

# Shai Halevi

## List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/11673533/publications.pdf>

Version: 2024-02-01

10  
papers

1,972  
citations

1162367

8  
h-index

1588620

8  
g-index

10  
all docs

10  
docs citations

10  
times ranked

781  
citing authors

#	ARTICLE	IF	CITATIONS
1	Candidate Indistinguishability Obfuscation and Functional Encryption for all Circuits. , 2013, , .		702
2	The random oracle methodology, revisited. Journal of the ACM, 2004, 51, 557-594.	1.8	614
3	Chosen-Plaintext Security from Identity-Based Encryption. SIAM Journal on Computing, 2007, 36, 1301-1328.	0.8	220
4	Universally Composable Password-Based Key Exchange. Lecture Notes in Computer Science, 2005, , 404-421.	1.0	169
5	Candidate Indistinguishability Obfuscation and Functional Encryption for All Circuits. SIAM Journal on Computing, 2016, 45, 882-929.	0.8	128
6	Smooth Projective Hashing and Two-Message Oblivious Transfer. Journal of Cryptology, 2012, 25, 158-193.	2.1	74
7	Non-Interactive Multiparty Computation Without Correlated Randomness. Lecture Notes in Computer Science, 2017, , 181-211.	1.0	24
8	Implementing BP-Obfuscation Using Graph-Induced Encoding. , 2017, , .		17
9	On the Implausibility of Differing-Inputs Obfuscation and Extractable Witness Encryption with Auxiliary Input. Algorithmica, 2017, 79, 1353-1373.	1.0	13
10	Efficient Commitment Schemes with Bounded Sender and Unbounded Receiver. Journal of Cryptology, 1999, 12, 77-89.	2.1	11