# Goutam Paul

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/4866243/publications.pdf

Version: 2024-02-01

|  |  |  |  |
|---|---|---|---|
|  |  | 623734 | 677142 |
| 59 | 679 | 14 | 22 |
| papers | citations | h-index | g-index |
| 62 | 62 | 62 | 448 |
| all docs | docs citations | times ranked | citing authors |

| # | Article | IF | Citations |
|---|---|---|---|
| 1 | Cryptanalysis of quantum secure direct communication protocol with mutual authentication based on single photons and Bell states. Europhysics Letters, 2022, 138, 48001. | 2.0 | 5 |
| 2 | Grover on KATAN: Quantum Resource Estimation. IEEE Transactions on Quantum Engineering, 2022, 3, 1-9. | 4.9 | 12 |
| 3 | A graph theoretic model to understand the behavioral difference of PPCA among its paralogs towards recognition of DXCA. Journal of Biosciences, 2021, 46, 1. | 1.1 | 2 |
| 4 | Two-point FFT-based high capacity image steganography using calendar based message encoding. Information Sciences, 2021, 552, 278-290. | 6.9 | 10 |
| 5 | Bound on Efficiency of Heat Engine from Uncertainty Relation Viewpoint. Entropy, 2021, 23, 439. | 2.2 | 12 |
| 6 | Maximum violation of monogamy of entanglement for indistinguishable particles by measures that are monogamous for distinguishable particles. Physical Review A, 2021, 104, . | 2.5 | 2 |
| 7 | A complete characterization of the optimal unitary attacks in quantum cryptography with a refined optimality criteria involving the attackerâ€™s Hilbert space only. European Physical Journal D, 2021, 75, 1. | 1.3 | 0 |
| 8 | Non-commutative space engine: A boost to thermodynamic processes. Modern Physics Letters A, 2021, 36, 2150174. | 1.2 | 4 |
| 9 | Quantum cycle in relativistic non-commutative space with generalized uncertainty principle correction. Physica A: Statistical Mechanics and Its Applications, 2021, 584, 126365. | 2.6 | 3 |
| 10 | Quantum Secure Direct Communication with Mutual Authentication using a Single Basis. International Journal of Theoretical Physics, 2021, 60, 4044-4065. | 1.2 | 8 |
| 11 | Binary Black Hole Information Loss Paradox and Future Prospects. Entropy, 2020, 22, 1387. | 2.2 | 1 |
| 12 | Improving the security of â€œmeasurement-device-independent quantum communication without encryptionâ€ Science Bulletin, 2020, 65, 2048-2049. | 9.0 | 5 |
| 13 | A PVD based high capacity steganography algorithm with embedding in non-sequential position. Multimedia Tools and Applications, 2020, 79, 13449-13479. | 3.9 | 18 |
| 14 | Hyper-hybrid entanglement, indistinguishability, and two-particle entanglement swapping. Physical Review A, 2020, 102, . | 2.5 | 6 |
| 15 | Quantumâ€‰Attacksâ€‰onâ€‰HCTRâ€‰andâ€‰Itsâ€‰Variants. IEEE Transactions on Quantum Engineering, 2020, 1, 1-8. | 4.9 | 3 |
| 16 | Two efficient measurement device independent quantum dialogue protocols. International Journal of Quantum Information, 2020, 18, 2050038. | 1.1 | 8 |
| 17 | Cryptanalysis of FlexAEAD. Lecture Notes in Computer Science, 2020, , 152-171. | 1.3 | 1 |
| 18 | Differential Fault Analysis of NORX. , 2020, , . |  | 1 |

| # | Article | IF | Citations |
|---|---|---|---|
| 19 | Probing Uncertainty Relations in Non-Commutative Space. International Journal of Theoretical Physics, 2019, 58, 2619-2631. | 1.2 | 8 |
| 20 | Dimensionality distinguishers. Quantum Information Processing, 2019, 18, 1. | 2.2 | 1 |
| 21 | High Level Synthesis for Symmetric Key Cryptography. Computer Architecture and Design Methodologies, 2019, , 51-90. | 0.8 | 1 |
| 22 | Relativistic quantum heat engine from uncertainty relation standpoint. Scientific Reports, 2019, 9, 16967. | 3.3 | 19 |
| 23 | Revisiting integer factorization using closed timelike curves. Quantum Information Processing, 2019, 18, 1. | 2.2 | 1 |
| 24 | An efficient multi-bit steganography algorithm in spatial domain with two-layer security. Multimedia Tools and Applications, 2018, 77, 18451-18481. | 3.9 | 18 |
| 25 | Analysis of burn-in period for RC4 state transition. Cryptography and Communications, 2018, 10, 881-908. | 1.4 | 1 |
| 26 | A machine learning approach towards the prediction of proteinâ€“ligand binding affinity based on fundamental molecular properties. RSC Advances, 2018, 8, 12127-12137. | 3.6 | 36 |
| 27 | On data complexity of distinguishing attacks versus message recovery attacks on stream ciphers. Designs, Codes, and Cryptography, 2018, 86, 1211-1247. | 1.6 | 3 |
| 28 | Revisiting RC4 key collision: Faster search algorithm and new 22-byte colliding key pairs. Cryptography and Communications, 2018, 10, 479-508. | 1.4 | 1 |
| 29 | Quantum to classical one-way function and its applications in quantum money authentication. Quantum Information Processing, 2018, 17, 1. | 2.2 | 13 |
| 30 | Keyless dynamic optimal multi-bit image steganography using energetic pixels. Multimedia Tools and Applications, 2017, 76, 7445-7471. | 3.9 | 26 |
| 31 | Revisiting optimal eavesdropping in quantum cryptography: Optimal interaction is unique up to rotation of the underlying basis. Physical Review A, 2017, 95, . | 2.5 | 3 |
| 32 | Device-independent quantum private query. Physical Review A, 2017, 95, . | 2.5 | 30 |
| 33 | RC4-AccSuite: A Hardware Acceleration Suite for RC4-Like Stream Ciphers. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2017, 25, 1072-1084. | 3.1 | 12 |
| 34 | Strong quantum solutions in conflicting-interest Bayesian games. Physical Review A, 2017, 96, . | 2.5 | 8 |
| 35 | RunFein: a rapid prototyping framework for Feistel and SPN-based block ciphers. Journal of Cryptographic Engineering, 2016, 6, 299-323. | 1.8 | 4 |
| 36 | Proposal for quantum rational secret sharing. Physical Review A, 2015, 92, . | 2.5 | 39 |

| # | Article | IF | Citations |
|---|---|---|---|
| 37 | Proving TLS-attack related open biases of RC4. Designs, Codes, and Cryptography, 2015, 77, 231-253. | 1.6 | 5 |
| 38 | A Resilient Quantum Secret Sharing Scheme. International Journal of Theoretical Physics, 2015, 54, 398-408. | 1.2 | 6 |
| 39 | (Non-)Random Sequences from (Non-)Random Permutationsâ€"Analysis of RC4 Stream Cipher. Journal of Cryptology, 2014, 27, 67-108. | 2.8 | 48 |
| 40 | Designing stream ciphers with scalable data-widths: a case study with HC-128. Journal of Cryptographic Engineering, 2014, 4, 135-143. | 1.8 | 2 |
| 41 | CoARX. , 2013, , . |  | 21 |
| 42 | RAPID-FeinSPN: A Rapid Prototyping Framework for Feistel and SPN-Based Block Ciphers. Lecture Notes in Computer Science, 2013, , 169-190. | 1.3 | 6 |
| 43 | Optimized GPU Implementation and Performance Analysis of HC Series of Stream Ciphers. Lecture Notes in Computer Science, 2013, , 293-308. | 1.3 | 3 |
| 44 | New Results on Generalization of Roos-Type Biases and Related Keystreams of RC4. Lecture Notes in Computer Science, 2013, , 222-239. | 1.3 | 8 |
| 45 | Efficient Multi-bit Image Steganography in Spatial Domain. Lecture Notes in Computer Science, 2013, , 270-284. | 1.3 | 6 |
| 46 | Generic cryptographic weakness of k-normal Boolean functions in certain stream ciphers and cryptanalysis of grain-128. Periodica Mathematica Hungarica, 2012, 65, 205-227. | 0.9 | 23 |
| 47 | Exploring security-performance trade-offs during hardware accelerator design of stream cipher RC4. , 2012, , . |  | 4 |
| 48 | Keyless Steganography in Spatial Domain Using Energetic Pixels. Lecture Notes in Computer Science, 2012, , 134-148. | 1.3 | 16 |
| 49 | Some observations on HC-128. Designs, Codes, and Cryptography, 2011, 59, 231-245. | 1.6 | 12 |
| 50 | Attack on Broadcast RC4 Revisited. Lecture Notes in Computer Science, 2011, , 199-217. | 1.3 | 26 |
| 51 | A generic weakness of the k-normal Boolean functions exposed to dedicated algebraic attack. , 2010, , . |  | 0 |
| 52 | Nearby-Friend Discovery Protocol for Multiple Users. , 2009, , . |  | 1 |
| 53 | On biases of permutation and keystream bytes of RC4 towards the secret key. Cryptography and Communications, 2009, 1, 225-268. | 1.4 | 7 |
| 54 | On non-negligible bias of the first output byte of RC4 towards the first three bytes of the secret key. Designs, Codes, and Cryptography, 2008, 49, 123-134. | 1.6 | 31 |

| # | Article | IF | Citations |
|---|---|---|---|
| 55 | A complete characterization of the evolution of RC4 pseudo random generation algorithm. Journal of Mathematical Cryptology, 2008, 2, . | 0.7 | 15 |
| 56 | Analysis of RC4 and Proposal of Additional Layers for Better Security Margin. Lecture Notes in Computer Science, 2008, , 27-39. | 1.3 | 42 |
| 57 | On Non-randomness of the Permutation After RC4 Key Scheduling. , 2007, , 100-109. |  | 8 |
| 58 | RC4 Stream Cipher and Its Variants. , 0, , . |  | 48 |
| 59 | Differential fault analysis of NORX using variants of coupon collector problem. Journal of Cryptographic Engineering, 0, , 1. | 1.8 | 0 |