Advances in Model and Data Engineering in the Digitalization Era : MEDI 2021 International Workshops : DETECT, SIAS, CSMML, BIOC, HEDA, Tallinn, Estonia, June 21–23, 2021 : proceedings
2021 https://doi.org/10.1007/978-3-030-87657-9

Black-box separations and their adaptability to the non-uniform model
Buldas, Ahto; Niitsoo, Margus Information security and privacy : 18th Australasian Conference, ACISP 2013, Brisbane, Australia, July 1-3, 2013 : proceedings 2013 / p. 152-167 https://doi.org/10.1007/978-3-642-39059-3_11 Conference Proceedings at Scopus Article at Scopus

Electronic Voting : 5th International Joint Conference, E-Vote-ID 2020, Bregenz, Austria, October 6–9, 2020 : proceedings
2020 https://doi.org/10.1007/978-3-030-60347-2

LiD-CAT: A lightweight detector for cache ATtacks
Reinbrecht, Cezar; Hamdioui, Said; Taouil, Mottaqiallah; **Niazmand, Behrad**; **Ghasempouri, Tara**; **Raik, Jaan**; Sepulveda, Johanna 2020 IEEE European Test Symposium (ETS) : ETS 2020, May 25-29, 2020 Tallinn, Estonia : proceedings 2020 / 6 p. : ill https://doi.org/10.1109/ETS48528.2020.9131603

Martínez-Guerra, Rafael; Montesinos-García, Juan Javier; Flores-Flores, Juan Pablo. Encryption and decryption algorithms for plain text and images using fractional calculus : [review)
Henno, Jaak Zentralblatt MATH 2024 / 1 p. https://zbmath.org/1531.94002

Mittelbach, Arno; Fischlin, Marc.The theory of hash functions and random oracles. An approach to modern cryptography.
Henno, Jaak zbMATH Open 2022 / 1 p. https://zbmath.org/1490.94001

Multiplierless design of high-speed very large constant multiplications
Aksoy, Levent; Roy, Debapriya Basu; **Imran, Malik**; **Pagliarini, Samuel Nascimento** 2024 29th Asia and South Pacific Design Automation Conference (ASP-DAC 2024) 2024 / p. 957-962 https://doi.org/10.1109/ASP-DAC58780.2024.10473954

Multiplierless design of very large constant multiplications in cryptography
Aksoy, Levent; Roy, Debapriya Basu; **Imran, Malik**; Karl, Patrick; **Pagliarini, Samuel Nascimento** IEEE Transactions on Circuits and Systems II : Express Briefs 2022 / p. 4503-4507 https://doi.org/10.1109/TCSII.2022.3191662 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

The once-only principle : The TOOP project
2021 https://doi.org/10.1007/978-3-030-79851-2

Zarebnia, M.; Parvaz, R. Image encryption algorithm by fractional based chaotic system and framelet transform
Henno, Jaak zbMATH Open 2022 / 1 p. https://zbmath.org/07577308

Zero-knowledge in EasyCrypt
Firsov, Denis; Unruh, Dominique 2023 IEEE 36th Computer Security Foundations Symposium : CSF 2023 : proceedings 2023 / 16 p. https://doi.org/10.1109/CSF57540.2023.00015

Unsatisfiability of comparison-based non-malleability for commitments
Firsov, Denis; Laur, Sven; **Zhuchko, Ekaterina** Theoretical Aspects of Computing - ICTAC 2022 : 19th International Colloquium, Tbilisi, Georgia, September 27-30, 2022 : proceedings 2022 / p. 188–194 https://doi.org/10.1007/978-3-031-17715-6_13 Conference Proceedings at Scopus Article at Scopus