering Attack against Systolic-Array-Based DNN Accelerator Using Correlation Power Analysis. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2021, E104.A, 152-161.	0.3	8
3	Black-Box Adversarial Attack against Deep Neural Network Classifier Utilizing Quantized Probability Output. Journal of Signal Processing, 2020, 24, 145-148.	0.3	1
4	Deep Learning Side-Channel Attack Against Hardware Implementations of AES. , 2019, , .		7
5	Model-Extraction Attack Against FPGA-DNN Accelerator Utilizing Correlation Electromagnetic Analysis. , 2019, , .		17
6	Simple Electromagnetic Analysis Attacks based on Geometric Leak on an ASIC Implementation of Ring-Oscillator PUF. , 2019, , .		9
7	Tamper-resistant cryptographic hardware. IEICE Electronics Express, 2017, 14, 20162004-20162004.	0.8	5
8	Tamper-resistant authentication system with side-channel attack resistant AES and PUF using MDR-ROM. , 2015, , .		8
9	Tamper Resistance Simulation on Algorithm Level Design. Electrical Engineering in Japan (English) Tj ETQq1 1 0.784314 rgBT /Overloc	0.4	0
10	On measurable side-channel leaks inside ASIC design primitives. Journal of Cryptographic Engineering, 2014, 4, 59-73.	1.8	6
11	Side-channel attack resistant AES cryptographic circuits with ROM reducing address-dependent EM leaks. , 2014, , .		8
12	Side-channel Attack Countermeasure Evaluation of Cryptographic Hardware Implementation Circuit. IEEJ Transactions on Electronics, Information and Systems, 2014, 134, 1767-1774.	0.2	0
13	On Measurable Side-Channel Leaks Inside ASIC Design Primitives. Lecture Notes in Computer Science, 2013, , 159-178.	1.3	35
14	Subkey Driven Hybrid Power Analysis Attack in Frequency Domain against Cryptographic LSIs and its Evaluation. IEEJ Transactions on Electronics, Information and Systems, 2013, 133, 1322-1330.	0.2	1
15	A Countermeasure Against Side Channel Attack on Cryptographic LSI using Clock Variation Mechanism. IEEJ Transactions on Electronics, Information and Systems, 2013, 133, 2134-2142.	0.2	3
16	Efficient DPA-Resistance Verification Method with Smaller Number of Power Traces on AES Cryptographic Circuit. , 2012, , .		4
17	Architecture Aware Fault Analysis Based on Differential Presumption for Multiple Errors and its Evaluation. IEEJ Transactions on Electronics, Information and Systems, 2012, 132, 1888-1896.	0.2	1
18	Implementation and verification of DPA-resistant cryptographic DES circuit using Domino-RSL. , 2011, , .		0

#	Article	IF	Citations
19	The arbiter-PUF with high uniqueness utilizing novel arbiter circuit with Delay-Time Measurement. , 2011, , .		25
20	Tamper Resistance Simulation on Algorithm Level Design. IEEJ Transactions on Electronics, Information and Systems, 2011, 131, 1940-1949.	0.2	0
21	20GHz uniform-phase uniform-amplitude standing-wave clock distribution. IEICE Electronics Express, 2006, 3, 11-16.	0.8	2
22	A 2.7 Gcps and 7-Multiplexing CDMA Serial Communication Chip for Real-Time Robot Control with Multiprocessors. Journal of Robotics and Mechatronics, 2005, 17, 463-468.	1.0	0