Advanced Hardware Protection Mechanisms : A Study on Logic Locking and Circuit Obfuscation Techniques [Võrguteavik] = Täiustatud riistvara kaitsemehhanismid : uuring loogikalukustamise ja hägustamise tehnikate kohta
Costa de Almeida, Antonio Felipe 2025 https://www.ester.ee/record=b5752171*est https://digikogu.taltech.ee/et/Item/9840306f-39a2-4ac7-b275-9a841a75857b https://doi.org/10.23658/taltech.42/2025

An overview of FPGA-inspired obfuscation techniques
Abideen, Zain Ul; **Gokulanathan, Sumathi**; **Aljafar, Muayad J.**; **Pagliarini, Samuel Nascimento** ACM computing surveys 2024 / art. 299, 35 p. : ill https://doi.org/10.1145/3677118 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

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

Benchmarking advanced security closure of physical layouts
Eslami, Mohammad; Knechtel, Johann; Sinanoglu, Ozgur; Karri, Ramesh; **Pagliarini, Samuel Nascimento** ISPD '23 : proceedings of the 2023 International Symposium on Physical Design 2023 / p. 256-264 https://doi.org/10.1145/3569052.3578924 https://dl.acm.org/doi/pdf/10.1145/3569052.3578924

CAC 2.0 : a corrupt and correct logic locking technique resilient to structural analysis attacks
Aksoy, Levent; Yasin, Muhammad; **Pagliarini, Samuel Nascimento** 2024 IEEE 25th Latin American Test Symposium (LATS) : 9-12 April 2024 (2024) 2024 https://doi.org/10.1109/LATS62223.2024.10534592 Article at Scopus

CAC 2.0 : a corrupt and correct logic locking technique resilient to structural analysis attacks
Aksoy, Levent; Yasin, Muhammad; **Pagliarini, Samuel Nascimento** arXiv.org 2024 / 6 p. : ill https://doi.org/10.48550/arXiv.2401.07142

Chip-to-Chip authentication method based on SRAM PUF and public key cryptography
Karageorgos, Ioannis; Isgenc, Mehmet Meric; **Pagliarini, Samuel Nascimento**; Pileggi, Larry Journal of hardware and systems security 2019 / p. 382–396 : ill https://doi.org/10.1007/s41635-019-00080-y

Design obfuscation versus test
Farahmandi, Farimah; Sinanoglu, Ozgur; Blanton, Ronald; **Pagliarini, Samuel Nascimento** 2020 IEEE European Test Symposium (ETS) : ETS 2020, May 25 - 29, 2020, Tallinn, Estonia 2020 / 10 p https://doi.org/10.1109/ETS48528.2020.9131590

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

Evaluating architectural, redundancy, and implementation strategies for radiation hardening of FinFET integrated circuits
Pagliarini, Samuel Nascimento; Benites, Luis; Martins, Mayler; Rech, Paolo; Kastensmidt, Fernanda IEEE transactions on nuclear science 2021 / p. 1045-1053 https://doi.org/10.1109/TNS.2021.3070643 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

From FPGAs to obfuscated eASICs : design and security trade-offs
Abideen, Zain Ul; **Perez, Tiago Diadami**; **Pagliarini, Samuel Nascimento** IEEE Asian Hardware-Oriented Security and Trust (AsianHOST) 2021 / p. 1-4 https://doi.org/10.1109/AsianHOST53231.2021.9699758

From virtual characterization to test-chips : DFM analysis through pattern enumeration
Martins, Mayler G.A.; **Pagliarini, Samuel Nascimento**; Isgenc, Mehmet Meric; Pileggi, Larry IEEE transactions on computer-aided design of integrated circuits and systems 2020 / p. 520-532 https://doi.org//10.1109/TCAD.2018.2889772

G-GPU : a fully-automated generator of GPU-like ASIC accelerators
Perez, Tiago Diadami; Gonçalves, Marcio M.; Gobatto, Leonardo; Brandalero, Marcelo; Azambuja, Jose Rodrigo; **Pagliarini, Samuel Nascimento** 2022 Design, Automation & Test in Europe Conference & Exhibition (DATE 2022) : proceedings 2022 / p. 544 - 547 https://doi.org/10.23919/DATE54114.2022.9774758

Hardware obfuscation of digital FIR filters
Aksoy, Levent; Hepp, Alexander; Baehr, Johanna; **Pagliarini, Samuel Nascimento** 2022 25th International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS) : Prague, Czech Republic : April 6-8, 2022 : proceedings 2022 / p. 68-73 https://doi.org/10.48550/arXiv.2202.10022 https://doi.org/10.1109/DDECS54261.2022.9770141

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

Hardware trojan insertion in finalized layouts : from methodology to a silicon demonstration
Perez, Tiago Diadami; **Pagliarini, Samuel Nascimento** IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 2023 / p. 2094-2107 https://doi.org/10.1109/TCAD.2022.3223846 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Hardware Trojans for confidence reduction and misclassifications on neural networks
Grailoo, Mahdieh; **Leier, Mairo**; **Pagliarini, Samuel Nascimento** Proceedings Of The Twenty Third International Symposium On Quality Electronic Design (ISQED 2022) 2022 / art. 180541, p. 230-235 https://doi.org/10.1109/ISQED54688.2022.9806246

High-level intellectual property obfuscation via decoy constants
Aksoy, Levent; Nguyen, Quang-Linh; **Almeida, Felipe**; **Raik, Jaan**; Flottes, Marie-Lise; Dupuis, Sophie; **Pagliarini, Samuel Nascimento** 2021 IEEE 27th International Symposium on On-Line Testing and Robust System Design (IOLTS) : Torino, Italy, 28-30 June 2021 2021 / p. 1-7 https://doi.org/10.1109/IOLTS52814.2021.9486714

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

Hybrid protection of digital FIR filters
Aksoy, Levent; Nguyen, Quang-Linh; **Almeida, Felipe**; **Raik, Jaan**; Flottes, Marie-Lise; Dupuis, Sophie; **Pagliarini, Samuel Nascimento** IEEE transactions on Very Large Scale Integration (VLSI) Systems 2023 / p. 812-825 : ill https://doi.org/10.1109/TVLSI.2023.3253641 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Impact of orientation on the bias of SRAM-based PUFs
Abideen, Zain Ul; Wang, Rui; **Perez, Tiago Diadami**; Schrijen, Geert-Jan; **Pagliarini, Samuel Nascimento** arXiv.org 2023 / 7 p. : ill https://doi.org/10.48550/arXiv.2308.06730

Impact of orientation on the bias of SRAM-based PUFs
Abideen, Zain Ul; Wang, Rui; **Perez, Tiago Diadami**; Schrijen, Geert-Jan; **Pagliarini, Samuel Nascimento** IEEE design & test 2024 / p. 14-20 https://doi.org/10.1109/MDAT.2023.3322621 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

KRATT : QBF-assisted removal and structural analysis attack against logic locking
Aksoy, Levent; Yasin, Muhammad; **Pagliarini, Samuel Nascimento** arXiv.org 2023 / 7 p. : ill https://doi.org/10.48550/arXiv.2311.05982

Latch-Based logic locking
Sweeney, J.; Mohammed Zackriya, V.; **Pagliarini, Samuel Nascimento**; Pileggi, Larry Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2020 2020 / p. 132−141 : ill https://doi.org/10.1109/HOST45689.2020.9300256

Latest trends in hardware security and privacy
Di Natale, Giorgio; Regazzoni, Francesco; Albanese, Vincent; Lhermet, Frank; Loisel, Yann; Sensaoui, Abderrahmane; **Pagliarini, Samuel Nascimento** 33rd IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT) : ESA-ESRIN, Italy (On-line Virtual Event),October 19–21, 2020 2020 / 4 p. : ill https://doi.org/10.1109/DFT50435.2020.9250816

Leveraging FPGA Reconfigurability as an Obfuscation Asset = FPGA ümberkonfigureeritavuse rakendamine hägustamise vahendina
Abideen, Zain Ul 2024 https://digikogu.taltech.ee/et/Item/660d923b-44d2-4993-898f-324ab2088199 https://www.ester.ee/record=b5649944*est https://doi.org/10.23658/taltech.1/2024

Leveraging layout-based effects for locking analog ICs
Aljafar, Muayad J.; Azais, Florence; Flottes, Marie-Lise; **Pagliarini, Samuel Nascimento** ASHES'22: Proceedings of the 2022 Workshop on Attacks and Solutions in Hardware Security 2022 / p. 5-13 https://doi.org/10.1145/3560834.3563826

Logic IP for low-cost IC design in advanced CMOS nodes
Isgenc, Mehmet Meric; Martins, Mayler G.A.; Zackriya, V. Mohammed; **Pagliarini, Samuel Nascimento**; Pileggi, Larry IEEE Transactions on Very Large Scale Integration (VLSI) Systems 2020 / p. 585-595 https://doi.org//10.1109/TVLSI.2019.2942825

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

Obfuscating the hierarchy of a digital IP
Basiashvili, Giorgi; **Abideen, Zain Ul**; **Pagliarini, Samuel Nascimento** Embedded Computer Systems : Architectures, Modeling, and Simulation :22nd International Conference, SAMOS 2022, Samos, Greece, July 3-7, 2022 : proceedings 2022 / p. 303-314 https://doi.org/10.1007/978-3-031-15074-6_28 Conference proceedings at Scopus Article at Scopus Conference proceedings at WOS Article at WOS

On the use of defensive schemes for hardware security = Kaitseskeemid riistvara turvalisuse tagamiseks
Eslami, Mohammad 2024 https://www.ester.ee/record=b5701420*est https://doi.org/10.23658/taltech.53/2024 https://digikogu.taltech.ee/et/Item/068530be-4810-4489-9604-fb838d298b45

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

An overview of FPGA-inspired obfuscation techniques
Abideen, Zain Ul; **Gokulanathan, Sumathi**; **Aljafar, Muayad J.**; **Pagliarini, Samuel Nascimento** arXiv.org 2023 / 30 p. : ill https://doi.org/10.48550/arXiv.2305.15999

A pragmatic methodology for blind hardware trojan insertion in finalized layouts
Hepp, Alexander; **Perez, Tiago Diadami**; **Pagliarini, Samuel Nascimento**; Sigl, Georg ICCAD '22: Proceedings of the 41st IEEE/ACM International Conference on Computer-Aided Design 2022 / art. 69, p. 1-9 : ill https://doi.org/10.1145/3508352.3549452 Conference Proceedings at Scopus Article at Scopus Article at WOS

Preventing distillation-based attacks on Neural Network IP
Grailoo, Mahdieh; **Abideen, Zain Ul**; **Leier, Mairo**; **Pagliarini, Samuel Nascimento** arXiv.org 2022 / 7 p. : ill https://doi.org/10.48550/arXiv.2204.00292

A probabilistic synapse with strained MTJs for Spiking Neural Networks
Pagliarini, Samuel Nascimento; Bhuin, Sudipta; Isgenc, Mehmet Meric; Biswas, Ayan Kumar; Pileggi, Larry IEEE Transactions on Neural Networks and Learning Systems 2020 / p. 1113-1123 : ill https://doi.org/10.1109/TNNLS.2019.2917819

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

RESAA: A Removal and Structural Analysis Attack Against Compound Logic Locking
Almeida, Felipe; **Aksoy, Levent**; **Pagliarini, Samuel Nascimento** IEEE Transactions on Very Large Scale Integration (VLSI) Systems 2025 / p. 1348-1360 https://doi.org//10.1109/TVLSI.2025.3534658

RESAA: A Removal and Structural Analysis Attack Against Compound Logic Locking : [preprint]
Almeida, Felipe; **Aksoy, Levent**; **Pagliarini, Samuel Nascimento** arXiv.org 2025 / 12 p. : ill https://doi.org/10.48550/arXiv.2409.16959

Resynthesis-based attacks against logic locking
Almeida, Felipe; **Aksoy, Levent**; Nguyen, Quang-Linh; Dupuis, Sophie; Flottes, Marie-Lise; **Pagliarini, Samuel Nascimento** 2023 24th International Symposium on Quality Electronic Design (ISQED) : San Francisco, 5-7 April 2023 2023 / 8 p. : ill https://doi.org/10.1109/ISQED57927.2023.10129403 Article at Scopus Article at WOS

Reusing verification assertions as security checkers for Hardware Trojan detection
Eslami, Mohammad; **Ghasempouri, Tara**; **Pagliarini, Samuel Nascimento** 2022 23rd International Symposium on Quality Electronic Design (ISQED), Santa Clara, CA, USA : 06-07 April 2022 2022 / p. 1-6 : ill
https://doi.org/10.1109/ISQED54688.2022.9806292

SALSy : security-aware layout synthesis
Eslami, Mohammad; **Perez, Tiago Diadami**; **Pagliarini, Samuel Nascimento** arXiv.org 2024 / 13 p. : ill
https://doi.org/10.48550/arXiv.2308.06201

SCARF : securing chips with a robust framework against fabrication-time hardware trojans
Eslami, Mohammad; **Ghasempouri, Tara**; **Pagliarini, Samuel Nascimento** IEEE Transactions on Computers 2024 / p. 2761-2775 https://doi.org/10.1109/TC.2024.3449082 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

SCARF : securing chips with a robust framework against fabrication-time hardware Trojans : preprint
Eslami, Mohammad; **Ghasempouri, Tara**; **Pagliarini, Samuel Nascimento** arXiv.org 2024 / 14 p. : ill
https://doi.org/10.48550/arXiv.2402.12162

A security-aware and LUT-based CAD flow for the physical synthesis of hASICs
Abideen, Zain Ul; **Perez, Tiago Diadami**; Martins, Mayler; **Pagliarini, Samuel Nascimento** IEEE transactions on computer-aided design of integrated circuits and systems 2023 / p. 3157-3170 : ill https://doi.org/10.1109/TCAD.2023.3244879 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Security-aware physical synthesis of integrated circuits = Integraallülituste turvateadlik füüsiline süntees
Perez, Tiago Diadami 2023 https://doi.org/10.23658/taltech.4/2023 https://digikogu.taltech.ee/et/Item/440f41fd-0950-4b5c-8e47-4f75a754cdae https://www.ester.ee/record=b5536743*est

Side-channel attacks on triple modular redundancy schemes
Almeida, Felipe; **Aksoy, Levent**; **Raik, Jaan**; **Pagliarini, Samuel Nascimento** 2021 IEEE 30th Asian Test Symposium ATS 2021 : proceedings 2021 / p. 79-84 : ill https://doi.org/10.1109/ATS52891.2021.00026 Conference Proceedings at Scopus Article at Scopus Article at WOS

A side-channel hardware trojan in 65nm CMOS with 2μW precision and multi-bit leakage capability
Perez, Tiago Diadami; **Pagliarini, Samuel Nascimento** 2022 27th Asia and South Pacific Design Automation Conference (ASP-DAC) : 17-20 January 2022 : Taipei, Taiwan 2022 / p. 9-10 : ill https://doi.org/10.1109/ASP-DAC52403.2022.9712490

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

Split-chip design to prevent IP reverse engineering
Pagliarini, Samuel Nascimento; Sweeney, Joseph; Mai, Ken; Blanton, Shawn; Mitra, Subhasish; Pileggi, Larry IEEE Design and Test 2020 / p. 109-118 https://doi.org/10.1109/MDAT.2020.3033255 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

A survey on split manufacturing : attacks, defenses, and challenges
Perez, Tiago Diadami; **Pagliarini, Samuel Nascimento** IEEE Access 2020 / p. 184013-184035
https://doi.org/10.1109/ACCESS.2020.3029339 Journal metrics at Scopus Article at Scopus Journal metrics at WOS 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

Toimiva digiühiskonna tagavad usaldusväärne tarkvara, turvaline riistvara ning energiasäästlikud ja nutikad asjad
Härmat, Karin Mente et Manu 2022 / lk. 32-33 https://www.ester.ee/record=b1242496*est

A tutorial on design obfuscation : from transistors to systems
Pagliarini, Samuel Nascimento 2021 IEEE 22nd Latin American Test Symposium (LATS), Punta del Este, Uruguay, 27-29 October 2021 2021 / 3 p. : ill https://doi.org/10.1109/LATS53581.2021.9651741

Uued inimesed TalTechis
Dashtimanesh, Abbas; **Gerstlberger, Wolfgang Dieter**; **Hoffmann, Thomas**; **Männik, Aarne**; **Niidu, Allan**; **Pagliarini, Samuel Nascimento**; **Sobocinski, Pawel Maria**; **Treffner, Ivar** Mente et Manu 2019 / lk. 26-32 : fot https://www.ester.ee/record=b1242496*est

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

Võitlus kiipides varitsevate troojalastega tõstab Eesti teadlased kilbile
Härmat, Karin err.ee 2023 Võitlus kiipides varitsevate troojalastega tõstab Eesti teadlased kilbile