

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>

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](#)