An area aware accelerator for elliptic curve point multiplication
Imran, Malik; **Pagliarini, Samuel Nascimento**; Rashid, Muhammad Haroon 27th IEEE International Conference on Electronics Circuits and Systems, (ICECS) 2020, Glasgow, UK, Virtual Conference, November 23-25, 2020 : proceedings 2020 / 4 p
https://doi.org/10.1109/ICECS49266.2020.9294908

Areeba : an area efficient binary huff-curve architecture
Sajid, Asher; Rashid, Muhammad; Jamal, Sajjad Shaukat; **Imran, Malik**; Alotaibi, Saud S.; Sinky, Mohammed H. Electronics (Switzerland) 2021 / art. 1490 https://doi.org/10.3390/electronics10121490 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Design space exploration of SABER in 65nm ASIC
Imran, Malik; **Almeida, Felipe**; **Raik, Jaan**; Basso, Andrea; Roy, Sujoy Sinha; **Pagliarini, Samuel Nascimento** ASHES '21 : proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security 2021 / p. 85-90
https://doi.org/10.1145/3474376.3487278

Elliptic-curve crypto processor for RFID applications
Rashid, Muhammad; Jamal, Sajjad Shaukat; Khan, Sikandar Zulqarnain; Alharbi, Adel R.; Aljaedi, Amer; **Imran, Malik** Applied Sciences (Switzerland) 2021 / art. 7079 https://doi.org/10.3390/app11157079 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Evaluating NTT/INTT implementation styles for post-quantum cryptography
Imran, Malik; Khan, Safiullah; Khalid, Ayesha; Rafferty, Ciara; Ali Shah, Yasir; Pagliarini, Samuel; Rashid, Muhammad; O'Neill, Maire IEEE Embedded Systems Letters 2024 / p. 485 - 488 https://doi.org/10.1109/LES.2024.3410516 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

An experimental study of building blocks of lattice-based NIST post-quantum cryptographic algorithms
Imran, Malik; **Abideen, Zain Ul**; **Pagliarini, Samuel Nascimento** Electronics 2020 / art. 1953, 26 p. : ill
https://doi.org/10.3390/electronics9111953 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

A 4-Stage pipelined architecture for point multiplication of binary huff curves
Rashid, Muhammad Imran; **Imran, Malik**; Jafri, Atif Raza; Mehmood, Zahid Journal of circuits, systems, and computers 2020 / art. 2050179 https://doi.org/10.1142/S0218126620501790

Hardware realization of lattice-based post-quantum cryptography = Võrel põhinev post-kvant-krüptograafia riistvaraline realisatsioon
Imran, Malik 2023 https://www.ester.ee/record=b5571216*est https://doi.org/10.23658/taltech.33/2023 https://digikogu.taltech.ee/et/Item/75aeb070-cb8b-4511-beaf-cbea3fca147d https://www.ester.ee/record=b5571216*est

High-speed design of postquantum cryptography with optimized hashing and multiplication
Imran, Malik; Aikata, Aikata; Roy, Sujoy Sinha; **Pagliarini, Samuel Nascimento** IEEE Transactions on Circuits and Systems II : Express Briefs 2023 / p. 847-851 : ill https://doi.org//10.1109/TCSII.2023.3273821 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

High-speed SABER key encapsulation mechanism in 65nm CMOS
Imran, Malik; **Almeida, Felipe**; Basso, Andrea; Roy, Sujoy Sinha; **Pagliarini, Samuel Nascimento** Journal of cryptographic engineering 2023 / p. 461-471 : ill https://doi.org/10.1007/s13389-023-00316-2 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

KaLi: a crystal for post-quantum security using kyber and dilithium
Aikata, Aikata; Mert, Ahmet Can; **Imran, Malik**; **Pagliarini, Samuel Nascimento**; Roy, Sujoy Sinha IEEE Transactions on Circuits and Systems I : regular papers 2023 / p. 747–758 https://doi.org/10.1109/TCSI.2022.3219555 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

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

An open-source library of large integer polynomial multipliers
Imran, Malik; **Abideen, Zain Ul**; **Pagliarini, Samuel Nascimento** 24th International Symposium on Design and Diagnostics of Electronic Circuits and Systems, Vienna, Austria, April 7-9 2021 2021 / p. 145-150 : ill
https://doi.org/10.1109/DDECS52668.2021.9417065

Ransomware attack as Hardware Trojan : a feasibility and demonstration study
Almeida, Felipe; **Imran, Malik**; **Raik, Jaan**; **Pagliarini, Samuel Nascimento** IEEE Access 2022 / p. 44827-44839
https://doi.org/10.1109/ACCESS.2022.3168991 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Side-channel Trojan insertion - a practical foundry-side attack via ECO
Perez, Tiago Diadami; **Imran, Malik**; **Vaz, Pablo**; **Pagliarini, Samuel Nascimento** 2021 IEEE International Symposium on Circuits and Systems (ISCAS), Daegu, Korea, May 22-28, 2021 : proceedings 2021 / 5 p. : ill https://doi.org/10.1109/ISCAS51556.2021.9401481 Conference Proceedings at Scopus Article at Scopus Article at WOS

A systematic study of lattice-based NIST PQC algorithms : from reference implementations to hardware accelerators
Imran, Malik; **Abideen, Zain Ul**; **Pagliarini, Samuel Nascimento** arXiv.org 2020 / 36 p. : ill

A versatile and flexible multiplier generator for Large integer polynomials
Imran, Malik; **Abideen, Zain Ul**; **Pagliarini, Samuel Nascimento** Journal of hardware and systems security 2023 / p. 55–71
https://doi.org/10.1007/s41635-023-00134-2