# Tatsuaki Okamoto

List of Publications by Year
in descending order



| | | | |
|---|---|---|---|
| 22 papers | 3,593 citations | 706676 14 h-index | 799663 21 g-index |
| 24 all docs | 24 docs citations | 24 times ranked | 1410 citing authors |

| # | Article | IF | Citations |
|---|---|---|---|
| 1 | Standard model leakage-resilient authenticated key exchange using inner-product extractors. Designs, Codes, and Cryptography, 2022, 90, 1059-1079. | 1.0 | 3 |
| 2 | Decentralized Attribute-Based Encryption and Signatures. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2020, E103.A, 41-73. | 0.2 | 13 |
| 3 | Fully Secure Functional Encryption with a Large Class of Relations from the Decisional Linear Assumption. Journal of Cryptology, 2019, 32, 1491-1573. | 2.1 | 3 |
| 4 | A Cryptographic Moving-Knife Cake-Cutting Protocol with High Social Surplus. Journal of Information Processing, 2015, 23, 299-304. | 0.3 | 1 |
| 5 | Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. Designs, Codes, and Cryptography, 2015, 77, 725-771. | 1.0 | 36 |
| 6 | Efficient Attribute-Based Signatures for Non-Monotone Predicates in the Standard Model. IEEE Transactions on Cloud Computing, 2014, 2, 409-421. | 3.1 | 22 |
| 7 | Secure Integration of Asymmetric and Symmetric Encryption Schemes. Journal of Cryptology, 2013, 26, 80-101. | 2.1 | 235 |
| 8 | Adaptively Attribute-Hiding (Hierarchical) Inner Product Encryption. Lecture Notes in Computer Science, 2012, , 591-608. | 1.0 | 118 |
| 9 | Fully Secure Unbounded Inner-Product and Attribute-Based Encryption. Lecture Notes in Computer Science, 2012, , 349-366. | 1.0 | 137 |
| 10 | Leakage resilient eCK-secure key exchange protocol without random oracles. , 2011, , . | | 25 |
| 11 | Achieving Short Ciphertexts or Short Secret-Keys for Adaptively Secure General Inner-Product Encryption. Lecture Notes in Computer Science, 2011, , 138-159. | 1.0 | 46 |
| 12 | Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption. Lecture Notes in Computer Science, 2010, , 62-91. | 1.0 | 795 |
| 13 | Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption. Lecture Notes in Computer Science, 2010, , 191-208. | 1.0 | 325 |
| 14 | Efficient Secure Auction Protocols Based on the Boneh-Goh-Nissim Encryption. Lecture Notes in Computer Science, 2010, , 149-163. | 1.0 | 7 |
| 15 | Hierarchical Predicate Encryption for Inner-Products. Lecture Notes in Computer Science, 2009, , 214-231. | 1.0 | 181 |
| 16 | Homomorphic Encryption and Signatures from Vector Decomposition. Lecture Notes in Computer Science, 2008, , 57-74. | 1.0 | 87 |
| 17 | RSA-OAEP Is Secure under the RSA Assumption. Lecture Notes in Computer Science, 2001, , 260-274. | 1.0 | 116 |
| 18 | Secure Integration of Asymmetric and Symmetric Encryption Schemes. Lecture Notes in Computer Science, 1999, , 537-554. | 1.0 | 610 |

| # | Article | IF | Citations |
|---|---|---|---|
| 19 | A digital multisignature scheme based on the Fiat-Shamir scheme. Lecture Notes in Computer Science, 1993, , 139-148. | 1.0 | 51 |
| 20 | Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes. , 1992, , 31-53. | | 339 |
| 21 | How to Utilize the Randomness of Zero-Knowledge Proofs. , 1990, , 456-475. | | 19 |
| 22 | A single publicâ€key authentication scheme for multiple users. Systems and Computers in Japan, 1987, 18, 14-24. | 0.2 | 5 |