JosÃ© Bacelar Almeida

List of Publications by Year
in descending order

18 papers	285 citations	1478505 6 h-index	1281871 11 g-index
19 all docs	19 docs citations	19 times ranked	146 citing authors

#	Article	IF	Citations
1	Jasmin. , 2017, , .		59
2	Formal verification of side-channel countermeasures using self-composition. Science of Computer Programming, 2013, 78, 796-812.	1.9	30
3	Certified computer-aided cryptography. , 2013, , .		29
4	Verifiable Side-Channel Security of Cryptographic Implementations: Constant-Time MEE-CBC. Lecture Notes in Computer Science, 2016, , 163-184.	1.3	27
5	A Certifying Compiler for Zero-Knowledge Proofs of Knowledge Based on Î£-Protocols. Lecture Notes in Computer Science, 2010, , 151-167.	1.3	26
6	A Fast and Verified Software Stack for Secure Function Evaluation. , 2017, , .		20
7	Full proof cryptography. , 2012, , .		17
8	Bounded Version Vectors. Lecture Notes in Computer Science, 2004, , 102-116.	1.3	15
9	Partial Derivative Automata Formalized in Coq. Lecture Notes in Computer Science, 2011, , 59-68.	1.3	10
10	Teaching how to program using automated assessment and functional glossy games (experience) Tj ETQq0 0 0 rgBT /Overlock 10 Tf 50		9
11	Enforcing Ideal-World Leakage Bounds in Real-World Secret Sharing MPC Frameworks. , 2018, , .		7
12	A Tool for Programming with Interaction Nets. Electronic Notes in Theoretical Computer Science, 2008, 219, 83-96.	0.9	4
13	Machine-checked ZKP for NP relations: Formally Verified Security Proofs and Implementations of MPC-in-the-Head. , 2021, , .		4
14	Verifying Cryptographic Software Correctness with Respect to Reference Implementations. Lecture Notes in Computer Science, 2009, , 37-52.	1.3	3
15	Token-passing Nets for Functional Languages. Electronic Notes in Theoretical Computer Science, 2008, 204, 181-198.	0.9	2
16	Deductive verification of cryptographic software. Innovations in Systems and Software Engineering, 2010, 6, 203-218.	2.1	2
17	A Local Graph-rewriting System for Deciding Equality in Sum-product Theories. Electronic Notes in Theoretical Computer Science, 2007, 176, 139-163.	0.9	1
18	CAOVerif: An open-source deductive verification platform for cryptographic software implementations. Science of Computer Programming, 2014, 91, 216-233.	1.9	0