

# Elena Dubrova

## List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/11854620/publications.pdf>

Version: 2024-02-01

20  
papers

302  
citations

1307594

7  
h-index

1474206

9  
g-index

21  
all docs

21  
docs citations

21  
times ranked

159  
citing authors

| #  | ARTICLE   | IF  | CITATIONS |
|----|---|-----|-----------|
| 1  | A Transformation From the Fibonacci to the Galois NLFSRs. IEEE Transactions on Information Theory, 2009, 55, 5263-5271.   | 2.4 | 67        |
| 2  | Ring oscillator physical unclonable function with multi level supply voltages. , 2012, , .  |     | 28        |
| 3  | Finding Matching Initial States for Equivalent NLFSRs in the Fibonacci and the Galois Configurations. IEEE Transactions on Information Theory, 2010, 56, 2961-2966. | 2.4 | 27        |
| 4  | CRC-PUF: A Machine Learning Attack Resistant Lightweight PUF Construction. , 2019, , .  |     | 22        |
| 5  | Compositional properties of random Boolean networks. Physical Review E, 2005, 71, 056116.   | 2.1 | 20        |
| 6  | CRC-Based Message Authentication for 5G Mobile Technology. , 2015, , .  |     | 17        |
| 7  | Synthesis of parallel binary machines. , 2011, , .  |     | 16        |
| 8  | Message Authentication Based on Cryptographically Secure CRC without Polynomial Irreducibility Test. Cryptography and Communications, 2018, 10, 383-399.            | 1.4 | 16        |
| 9  | MVLâ€”PUFs: multipleâ€”evaluated logic physical unclonable functions. International Journal of Circuit Theory and Applications, 2017, 45, 292-304.                  | 2.0 | 15        |
| 10 | Multi-Source Training Deep-Learning Side-Channel Attacks. , 2020, , .   |     | 15        |
| 11 | Synthesis of Binary Machines. IEEE Transactions on Information Theory, 2011, 57, 6890-6893.   | 2.4 | 14        |
| 12 | Generation of full cycles by a composition of NLFSRs. Designs, Codes, and Cryptography, 2014, 73, 469-486.  | 1.6 | 12        |
| 13 | A BDD-Based Approach to Constructing LFSRs for Parallel CRC Encoding. , 2012, , .   |     | 8         |
| 14 | Area-efficient high-coverage LBIST. Microprocessors and Microsystems, 2014, 38, 368-374.  | 2.8 | 7         |
| 15 | An Algorithm for Constructing a Minimal Register with Non-linear Update Generating a Given Sequence. , 2014, , .  |     | 6         |
| 16 | Temperature aware phase/frequency detector-basec RO-PUFs exploiting bulk-controlled oscillators. , 2017, , .  |     | 4         |
| 17 | On Constructing Secure and Hardware-Efficient Invertible Mappings. , 2016, , .  |     | 2         |
| 18 | Lightweight Message Authentication for Constrained Devices. , 2018, , .   |     | 2         |

| #  | ARTICLE  | IF | CITATIONS |
|----|--|----|-----------|
| 19 | Evaluation of alternative LBIST flows: A case study. , 2014, , .   |    | 1         |
| 20 | Synthesis of power- and area-efficient binary machines for incompletely specified sequences. , 2014, , . |    | 1         |