Jean-Pierre Tillich

List of Publications by Year
in descending order

18	830	759233 12	1058476 14
papers	citations	h-index	g-index

19	19	19	348
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes. , 2013, , .		250
2	Quantum Serial Turbo Codes. IEEE Transactions on Information Theory, 2009, 55, 2776-2798.	2.4	84
3	Description of a Quantum Convolutional Code. Physical Review Letters, 2003, 91, 177902.	7.8	82
4	Distinguisher-based attacks on public-key cryptosystems using Reedâ€“Solomon codes. Designs, Codes, and Cryptography, 2014, 73, 641-666.	1.6	76
5	Cryptanalysis of Two McEliece Cryptosystems Based on Quasi-Cyclic Codes. Mathematics in Computer Science, 2010, 3, 129-140.	0.4	66
6	A Distinguisher for High-Rate McEliece Cryptosystems. IEEE Transactions on Information Theory, 2013, 59, 6830-6844.	2.4	57
7	A class of quantum LDPC codes: construction and performances under iterative decoding. , 2007, , .		40
8	Cryptanalysis of the McEliece Public Key Cryptosystem Based on Polar Codes. Lecture Notes in Computer Science, 2016, , 118-143.	1.3	28
9	Polynomial Time Attack on Wild McEliece Over Quadratic Extensions. IEEE Transactions on Information Theory, 2017, 63, 404-427.	2.4	28
10	Structural cryptanalysis of McEliece schemes with compact keys. Designs, Codes, and Cryptography, 2016, 79, 87-112.	1.6	26
11	A Polynomial-Time Attack on the BBCRS Scheme. Lecture Notes in Computer Science, 2015, , 175-193.	1.3	18
12	An Efficient Attack on a Code-Based Signature Scheme. Lecture Notes in Computer Science, 2016, , 86-103.	1.3	17
13	CAKE: Code-Based Algorithm for Key Encapsulation. Lecture Notes in Computer Science, 2017, , 207-226.	1.3	13
14	Quantum serial turbo-codes. , 2008, , .		8
15	Recovering Short Secret Keys of RLCE in Polynomial Time. Lecture Notes in Computer Science, 2019, , 133-152.	1.3	6
16	Trellises for stabilizer codes: Definition and uses. Physical Review A, 2006, 74, .	2.5	5
17	A family of quantum codes with performances close to the hashing bound under iterative decoding. , 2013, , .		4
18	Using Reed-Solomon codes in the (U | U + V) construction and an application to cryptography. , 2016, , .		3