Carla RÃ fols

List of Publications by Year
in descending order

15 papers	420 citations	1040056 9 h-index	996975 15 g-index
15 all docs	15 docs citations	15 times ranked	139 citing authors

#	Article	IF	Citations
1	An Algebraic Framework for Diffie-Hellman Assumptions. Lecture Notes in Computer Science, 2013, , 129-147.	1.3	203
2	An Algebraic Framework for Diffieâ€“Hellman Assumptions. Journal of Cryptology, 2017, 30, 242-288.	2.8	58
3	The Kernel Matrix Diffie-Hellman Assumption. Lecture Notes in Computer Science, 2016, , 729-758.	1.3	36
4	Stretching Groth-Sahai: NIZK Proofs of Partial Satisfiability. Lecture Notes in Computer Science, 2015, , 247-276.	1.3	23
5	Polynomial Spaces: A New Framework for Composite-to-Prime-Order Transformations. Lecture Notes in Computer Science, 2014, , 261-279.	1.3	21
6	QA-NIZK Arguments in Asymmetric Groups: New Tools and New Constructions. Lecture Notes in Computer Science, 2015, , 605-629.	1.3	20
7	An Algebraic Framework for Universal and Updatable SNARKs. Lecture Notes in Computer Science, 2021, , 774-804.	1.3	15
8	Shorter Quadratic QA-NIZK Proofs. Lecture Notes in Computer Science, 2019, , 314-343.	1.3	15
9	New Techniques for Non-interactive Shuffle and Range Arguments. Lecture Notes in Computer Science, 2016, , 427-444.	1.3	14
10	Shorter Pairing-Based Arguments Under Standard Assumptions. Lecture Notes in Computer Science, 2019, , 728-757.	1.3	7
11	QA-NIZK Arguments of Same Opening for Bilateral Commitments. Lecture Notes in Computer Science, 2020, , 3-23.	1.3	3
12	Signatures of knowledge for Boolean circuits under standard assumptions. Theoretical Computer Science, 2022, 916, 86-110.	0.9	2
13	Dynamic group size accreditation and group discounts preserving anonymity. International Journal of Information Security, 2018, 17, 243-260.	3.4	1
14	Short tightly secure signatures for signing a vector of group elements: A new approach. Theoretical Computer Science, 2019, 795, 225-239.	0.9	1
15	Signatures of Knowledge for Boolean Circuits Under Standard Assumptions. Lecture Notes in Computer Science, 2020, , 24-44.	1.3	1