Sylvain Guilley

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/4810608/publications.pdf

Version: 2024-02-01

184	4,271	218677	265206
papers	citations	26	42
		h-index	g-index

190	190	190	1364
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Boolean Functions for Cryptography and Error-Correcting Codes. , 2010, , 257-397.		464
2	Vectorial Boolean Functions for Cryptography. , 2010, , 398-470.		242
3	Four decades of research on bent functions. Designs, Codes, and Cryptography, 2016, 78, 5-50.	1.6	156
4	Complementary dual codes for counter-measures to side-channel attacks. Advances in Mathematics of Communications, 2016, 10, 131-150.	0.7	131
5	RSM: A small and fast countermeasure for AES, secure against 1st and 2nd-order zero-offset SCAs. , 2012, , .		116
6	Practical Setup Time Violation Attacks on AES. , 2008, , .		103
7	Hardware Trojan Horses in Cryptographic IP Cores. , 2013, , .		100
8	Higher-Order Masking Schemes for S-Boxes. Lecture Notes in Computer Science, 2012, , 366-384.	1.3	84
9	Further properties of several classes of Boolean functions with optimum algebraic immunity. Designs, Codes, and Cryptography, 2009, 52, 303-338.	1.6	82
10	Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts. Lecture Notes in Computer Science, 2016, , 311-343.	1.3	78
11	Classes of Quadratic APN Trinomials and Hexanomials and Related Structures. IEEE Transactions on Information Theory, 2008, 54, 2354-2357.	2.4	76
12	Euclidean and Hermitian LCD MDS codes. Designs, Codes, and Cryptography, 2018, 86, 2605-2618.	1.6	75
13	Recursive Lower Bounds on the Nonlinearity Profile of Boolean Functions and Their Applications. IEEE Transactions on Information Theory, 2008, 54, 1262-1272.	2.4	69
14	Differential Power Analysis Model and Some Results. International Federation for Information Processing, 2004, , 127-142.	0.4	61
15	Side-channel analysis and machine learning: A practical perspective. , 2017, , .		59
16	An Easy-to-Design PUF Based on a Single Oscillator: The Loop PUF. , 2012, , .		57
17	Orthogonal Direct Sum Masking. Lecture Notes in Computer Science, 2014, , 40-56.	1.3	55
18	Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. Designs, Codes, and Cryptography, 2011, 59, 89-109.	1.6	54

#	Article	IF	Citations
19	Differentially 4-uniform bijections by permuting the inverse function. Designs, Codes, and Cryptography, 2015, 77, 117-141.	1.6	52
20	BCDL: A high speed balanced DPL for FPGA with global precharge and no early evaluation. , 2010, , .		51
21	Linear complementary dual code improvement to strengthen encoded circuit against hardware Trojan horses. , 2015, , .		43
22	Best Information is Most Successful. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 49-79.	0.0	42
23	WDDL is Protected against Setup Time Violation Attacks. , 2009, , .		41
24	New Characterization and Parametrization of LCD Codes. IEEE Transactions on Information Theory, 2019, 65, 39-49.	2.4	40
25	Good Is Not Good Enough. Lecture Notes in Computer Science, 2014, , 55-74.	1.3	39
26	Evolutionary Algorithms for Boolean Functions in Diverse Domains of Cryptography. Evolutionary Computation, 2016, 24, 667-694.	3.0	38
27	On Highly Nonlinear S-Boxes and Their Inability to Thwart DPA Attacks. Lecture Notes in Computer Science, 2005, , 49-62.	1.3	37
28	Detecting Hidden Leakages. Lecture Notes in Computer Science, 2014, , 324-342.	1.3	37
29	On Semibent Boolean Functions. IEEE Transactions on Information Theory, 2012, 58, 3287-3292.	2.4	36
30	The â€œBackend Duplicationâ€•Method. Lecture Notes in Computer Science, 2005, , 383-397.	1.3	35
31	Security Evaluation of WDDL and SecLib Countermeasures against Power Attacks. IEEE Transactions on Computers, 2008, 57, 1482-1497.	3.4	33
32	Wavelet transform based pre-processing for side channel analysis. , 2012, , .		33
33	Portability of templates. Journal of Cryptographic Engineering, 2012, 2, 63-74.	1.8	32
34	On Linear Complementary Pairs of Codes. IEEE Transactions on Information Theory, 2018, 64, 6583-6589.	2.4	32
35	Evaluation of Power Constant Dual-Rail Logics Countermeasures against DPA with Design Time Security Metrics. IEEE Transactions on Computers, 2010, 59, 1250-1263.	3.4	31
36	Template attack versus Bayes classifier. Journal of Cryptographic Engineering, 2017, 7, 343-351.	1.8	31

#	Article	IF	Citations
37	On $sigma$ -LCD Codes. IEEE Transactions on Information Theory, 2019, 65, 1694-1704.	2.4	29
38	Analysis and Improvements of the DPA Contest v4 Implementation. Lecture Notes in Computer Science, 2014, , 201-218.	1.3	29
39	Silicon-level Solutions to Counteract Passive and Active Attacks. , 2008, , .		28
40	A New Representation of Boolean Functions. Lecture Notes in Computer Science, 1999, , 94-103.	1.3	27
41	Practical improvements of side-channel attacks on AES: feedback from the 2nd DPA contest. Journal of Cryptographic Engineering, 2014, 4, 259-274.	1.8	27
42	Leakage Squeezing Countermeasure against High-Order Attacks. Lecture Notes in Computer Science, 2011, , 208-223.	1.3	27
43	Side-channel leakage and trace compression using normalized inter-class variance. , 2014, , .		25
44	Algebraic Decomposition for Probing Security. Lecture Notes in Computer Science, 2015, , 742-763.	1.3	25
45	Leakage Squeezing of Order Two. Lecture Notes in Computer Science, 2012, , 120-139.	1.3	25
46	Masks Will Fall Off. Lecture Notes in Computer Science, 2014, , 344-365.	1.3	25
47	Fault Injection Resilience. , 2010, , .		24
48	Analysis of the algebraic side channel attack. Journal of Cryptographic Engineering, 2012, 2, 45-62.	1.8	23
49	Multiply Constant-Weight Codes and the Reliability of Loop Physically Unclonable Functions. IEEE Transactions on Information Theory, 2014, 60, 7026-7034.	2.4	23
50	Method taking into account process dispersion to detect hardware Trojan Horse by side-channel analysis. Journal of Cryptographic Engineering, 2016, 6, 239-247.	1.8	23
51	Lightweight Ciphers and Their Side-Channel Resilience. IEEE Transactions on Computers, 2020, 69, 1434-1448.	3.4	23
52	First Principal Components Analysis: A New Side Channel Distinguisher. Lecture Notes in Computer Science, 2011, , 407-419.	1.3	22
53	Place-and-route impact on the security of DPL designs in FPGAs. , 2008, , .		21
54	Overview of Dual rail with Precharge logic styles to thwart implementation-level attacks on hardware cryptoprocessors. , 2009, , .		21

#	Article	IF	Citations
55	A synthesis of side-channel attacks on elliptic curve cryptography in smart-cards. Journal of Cryptographic Engineering, 2013, 3, 241-265.	1.8	21
56	Statistical properties of side-channel and fault injection attacks using coding theory. Cryptography and Communications, 2018, 10, 909-933.	1.4	21
57	Formal Analysis of the Entropy / Security Trade-off in First-Order Masking Countermeasures against Side-Channel Attacks. Lecture Notes in Computer Science, 2011, , 22-39.	1.3	21
58	A New Class of Codes for Boolean Masking of Cryptographic Computations. IEEE Transactions on Information Theory, 2012, 58, 6000-6011.	2.4	20
59	Achieving side-channel high-order correlation immunity with leakage squeezing. Journal of Cryptographic Engineering, 2014, 4, 107-121.	1.8	20
60	CCZ-equivalence of bent vectorial functions and related constructions. Designs, Codes, and Cryptography, 2011, 59, 69-87.	1.6	19
61	Impact of Aging on the Reliability of Delay PUFs. Journal of Electronic Testing: Theory and Applications (JETTA), 2018, 34, 571-586.	1.2	19
62	Security evaluation of different AES implementations against practical setup time violation attacks in FPGAs. , 2009, , .		18
63	Comments on "Constructions of Cryptographically Significant Boolean Functions Using Primitive Polynomials. IEEE Transactions on Information Theory, 2011, 57, 4852-4853.	2.4	18
64	New secondary constructions of Bent functions. Applicable Algebra in Engineering, Communications and Computing, 2016, 27, 413-434.	0.5	18
65	Optimizing Inner Product Masking Scheme by a Coding Theory Approach. IEEE Transactions on Information Forensics and Security, 2021, 16, 220-235.	6.9	18
66	A Theoretical Study of Kolmogorov-Smirnov Distinguishers. Lecture Notes in Computer Science, 2014, , 9-28.	1.3	18
67	Side-Channel Analysis of Lightweight Ciphers: Does Lightweight Equal Easy?. Lecture Notes in Computer Science, 2017, , 91-104.	1.3	18
68	From cryptography to hardware: analyzing and protecting embedded Xilinx BRAM for cryptographic applications. Journal of Cryptographic Engineering, 2013, 3, 213-225.	1.8	17
69	A formal proof of countermeasures against fault injection attacks on CRT-RSA. Journal of Cryptographic Engineering, 2014, 4, 173-185.	1.8	17
70	Linear codes with small hulls in semi-primitive case. Designs, Codes, and Cryptography, 2019, 87, 3063-3075.	1.6	17
71	On the entropy of Physically Unclonable Functions. , 2016, , .		16
72	Optimal side-channel attacks for multivariate leakages and multiple models. Journal of Cryptographic Engineering, 2017, 7, 331-341.	1.8	16

#	Article	IF	Citations
73	Trade-Offs for S-Boxes: Cryptographic Properties and Side-Channel Resilience. Lecture Notes in Computer Science, 2017, , 393-414.	1.3	16
74	Evolutionary Approach for Finding Correlation Immune Boolean Functions of Order t with Minimal Hamming Weight. Lecture Notes in Computer Science, 2015, , 71-82.	1.3	16
75	Dismantling Real-World ECC with Horizontal and Vertical Template Attacks. Lecture Notes in Computer Science, 2016, , 88-108.	1.3	16
76	Comparison between Side-Channel Analysis Distinguishers. Lecture Notes in Computer Science, 2012, , 331-340.	1.3	16
77	Correlation Immunity of Boolean Functions. , 2015, , .		15
78	Formally proved security of assembly code against power analysis. Journal of Cryptographic Engineering, 2016, 6, 201-216.	1.8	15
79	Stochastic Collision Attack. IEEE Transactions on Information Forensics and Security, 2017, 12, 2090-2104.	6.9	14
80	A Key to Success. Lecture Notes in Computer Science, 2015, , 270-290.	1.3	14
81	Practical Improvements of Profiled Side-Channel Attacks on a Hardware Crypto-Accelerator. Lecture Notes in Computer Science, 2010, , 243-260.	1.3	14
82	A Pre-processing Composition for Secret Key Recovery on Android Smartphone. Lecture Notes in Computer Science, 2014, , 76-91.	1.3	14
83	A low-entropy first-degree secure provable masking scheme for resource-constrained devices. , 2013, , .		13
84	Leakage squeezing: Optimal implementation and security evaluation. Journal of Mathematical Cryptology, 2014, 8, 249-295.	0.7	13
85	On the optimality and practicability of mutual information analysis in some scenarios. Cryptography and Communications, 2018, 10, 101-121.	1.4	13
86	Detecting Failures and Attacks via Digital Sensors. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2021, 40, 1315-1326.	2.7	13
87	A First-Order Leak-Free Masking Countermeasure. Lecture Notes in Computer Science, 2012, , 156-170.	1.3	13
88	DRECON: DPA Resistant Encryption by Construction. Lecture Notes in Computer Science, 2014, , 420-439.	1.3	12
89	Time-Frequency Analysis for Second-Order Attacks. Lecture Notes in Computer Science, 2014, , 108-122.	1.3	12
90	Formal Framework for the Evaluation of Waveform Resynchronization Algorithms. Lecture Notes in Computer Science, 2011, , 100-115.	1.3	12

#	Article	IF	Citations
91	Optimal First-Order Masking with Linear and Non-linear Bijections. Lecture Notes in Computer Science, 2012, , 360-377.	1.3	12
92	Secured CAD Back-End Flow for Power-Analysis-Resistant Cryptoprocessors. IEEE Design and Test of Computers, 2007, 24, 546-555.	1.0	11
93	Efficient Dual-Rail Implementations in FPGA Using Block RAMs. , 2011, , .		11
94	Multiply constant weight codes. , 2013, , .		11
95	Integrated Sensor: A Backdoor for Hardware Trojan Insertions?. , 2015, , .		11
96	Delay PUF Assessment Method Based on Side-Channel and Modeling Analyzes: The Final Piece of All-in-One Assessment Methodology. , 2016, , .		11
97	On the Effect of Aging on Digital Sensors. , 2020, , .		11
98	Same Values Power Analysis Using Special Points on Elliptic Curves. Lecture Notes in Computer Science, 2012, , 183-198.	1.3	10
99	Exploiting FPGA block memories for protected cryptographic implementations. , 2013, , .		10
100	Encoding the state of integrated circuits. , 2014, , .		10
101	Connecting and Improving Direct Sum Masking and Inner Product Masking. Lecture Notes in Computer Science, 2018, , 123-141.	1.3	10
102	Effect of Aging on PUF Modeling Attacks based on Power Side-Channel Observations. , 2020, , .		10
103	Boosting Higher-Order Correlation Attacks by Dimensionality Reduction. Lecture Notes in Computer Science, 2014, , 183-200.	1.3	10
104	On the dual of bent functions with 2^r Niho exponents. , 2011, , .		9
105	Enhanced Boolean functions suitable for the filter model of pseudo-random generator. Designs, Codes, and Cryptography, 2015, 76, 571-587.	1.6	9
106	Predictive Aging of Reliability of Two Delay PUFs. Lecture Notes in Computer Science, 2016, , 213-232.	1.3	9
107	Side-Channel Analysis and Countermeasure Design on ARM-Based Quantum-Resistant SIKE. IEEE Transactions on Computers, 2020, 69, 1681-1693.	3.4	9
108	Intrinsic Resiliency of S-Boxes Against Side-Channel Attacksâ€“Best and Worst Scenarios. IEEE Transactions on Information Forensics and Security, 2021, 16, 203-218.	6.9	9

#	Article	IF	Citations
109	Exploiting FPGA Block Memories for Protected Cryptographic Implementations. ACM Transactions on Reconfigurable Technology and Systems, 2015, 8, 1-16.	2.5	8
110	Cryptographic properties of monotone Boolean functions. Journal of Mathematical Cryptology, 2016, 10, 1-14.	0.7	8
111	Cache-Timing Attack Detection and Prevention. Lecture Notes in Computer Science, 2019, , 13-21.	1.3	8
112	Codes for Side-Channel Attacks and Protections. Lecture Notes in Computer Science, 2017, , 35-55.	1.3	8
113	Correlation-Immune Boolean Functions for Leakage Squeezing and Rotating S-Box Masking against Side Channel Attacks. Lecture Notes in Computer Science, 2013, , 70-74.	1.3	8
114	A Survey on Nonlinear Boolean Functions with Optimal Algebraic Immunity Suitable for Stream Ciphers. Vietnam Journal of Mathematics, 2013, 41, 527-541.	0.8	7
115	Niho bent functions from quadratic o-monomials. , 2014, , .		7
116	Higher-Order CIS Codes. IEEE Transactions on Information Theory, 2014, 60, 5283-5295.	2.4	7
117	Exploiting Small Leakages in Masks to Turn a Second-Order Attack into a First-Order Attack and Improved Rotating Substitution Box Masking with Linear Code Cosets. Scientific World Journal, The, 2015, 2015, 1-10.	2.1	7
118	Correlated Extra-Reductions Defeat Blinded Regular Exponentiation. Lecture Notes in Computer Science, 2016, , 3-22.	1.3	7
119	On the Effect of Aging in Detecting Hardware Trojan Horses with Template Analysis. , 2018, , .		7
120	On the power of template attacks in highly multivariate context. Journal of Cryptographic Engineering, 2020, 10, 337-354.	1.8	7
121	End-to-end automated cache-timing attack driven by machine learning. Journal of Cryptographic Engineering, 2021, 11, 135-146.	1.8	7
122	Taylor Expansion of Maximum Likelihood Attacks for Masked and Shuffled Implementations. Lecture Notes in Computer Science, 2016, , 573-601.	1.3	7
123	Cross-PUF Attacks on Arbiter-PUFs through their Power Side-Channel. , 2020, , .		7
124	Exploiting Dual-Output Programmable Blocks to Balance Secure Dual-Rail Logics. International Journal of Reconfigurable Computing, 2010, 2010, 1-12.	0.2	6
125	Multivariate High-Order Attacks of Shuffled Tables Recomputation. Journal of Cryptology, 2018, 31, 351-393.	2.8	6
126	Detecting Cache-Timing Vulnerabilities in Post-Quantum Cryptography Algorithms. , 2018, , .		6

#	Article	IF	Citations
127	On APN exponents, characterizations of differentially uniform functions by the Walsh transform, and related cyclic-difference-set-like structures. Designs, Codes, and Cryptography, 2019, 87, 203-224.	1.6	6
128	Polynomial direct sum masking to protect against both SCA and FIA. Journal of Cryptographic Engineering, 2019, 9, 303-312.	1.8	6
129	Failure and Attack Detection by Digital Sensors. , 2020, , .		6
130	Evolutionary algorithms-assisted construction of cryptographic boolean functions. , 2021, , .		6
131	Assessment and Mitigation of Power Side-Channel-Based Cross-PUF Attacks on Arbiter-PUFs and Their Derivatives. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2022, 30, 187-200.	3.1	6
132	The Conflicted Usage of RLUTs for Security-Critical Applications on FPGA. Journal of Hardware and Systems Security, 2018, 2, 162-178.	1.3	5
133	On the nonlinearity of monotone Boolean functions. Cryptography and Communications, 2018, 10, 1051-1061.	1.4	5
134	On the Performance and Security of Multiplication in GF(2N). Cryptography, 2018, 2, 25.	2.3	5
135	The Big Picture of Delay-PUF Dependability. , 2020, , .		5
136	A direct proof of APN-ness of the Kasami functions. Designs, Codes, and Cryptography, 2021, 89, 441-446.	1.6	5
137	Making Obfuscated PUFs Secure Against Power Side-Channel Based Modeling Attacks. , 2021, , .		5
138	On the Higher Order Nonlinearities of Boolean Functions and S-boxes. , 2009, , .		4
139	Formal Analysis of CRT-RSA Vigilant's Countermeasure Against the BellCoRe Attack. , 2014, , .		4
140	Impact of Aging on Template Attacks. , 2018, , .		4
141	Identifier Randomization: An Efficient Protection Against CAN-Bus Attacks. , 2018, , 219-254.		4
142	Using Digital Sensors to Leverage Chips' Security. , 2020, , .		4
143	Reducing Aging Impacts in Digital Sensors via Run-Time Calibration. Journal of Electronic Testing: Theory and Applications (JETTA), 2021, 37, 653-673.	1.2	4
144	Vade mecum on side-channels attacks and countermeasures for the designer and the evaluator. , 2011, , .		3

#	Article	IF	Citations
145	Register leakage masking using Gray code. , 2012, , .		3
146	Private circuits II versus fault injection attacks. , 2015, , .		3
147	Impact of the switching activity on the aging of delay-PUFs. , 2017, , .		3
148	Implementation flaws in the masking scheme of DPA Contest v4. IET Information Security, 2017, 11, 356-362.	1.7	3
149	Some (almost) optimally extendable linear codes. Designs, Codes, and Cryptography, 2019, 87, 2813-2834.	1.6	3
150	On those multiplicative subgroups of $${mathbb F}_{2^n}^*$$ which are Sidon sets and/or sum-free sets. Journal of Algebraic Combinatorics, 2022, 55, 43-59.	0.8	3
151	Detecting faults in inner product masking scheme. Journal of Cryptographic Engineering, 2021, 11, 119-133.	1.8	3
152	Linear Programming Bounds on the Kissing Number of q-ary Codes. , 2021, , .		3
153	On the arithmetic Walsh coefficients of Boolean functions. Designs, Codes, and Cryptography, 2014, 73, 299-318.	1.6	2
154	Exploiting small leakages in masks to turn a second-order attack into a first-order attack. , 2015, , .		2
155	On the (non-)existence of APN (n, n)-functions of algebraic degree n. , 2016, , .		2
156	Using modular extension to provably protect Edwards curves against fault attacks. Journal of Cryptographic Engineering, 2017, 7, 321-330.	1.8	2
157	Binary Data Analysis for Source Code Leakage Assessment. Lecture Notes in Computer Science, 2019, , 391-409.	1.3	2
158	Analysis of Multiplicative Low Entropy Masking Schemes Against Correlation Power Attack. IEEE Transactions on Information Forensics and Security, 2021, 16, 4466-4481.	6.9	2
159	Highly Reliable PUFs for Embedded Systems, Protected Against Tampering. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2021, , 167-184.	0.3	2
160	Spectral approach to process the (multivariate) high-order template attack against any masking scheme. Journal of Cryptographic Engineering, 2022, 12, 75-93.	1.8	2
161	Low-Cost Countermeasure against RPA. Lecture Notes in Computer Science, 2013, , 106-122.	1.3	2
162	Security Evaluation Against Side-Channel Analysis at Compilation Time. Communications in Computer and Information Science, 2019, , 129-148.	0.5	2

#	Article	IF	Citations
163	Information Leakage in Code-Based Masking: A Systematic Evaluation by Higher-Order Attacks. IEEE Transactions on Information Forensics and Security, 2022, 17, 1624-1638.	6.9	2
164	Cross-PUF Attacks: Targeting FPGA Implementation of Arbiter-PUFs. Journal of Electronic Testing: Theory and Applications (JETTA), 2022, 38, 261-277.	1.2	2
165	Editorial: Cryptography and Communications, Volume 1, Issue 1. Cryptography and Communications, 2009, 1, 1-2.	1.4	1
166	A formal study of two physical countermeasures against side channel attacks. Journal of Cryptographic Engineering, 2013, 3, 169-180.	1.8	1
167	Advanced Analysis of Faults Injected Through Conducted Intentional Electromagnetic Interferences. IEEE Transactions on Electromagnetic Compatibility, 2013, 55, 589-596.	2.2	1
168	Aging Effects on Template Attacks Launched on Dual-Rail Protected Chips. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2022, 41, 1276-1289.	2.7	1
169	SCA Countermeasures. , 2021, , 35-46.		1
170	Stochastic methods defeat regular RSA exponentiation algorithms with combined blinding methods. Journal of Mathematical Cryptology, 2021, 15, 408-433.	0.7	1
171	Physical Security Versus Masking Schemes. , 2018, , 269-284.		1
172	Confused yet Successful:. Lecture Notes in Computer Science, 2019, , 533-553.	1.3	1
173	Editorial about PROOFS 2015. Journal of Cryptographic Engineering, 2017, 7, 19-20.	1.8	0
174	Side-Channel Evaluation Methodology on Software. Cryptography, 2020, 4, 27.	2.3	0
175	Coalescence Principle. , 2021, , 67-77.		0
176	On the Implementation Efficiency of Linear Regression-Based Side-Channel Attacks. Lecture Notes in Computer Science, 2021, , 147-172.	1.3	0
177	Side-Channel Distinguishers. , 2021, , 21-34.		0
178	Spectral Approach to Process the High-Order Template Attack Against any Masking Scheme. , 2021, , 133-160.		0
179	Template Attack with Coalescence Principle. , 2021, , 101-131.		0
180	Categorizing all linear codes of IPM over ${mathbb {F}}_{2^{8}}$. Cryptography and Communications, 2021, 13, 527-542.	1.4	0

#	Article	IF	Citations
181	Cumulant Expansion of Mutual Information for Quantifying Leakage of a Protected Secret. , 2021, , .		0
182	Linear Regression Analysis with Coalescence Principle. , 2021, , 79-100.		0
183	Software Camouflage. Lecture Notes in Computer Science, 2014, , 122-139.	1.3	0
184	Side-Channel Information Leakage of Code-Based Masked Implementations. , 2022, , .		0