

# Jean-Pierre Tillich

## List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/11608867/publications.pdf>

Version: 2024-02-01

18  
papers

830  
citations

759233

12  
h-index

1058476

14  
g-index

19  
all docs

19  
docs citations

19  
times ranked

348  
citing authors

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