Dominique SchrÃ¶der

List of Publications by Year
in descending order

49	981	471509 17	501196 28
papers	citations	h-index	g-index

51	51	51	401
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Everlasting UC Commitments from Fully Malicious PUFs. Journal of Cryptology, 2022, 35, .	2.8	3
2	Controlling my genome with my smartphone: first clinical experiences of the PROMISE system. Clinical Research in Cardiology, 2021, , 1.	3.3	3
3	Verifiable Timed Signatures Made Practical. , 2020, , .		22
4	Threshold Password-Hardened Encryption Services. , 2020, , .		5
5	The Patient as Genomic Data Manager - Evaluation of the PROMISE App. Studies in Health Technology and Informatics, 2020, 270, 1061-1065.	0.3	1
6	Efficient Invisible and Unlinkable Sanitizable Signatures. Lecture Notes in Computer Science, 2019, , 159-189.	1.3	12
7	On Tight Security Proofs for Schnorr Signatures. Journal of Cryptology, 2019, 32, 566-599.	2.8	15
8	Group ORAM for privacy and access control in outsourced personal records. Journal of Computer Security, 2019, 27, 1-47.	0.8	2
9	Delegatable functional signatures. IET Information Security, 2018, 12, 194-206.	1.7	0
10	Efficient unlinkable sanitizable signatures from signatures with reâ€randomizable keys. IET Information Security, 2018, 12, 166-183.	1.7	2
11	Functional Credentials. Proceedings on Privacy Enhancing Technologies, 2018, 2018, 64-84.	2.8	8
12	Security of Blind Signatures Revisited. Journal of Cryptology, 2017, 30, 470-494.	2.8	7
13	Maliciously Secure Multi-Client ORAM. Lecture Notes in Computer Science, 2017, , 645-664.	1.3	16
14	Efficient Ring Signatures in the Standard Model. Lecture Notes in Computer Science, 2017, , 128-157.	1.3	21
15	Efficient Sanitizable Signatures Without Random Oracles. Lecture Notes in Computer Science, 2016, , 363-380.	1.3	21
16	Efficient Cryptographic Password Hardening Services from Partially Oblivious Commitments. , 2016, , .		16
17	Efficient Unlinkable Sanitizable Signatures from Signatures with Re-randomizable Keys. Lecture Notes in Computer Science, 2016, , 301-330.	1.3	39
18	Delegatable Functional Signatures. Lecture Notes in Computer Science, 2016, , 357-386.	1.3	16

#	Article	IF	Citations
19	Nearly Optimal Verifiable Data Streaming. Lecture Notes in Computer Science, 2016, , 417-445.	1.3	21
20	Two-Message, Oblivious Evaluation of Cryptographic Functionalities. Lecture Notes in Computer Science, 2016, , 619-648.	1.3	6
21	Liar, Liar, Coins on Fire!. , 2015, , .		54
22	Privacy and Access Control for Outsourced Personal Records. , 2015, , .		43
23	Verifiably Encrypted Signatures: Security Revisited and a New Construction. Lecture Notes in Computer Science, 2015, , 146-164.	1.3	8
24	Efficient Pseudorandom Functions via On-the-Fly Adaptation. Lecture Notes in Computer Science, 2015, , 329-350.	1.3	17
25	Foundations of Reconfigurable PUFs. Lecture Notes in Computer Science, 2015, , 579-594.	1.3	0
26	WebTrust â€“ A Comprehensive Authenticity and Integrity Framework for HTTP. Lecture Notes in Computer Science, 2014, , 401-418.	1.3	7
27	Ubic: Bridging the Gap between Digital Cryptography and the Physical World. Lecture Notes in Computer Science, 2014, , 56-75.	1.3	6
28	(Efficient) Universally Composable Oblivious Transfer Using a Minimal Number of Stateless Tokens. Lecture Notes in Computer Science, 2014, , 638-662.	1.3	14
29	Feasibility and Infeasibility of Secure Computation with Malicious PUFs. Lecture Notes in Computer Science, 2014, , 405-420.	1.3	10
30	On Tight Security Proofs for Schnorr Signatures. Lecture Notes in Computer Science, 2014, , 512-531.	1.3	31
31	Security of blind signatures under aborts and applications to adaptive oblivious transfer. Journal of Mathematical Cryptology, 2012, 5, .	0.7	2
32	History-Free Sequential Aggregate Signatures. Lecture Notes in Computer Science, 2012, , 113-130.	1.3	19
33	Uniqueness Is a Different Story: Impossibility of Verifiable Random Functions from Trapdoor Permutations. Lecture Notes in Computer Science, 2012, , 636-653.	1.3	15
34	Security of Blind Signatures Revisited. Lecture Notes in Computer Science, 2012, , 662-679.	1.3	20
35	Expedient Non-malleability Notions for Hash Functions. Lecture Notes in Computer Science, 2011, , 268-283.	1.3	7
36	Impossibility of Blind Signatures from One-Way Permutations. Lecture Notes in Computer Science, 2011, , 615-629.	1.3	13

#	Article	IF	Citations
37	Round Optimal Blind Signatures. Lecture Notes in Computer Science, 2011, , 630-648.	1.3	44
38	How to Aggregate the CL Signature Scheme. Lecture Notes in Computer Science, 2011, , 298-314.	1.3	16
39	Fair Partially Blind Signatures. Lecture Notes in Computer Science, 2010, , 34-51.	1.3	1
40	Public-Key Encryption with Non-Interactive Opening: New Constructions and Stronger Definitions. Lecture Notes in Computer Science, 2010, , 333-350.	1.3	22
41	Unlinkability of Sanitizable Signatures. Lecture Notes in Computer Science, 2010, , 444-461.	1.3	60
42	Confidential Signatures and Deterministic Signcryption. Lecture Notes in Computer Science, 2010, , 462-479.	1.3	12
43	On the Impossibility of Three-Move Blind Signature Schemes. Lecture Notes in Computer Science, 2010, , 197-215.	1.3	48
44	Redactable Signatures for Tree-Structured Data: Definitions and Constructions. Lecture Notes in Computer Science, 2010, , 87-104.	1.3	74
45	History-Free Aggregate Message Authentication Codes. Lecture Notes in Computer Science, 2010, , 309-328.	1.3	26
46	Security of Blind Signatures under Aborts. Lecture Notes in Computer Science, 2009, , 297-316.	1.3	25
47	Security of Sanitizable Signatures Revisited. Lecture Notes in Computer Science, 2009, , 317-336.	1.3	93
48	Aggregate and Verifiably Encrypted Signatures from Multilinear Maps without Random Oracles. Lecture Notes in Computer Science, 2009, , 750-759.	1.3	23
49	Security of Verifiably Encrypted Signatures and a Construction without Random Oracles. Lecture Notes in Computer Science, 2009, , 17-34.	1.3	35