# Subhadeep Banik

List of Publications by Year
in descending order

| | | | |
|---|---|---|---|
| 55
papers | 1,001
citations | 566801
15
h-index | 454577
30
g-index |
| 60
all docs | 60
docs citations | 60
times ranked | 459
citing authors |

| # | Article | IF | Citations |
|---|---------|-----|-----------|
| 1 | Melting SNOW-V: improved lightweight architectures. Journal of Cryptographic Engineering, 2022, 12, 53-73. | 1.5 | 6 |
| 2 | Further Results on Efficient Implementations of Block Cipher Linear Layers. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2021, E104.A, 213-225. | 0.2 | 6 |
| 3 | WARP : Revisiting GFN for Lightweight 128-Bit Block Cipher. Lecture Notes in Computer Science, 2021, , 535-564. | 1.0 | 15 |
| 4 | A Deeper Look at the Energy Consumption of Lightweight Block Ciphers. , 2021, , . | | 2 |
| 5 | Six shades lighter: a bit-serial implementation of the AES family. Journal of Cryptographic Engineering, 2021, 11, 417-439. | 1.5 | 2 |
| 6 | New Attacks on LowMC Instances with a Single Plaintext/Ciphertext Pair. Lecture Notes in Computer Science, 2021, , 303-331. | 1.0 | 6 |
| 7 | Synthesis of Flexible Accelerators for Early Adoption of Ring-LWE Post-quantum Cryptography. Transactions on Embedded Computing Systems, 2020, 19, 1-17. | 2.1 | 7 |
| 8 | Energy Analysis of Lightweight AEAD Circuits. Lecture Notes in Computer Science, 2020, , 23-42. | 1.0 | 7 |
| 9 | Cryptanalysis of ForkAES. Lecture Notes in Computer Science, 2019, , 43-63. | 1.0 | 7 |
| 10 | Compact circuits for combined AES encryption/decryption. Journal of Cryptographic Engineering, 2019, 9, 69-83. | 1.5 | 16 |
| 11 | More Results on Shortest Linear Programs. Lecture Notes in Computer Science, 2019, , 109-128. | 1.0 | 15 |
| 12 | A Study of Persistent Fault Analysis. Lecture Notes in Computer Science, 2019, , 13-33. | 1.0 | 9 |
| 13 | Exploring Lightweight Efficiency of ForkAES. Lecture Notes in Computer Science, 2019, , 514-534. | 1.0 | 1 |
| 14 | On Design of Robust Lightweight Stream Cipher with Short Internal State. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2018, E101.A, 99-109. | 0.2 | 3 |
| 15 | Inverse gating for low energy encryption. , 2018, , . | | 3 |
| 16 | Theoretical Understanding of Some Conditional and Joint Biases in RC4 Stream Cipher. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2018, E101.A, 1869-1879. | 0.2 | 0 |
| 17 | Related-Key Impossible-Differential Attack on Reduced-Round Skinny. Lecture Notes in Computer Science, 2017, , 208-228. | 1.0 | 16 |
| 18 | Efficient configurations for block ciphers with unified ENC/DEC paths. , 2017, , . | | 2 |

| # | Article | IF | Citations |
|---|---------|----|-----------| 
| 19 | A scheme for conditional access-based systems using index locations of DCT coefficients. Journal of Real-Time Image Processing, 2017, 13, 363-373. | 2.2 | 1 |
| 20 | Analysis and Improvements of the Full Spritz Stream Cipher. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, E100.A, 1296-1305. | 0.2 | 1 |
| 21 | GIFT: A Small Present. Lecture Notes in Computer Science, 2017, , 321-345. | 1.0 | 221 |
| 22 | Hold Your Breath, PRIMATEs Are Lightweight. Lecture Notes in Computer Science, 2017, , 197-216. | 1.0 | 0 |
| 23 | Cryptanalysis of the Full Spritz Stream Cipher. Lecture Notes in Computer Science, 2016, , 63-77. | 1.0 | 9 |
| 24 | Adaptable AES implementation with power-gating support. , 2016, , . | | 3 |
| 25 | Conditional differential cryptanalysis of 105 round Grain v1. Cryptography and Communications, 2016, 8, 113-137. | 0.9 | 11 |
| 26 | Round gating for low energy block ciphers. , 2016, , . | | 10 |
| 27 | Low-area hardware implementations of CLOC, SILC and AES-OTR. , 2016, , . | | 5 |
| 28 | Exploring Energy Efficiency of Lightweight Block Ciphers. Lecture Notes in Computer Science, 2016, , 178-194. | 1.0 | 31 |
| 29 | Atomic-AES: A Compact Implementation of the AES Encryption/Decryption Core. Lecture Notes in Computer Science, 2016, , 173-190. | 1.0 | 17 |
| 30 | Some Proofs of Joint Distributions of Keystream Biases in RC4. Lecture Notes in Computer Science, 2016, , 305-321. | 1.0 | 5 |
| 31 | Some security results of the RC4+ stream cipher. Security and Communication Networks, 2015, 8, 4061-4072. | 1.0 | 9 |
| 32 | Differential Fault Attack against Grain Family with Very Few Faults and Minimal Assumptions. IEEE Transactions on Computers, 2015, 64, 1647-1657. | 2.4 | 32 |
| 33 | Exploring the energy consumption of lightweight blockciphers in FPGA. , 2015, , . | | 5 |
| 34 | Improved differential fault attack on MICKEY 2.0. Journal of Cryptographic Engineering, 2015, 5, 13-29. | 1.5 | 18 |
| 35 | Cryptanalysis of Two Fault Countermeasure Schemes. Lecture Notes in Computer Science, 2015, , 241-252. | 1.0 | 8 |
| 36 | How Not to Combine RC4 States. Lecture Notes in Computer Science, 2015, , 95-112. | 1.0 | 4 |

| # | ARTICLE | IF | CITATIONS |
|---|---------|----|-----------|
| 37 | Some Results on Sprout. Lecture Notes in Computer Science, 2015, , 124-139. | 1.0 | 19 |
| 38 | Midori: A Block Cipher for Low Energy. Lecture Notes in Computer Science, 2015, , 411-436. | 1.0 | 221 |
| 39 | Some Insights into Differential Cryptanalysis of Grain v1. Lecture Notes in Computer Science, 2014, , 34-49. | 1.0 | 14 |
| 40 | Cryptanalysis of the Double-Feedback XOR-Chain Scheme Proposed in Indocrypt 2013. Lecture Notes in Computer Science, 2014, , 179-196. | 1.0 | 12 |
| 41 | Random Walks based Image Segmentation Using Color Space Graphs. Procedia Technology, 2013, 10, 271-278. | 1.1 | 10 |
| 42 | A Chosen IV Related Key Attack on Grain-128a. Lecture Notes in Computer Science, 2013, , 13-26. | 1.0 | 19 |
| 43 | Improved Scan-Chain Based Attacks and Related Countermeasures. Lecture Notes in Computer Science, 2013, , 78-97. | 1.0 | 15 |
| 44 | Security Analysis of the RC4+ Stream Cipher. Lecture Notes in Computer Science, 2013, , 297-307. | 1.0 | 8 |
| 45 | A Differential Fault Attack on MICKEY 2.0. Lecture Notes in Computer Science, 2013, , 215-232. | 1.0 | 23 |
| 46 | A Differential Fault Attack on the Grain Family of Stream Ciphers. Lecture Notes in Computer Science, 2012, , 122-139. | 1.0 | 49 |
| 47 | Some Results on Related Key-IV Pairs of Grain. Lecture Notes in Computer Science, 2012, , 94-110. | 1.0 | 5 |
| 48 | A Differential Fault Attack on Grain-128a Using MACs. Lecture Notes in Computer Science, 2012, , 111-125. | 1.0 | 17 |
| 49 | A Differential Fault Attack on the Grain Family under Reasonable Assumptions. Lecture Notes in Computer Science, 2012, , 191-208. | 1.0 | 23 |
| 50 | A low power 1.8 V 4-bit 400-MHz flash ADC in 0.18/spl mu/ digital CMOS. , 2006, , . | | 9 |
| 51 | Design steps for bulk micro machined single axis silicon capacitive accelerometer with optimised device dimensions. Journal of Physics: Conference Series, 2006, 34, 722-727. | 0.3 | 7 |
| 52 | Orthros: A Low-Latency PRF. IACR Transactions on Symmetric Cryptology, 0, , 37-77. | 0.0 | 12 |
| 53 | Atom: A Stream Cipher with Double Key Filter. IACR Transactions on Symmetric Cryptology, 0, , 5-36. | 0.0 | 2 |
| 54 | Cryptanalysis of LowMC instances using single plaintext/ciphertext pair. IACR Transactions on Symmetric Cryptology, 0, , 130-146. | 0.0 | 11 |

| # | ARTICLE | IF | CITATIONS |
|---|---------|-----|-----------|
| 55 | The Area-Latency Symbiosis: Towards Improved Serial Encryption Circuits. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 239-278. | 0.0 | 1 |