

CÃ©dric Fournet

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/11310087/publications.pdf>

Version: 2024-02-01

51
papers

2,955
citations

430874

18
h-index

345221

36
g-index

53
all docs

53
docs citations

53
times ranked

1060
citing authors

#	ARTICLE	IF	CITATIONS
1	Mobile values, new names, and secure communication. , 2001, , .		421
2	VC3: Trustworthy Data Analytics in the Cloud Using SGX. , 2015, , .		380
3	A calculus of mobile agents. Lecture Notes in Computer Science, 1996, , 406-421.	1.3	217
4	Mobile values, new names, and secure communication. ACM SIGPLAN Notices, 2001, 36, 104-115.	0.2	188
5	Automated verification of selected equivalences for security protocols. The Journal of Logic and Algebraic Programming, 2008, 75, 3-51.	1.4	171
6	Triple Handshakes and Cookie Cutters: Breaking and Fixing Authentication over TLS. , 2014, , .		118
7	Secure distributed programming with value-dependent types. , 2011, , .		114
8	Refinement types for secure implementations. ACM Transactions on Programming Languages and Systems, 2011, 33, 1-45.	2.1	97
9	Private authentication. Theoretical Computer Science, 2004, 322, 427-476.	0.9	93
10	The Applied Pi Calculus. Journal of the ACM, 2018, 65, 1-41.	2.2	82
11	Refinement Types for Secure Implementations. , 2008, , .		73
12	Just fast keying in the pi calculus. ACM Transactions on Information and System Security, 2007, 10, 9.	4.5	65
13	Cryptographically verified implementations for TLS. , 2008, , .		65
14	Modular verification of security protocol code by typing. , 2010, , .		60
15	Fully abstract compilation to JavaScript. , 2013, , .		57
16	Cryptographic Protocol Synthesis and Verification for Multiparty Sessions. , 2009, , .		53
17	Modular code-based cryptographic verification. , 2011, , .		52
18	Secure Implementation of Channel Abstractions. Information and Computation, 2002, 174, 37-83.	0.7	46

#	ARTICLE	IF	CITATIONS
19	Verified interoperable implementations of security protocols. ACM Transactions on Programming Languages and Systems, 2008, 31, 1-61.	2.1	42
20	Authentication primitives and their compilation. , 2000, , .		41
21	A hierarchy of equivalences for asynchronous calculi. Lecture Notes in Computer Science, 1998, , 844-855.	1.3	38
22	Secure distributed programming with value-dependent types. ACM SIGPLAN Notices, 2011, 46, 266-278.	0.2	34
23	Modern Concurrency Abstractions for C#. Lecture Notes in Computer Science, 2002, , 415-440.	1.3	32
24	Implicit typing Ã la ML for the join-calculus. Lecture Notes in Computer Science, 1997, , 196-212.	1.3	31
25	Verified implementations of the information card federated identity-management protocol. , 2008, , .		29
26	Hiding Names: Private Authentication in the Applied Pi Calculus. Lecture Notes in Computer Science, 2003, , 317-338.	1.3	28
27	Verified Cryptographic Implementations for TLS. ACM Transactions on Information and System Security, 2012, 15, 1-32.	4.5	27
28	Downgrade Resilience in Key-Exchange Protocols. , 2016, , .		27
29	Secure distributed programming with value-dependent types. Journal of Functional Programming, 2013, 23, 402-451.	0.8	26
30	A hierarchy of equivalences for asynchronous calculi. The Journal of Logic and Algebraic Programming, 2005, 63, 131-173.	1.4	25
31	Cryptographically Sound Implementations for Communicating Processes. Lecture Notes in Computer Science, 2006, , 83-94.	1.3	25
32	Secure Implementations for Typed Session Abstractions. Computer Security Foundations Workshop (CSFW), Proceedings of the IEEE, 2007, , .	0.0	20
33	Inheritance in the join calculus. The Journal of Logic and Algebraic Programming, 2003, 57, 23-69.	1.4	18
34	Code-Carrying Authorization. Lecture Notes in Computer Science, 2008, , 563-579.	1.3	15
35	Bisimulations in the join-calculus. Theoretical Computer Science, 2001, 266, 569-603.	0.9	14
36	A messy state of the union. Communications of the ACM, 2017, 60, 99-107.	4.5	14

#	ARTICLE	IF	CITATIONS
37	A secure compiler for session abstractions. <i>Journal of Computer Security</i> , 2008, 16, 573-636.	0.8	12
38	Modular verification of security protocol code by typing. <i>ACM SIGPLAN Notices</i> , 2010, 45, 445-456.	0.2	12
39	A monadic framework for relational verification: applied to information security, program equivalence, and optimizations. , 2018, , .		12
40	miTLS: Verifying Protocol Implementations against Real-World Attacks. <i>IEEE Security and Privacy</i> , 2016, 14, 18-25.	1.2	10
41	Fully abstract compilation to JavaScript. <i>ACM SIGPLAN Notices</i> , 2013, 48, 371-384.	0.2	8
42	Gradual typing embedded securely in JavaScript. <i>ACM SIGPLAN Notices</i> , 2014, 49, 425-437.	0.2	8
43	Recalling a witness: foundations and applications of monotonic state. , 2018, 2, 1-30.		7
44	Toward Confidential Cloud Computing. <i>Queue</i> , 2021, 19, 49-76.	1.1	7
45	Cryptographically sound implementations for typed information-flow security. <i>ACM SIGPLAN Notices</i> , 2008, 43, 323-335.	0.2	5
46	Compiling Information-Flow Security to Minimal Trusted Computing Bases. <i>Lecture Notes in Computer Science</i> , 2011, , 216-235.	1.3	5
47	Self-certification. <i>ACM SIGPLAN Notices</i> , 2012, 47, 571-584.	0.2	4
48	A Top-Down Look at a Secure Message. <i>Lecture Notes in Computer Science</i> , 1999, , 122-141.	1.3	4
49	A Formal Implementation of Value Commitment. , 2008, , 383-397.		3
50	A semantics for web services authentication. <i>ACM SIGPLAN Notices</i> , 2004, 39, 198-209.	0.2	2
51	A monadic framework for relational verification: applied to information security, program equivalence, and optimizations. , 2018, , .		1