

A user interface for a game-based protocol verification tool

Laud, Peeter; **Tšahhirov, Ilja** Formal Aspects in Security and Trust : 6th International Workshop : FAST 2009, Eindhoven, Netherlands, November 5-6, 2009 : Revised Selected Papers 2010 / p. 263-278 : ill <https://research.cyber.ee/~peeter/research/fast09.pdf>

A VLSI implementation of RSA and IDEA encryption engine

Buldas, Ahto; Põldre, Jüri Proceedings [of the] 15th NORCHIP Conference, Tallinn, 10-11 November 1997 1997 / p. 281-288: ill

AES : uue krüptostandardi otsinguil

Praust, Valdo Arvutimaailm 1999 / 4, lk. 60-62: ill

An enhanced lightweight authentication scheme for secure access to cloud data

Hammami, Hamza; Obaidat, Mohammad S.; **Ben Yahia, Sadok** Proceedings of the 17th International Joint Conference on e-Business and Telecommunications, ICETE 2020 - Volume 3: ICE-B, Lieusaint, Paris, France, July 8-10, 2020 2020 / p. 110-117 <https://doi.org/10.5220/0009824301100117>

Analyzing and investigating encrypted traffic for social media application Instagram

Iqbal, Hameed; Ahmad, Rizwan; Ahmed, Waqas; Qazi, Shams; **Alam, Muhammad Mahtab** 2022 18th Biennial Baltic Electronics Conference (BEC) 2022 / 6 p. : ill <https://doi.org/10.1109/BEC56180.2022.9935603>

Applebaum, Benny. Cryptography in constant parallel time. Information Security and Cryptography. Berlin: Springer (ISBN 978-3-642-17366-0/hbk; 978-3-642-17367-7/ebook). xvi, 193 p. (2014) : [review]

Henno, Jaak Zentralblatt MATH 2014 / [1] p

Application of dependency graphs to security protocol analysis

Tšahhirov, Ilja; Laud, Peeter Trustworthy global computing 2008 / p. 294-311 : ill https://link.springer.com/chapter/10.1007/978-3-540-78663-4_20

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](#)

Attribute-based encryption for named data networking

Lenin, Aleksandr; Laud, Peeter ICN '21 : Proceedings of the 8th ACM Conference on Information-Centric Networking 2021 / p. 118–120 <https://doi.org/10.1145/3460417.3483371>

Beimel, A.; Haitner, I.; Makriyannis, N.; Omri, E. Tighter bounds on multiparty coin flipping via augmented weak martingales and differentially private sampling : [review]

Henno, Jaak zbMATH Open 2022 / 1 p. <https://doi.org/10.1137/18M1210782>

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

BLT+L : efficient signatures from timestamping and endorsements

Firsov, Denis; Lakk, Henri; Laur, Sven; Truu, Ahto Proceedings of the 18th International Conference on Security and Cryptography - SECRYPT. Vol. 1 2021 / p. 75-86 <https://doi.org/10.5220/0010530000750086>

Bounded pre-image awareness and the security of hash-tree keyless signatures

Buldas, Ahto; Laanoja, Risto; Laud, Peeter; Truu, Ahto Provable security : 8th International Conference, ProvSec 2014, Hong Kong, China, October 9-10, 2014 : proceedings 2014 / p. 130-145 : ill

Brier, Éric; Ferradi, Houda; Joye, Marc; Naccache, David. New number-theoretic cryptographic primitives : [review]

Henno, Jaak Zentralblatt MATH 2020 / 1 p <https://www.zbmath.org/?q=an:07342049>

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>

Creating randomness with games

Henno, Jaak; Jaakkola, Hannu; Mäkelä, Jukka Acta Polytechnica Hungarica : journal of applied sciences at Budapest Polytechnic Hungary 2019 / p. 193-212 : ill http://acta.uni-obuda.hu/Henno_Jaakkola_Makela_96.pdf <https://doi.org/10.12700/APH.16.9.2019.9.11> [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>

Developing requirements for the new encryption mechanisms in the Estonian eID infrastructure

Oruaas, Mart; Willemson, Jan Databases and Information Systems : 14th International Baltic Conference, DB&IS 2020, Tallinn, Estonia, June 16-19, 2020 : Proceedings 2020 / p. 13-20 https://doi.org/10.1007/978-3-030-57672-1_2

Does secure time-stamping imply collision-free hash functions

Buldas, Ahto; Jürgenson, Aivo Info- ja kommunikatsioonitehnoloogia doktorikooli IKTDK kolmanda aastakonverentsi artiklite kogumik : 25.-26. aprill 2008, Voore külalistemaja 2008 / p. 59-63 : ill

Does secure time-stamping imply collision-free hash functions?

Buldas, Ahto; Jürgenson, Aivo Lecture notes in computer science 2007 / p. 138-150

Eestis arendatud plokiahel soovib saada maailmaturu liidriks

Rumm, Hannes Eesti Ekspress 2023 / lk. 30-33 <https://dea.digar.ee/article/eestiekspress/2023/05/10/13.6>

Efficiency bounds for adversary constructions in black-box reductions

Buldas, Ahto; Jürgenson, Aivo; Niitsoo, Margus Information Security and Privacy : 14th Australasian Conference : ACISP 2009 : Brisbane, Australia, July 1-3, 2009 : proceedings 2009 / p. 264-275 https://link.springer.com/chapter/10.1007/978-3-642-02620-1_19

eGovernment services : How to develop them, how to manage them?

Kalja, Ahto; Kindel, Kristiina; Kivi, Riina; **Robal, Tarmo** Proceedings of PICMET'07 : Management of Converging Technologies : Portland, OR, USA, 5-9. August 2007 2007 / p. 2795-2798 <https://ieeexplore.ieee.org/document/4349620>

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>

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](#)

Euler, sudoku ja küberrünnakud

Võhandu, Leo A & A 2007 / 6, lk. 45-53 https://artiklid.elnet.ee/record=b1021181*est

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 fault-resistant architecture for AES S-box architecture

Taheri, Mahdi; Sheikhpour, Saeideh; Ansari, Mohammad Saeed; Mahani, Ali Journal of Applied Research in Electrical Engineering 2021 / p. 86-92 <https://doi.org/10.22055/jaree.2021.36230.1020>

A foundation for ledger structures

Nester, Chad Mitchell 2nd International Conference on Blockchain Economics, Security and Protocols : Tokenomics 2020, October 26–27, 2020, Toulouse, France 2021 / art. 7, p. 7:1–7:31 <https://doi.org/10.4230/OASlcs.Tokenomics.2020.7>

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>

The future of law and eTechnologies

2016 <http://dx.doi.org/10.1007/978-3-319-26896-5> https://www.ester.ee/record=b4601923*est

Ghinea, Diana; Goyal, Vipul; Liu-Zhang, Chen-Da. Round-optimal Byzantine agreement : [review]

Henno, Jaak zbMATH Open 2022 / p. 1 <https://zbmath.org/pdf/1497.94091.pdf>

Hardware realization of lattice-based post-quantum cryptography = Võrel põhinev post-kvant-krüptograafia riistvaraline realiseatsioon

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>

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>

Image encryption using fractional singular chaotic systems : an extended Kalman filtering approach

Nosrati, Komeil; Belikov, Juri; Tepljakov, Aleksei; Petlenkov, Eduard 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET) 2022 / 6 p. : ill <https://doi.org/10.1109/ICECET55527.2022.9873484>

Infosüsteemide turve

Hanson, Vello; **Buldas, Ahto; Praust, Valdo** 1998 https://www.ester.ee/record=b1191671*est

Keyless signature infrastructure and PKI : hash-tree signatures in pre- and post-quantum world

Buldas, Ahto; Laanoja, Risto; Truu, Ahto International journal of services technology and management 2017 / p. 117-130 : ill <http://dx.doi.org/10.1504/IJSTM.2017.10002708>

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>

Krüptograafia kõrgtehnoloogia: kiip Clipper

Praust, Valdo Arvutimaailm 1994 / 10, lk. 48-50: ill

Krüptograafiapoliitika arutelu Pariisis

Praust, Valdo Arvutimaailm 1998 / 2, lk. 8-9: ill

Krüptoloogia massidesse: algoritm DES

Praust, Valdo Arvutimaailm 1994 / 8, lk. 17-19: ill

Krüptoloogia. Miks ja kuidas?

Buldas, Ahto Arvutimaailm 1994 / 3, lk. 14-15

Lahendus tulevikuks - PKI : ülevaade

Sepp, Olev A & A 2000 / 1, lk. 35-45 https://artiklid.elnet.ee/record=b1003332*est

Lattice-based threshold signature implementation for constrained devices

Dobias, Patrik; Ricci, Sara; Dzurenda, Petr; Malina, Lukas; Snetkov, Nikita Proceedings of the 20th International Conference on Security and Cryptography. Vol. 1 2023 / p. 724-730 <https://doi.org/10.5220/0012112700003555>

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>

A lightweight Mmssage authentication code for virtual work in future smart cities

Pindar, Zahraddeen A.; Fayomi, Joshua O.; Waziri, Nazir H.; Abdulhamid, Bala M.; Jamel, Sapiee 2020 IEEE European Technology and Engineering Management Summit (E-TEMS), 5-7 March 2020, Dortmund University of Applied Sciences and Art 2020 / 5 p <https://doi.org/10.1109/E-TEMS46250.2020.9111859>

Liu, Feng; Yan, Wei Qi. Visual cryptography for image processing and security. Theory, methods, and applications.

Cham: Springer. xvi, 143 p. (2014) : [review]

Henno, Jaak Zentralblatt MATH 2015 / [1] p

Long-term secure commitments via extractable-binding commitments

Buldas, Ahto; Geihs, Matthias; Buchmann, Johannes Information Security and Privacy : 22nd Australasian Conference, ACISP 2017, Auckland, New Zealand, July 3-5, 2017 : Proceedings, Part I 2017 / p. 65-81 http://doi.org/10.1007/978-3-319-60055-0_4

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](#)

A novel anonymous authentication and key agreement scheme for smart grid

Hammami, Hamza; Obaidat, Mohammad S.; **Ben Yahia, Sadok** Proceedings of the 17th International Joint Conference on e-Business and Telecommunications, ICETE 2020 - Volume 3: ICE-B, Lieusaint, Paris, France, July 8-10, 2020 2020 / p. 357-362 <https://doi.org/10.5220/0009824203570362>

PASCAL : timing SCA resistant design and verification flow

Lai, Xinhui; Jenihhin, Maksim; Raik, Jaan; Paul, Kolin 2019 IEEE 25th International Symposium on On-Line Testing and Robust System Design (IOLTS 2019) : 1-3 July 2019, Greece 2019 / p. 239-242 : ill <https://doi.org/10.1109/IOLTS.2019.8854458>

Reflection, rewinding, and coin-toss in EasyCrypt

Firsov, Denis; Unruh, Dominique CPP 2022 - Proceedings of the 11th ACM SIGPLAN International Conference on Certified Programs and Proofs, co-located with POPL 2022 2022 / p. 166-179 <https://doi.org/10.1145/3497775.3503693>

Security proofs for hash tree time-stamping using hash functions with small output size

Buldas, Ahto; Laanoja, Risto Information security and privacy : 18th Australasian Conference, ACISP 2013, Brisbane, Australia, July 1-3, 2013 : proceedings 2013 / p. 235-250 : ill

Security protocols analysis in the computational model - dependency flow graphs-based approach = Turvaprotokollide analüüs arvutuslikul mudelil - sõltuvusgraafidel põhinev lähenemisviis

Tšahhiov, Ilja 2008 https://www.ester.ee/record=b2449152*est

Server-supported decryption for mobile devices

Kirss, Johanna Maria; Laud, Peeter; **Snetkov, Nikita;** Vakarjuk, Jelizaveta Security and Trust Management : 18th International Workshop, STM 2022 Copenhagen, Denmark, September 29, 2022 : proceedings 2023 / p. 71-81 https://doi.org/10.1007/978-3-031-29504-1_4 [Journal metrics at Scopus](#) [Article at Scopus](#)

Server-supported RSA signatures for mobile devices

Buldas, Ahto; Kalu, Aivo; Laud, Peeter; Oruaas, Mart Computer Security - ESORICS 2017 : 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017 : proceedings, part I 2017 / p. 315-333 : ill http://doi.org/10.1007/978-3-319-66402-6_19

Song, Wei; Zheng, Yu; Fu, Chong; Shan, Pufang. A novel batch image encryption algorithm using parallel computing : [review]

Henno, Jaak Zentralblatt MATH 2020 / 1 p <https://www.zbmath.org/?q=an:07333047>

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

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>

Technological sovereignty : missing the point?

Maurer, Tim; Skierka-Canton, Isabel; Morgus, Robert; Hohmann, Mirko 2015 7th International Conference on Cyber Conflict : Architectures in Cyberspace : 26-29 May 2015, Tallinn, Estonia 2015 / p. 53-67

The method of quantum optical communication based on entangled photon pairs

Udal, Andres; Jaanus, Martin; Umbleja, Kadri; Reeder, Reeno BEC 2014 : 2014 14th Biennial Baltic Electronics Conference : proceedings of the 14th Biennial Baltic Electronics Conference : Tallinn University of Technology, October 6-8, 2014, Tallinn, Estonia 2014 / p. 33-36 : ill

Turvalisust tagav liit

Krustok, Jüri Tehnikamaailm 2003 / 11, lk. 86-88 https://artiklid.elnet.ee/record=b1043973*est

Tänapäeva krüptoloogia : meetodid ja standardid

Praust, Valdo Arvutimaailm 1994 / 6, lk. 46-48

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](#)

Using games to understand and create randomness

Henno, Jaak; Jaakkola, Hannu; Mäkeläinen, Jukka Proceedings of the SQAMIA 2018: 7th Workshop of Software Quality, Analysis, Monitoring, Improvement, and Applications, Novi Sad, Serbia, 27-30. August 2018 2018 <https://www.scopus.com/record/display.uri?eid=2-s2.0-85054376554&origin=inward&txGid=738e163a0c73e3a2a124039455cafce7> Conference Proceedings at Scopus Article at Scopus

Verified multiple-time signature scheme from one-time signatures and timestamping

Firsov, Denis; Lakk, Henri; Truu, Ahto 2021 IEEE 34th Computer Security Foundations Symposium (CSF) : June 21-25, 2021, Virtual Conference : proceedings 2021 / 13 p <https://doi.org/10.1109/CSF51468.2021.00051>

Verified security of BLT signature scheme

Firsov, Denis; Buldas, Ahto; Truu, Ahto; Laanoja, Risto CPP 2020 - Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, co-located with POPL 2020, New Orleans 20 January 2020 through 21 January 2020 2020 / p. 244-257 <https://doi.org/10.1145/3372885.3373828>

Wireless PKI security and mobile voting

Tepandi, Jaak; Vassiljev, Stanislav; Tšahhirov, Ilja Computer 2010 / 6, p. 54-60
<https://www.computer.org/csdl/magazine/co/2010/06/mco2010060054/13rUILLkGV>

Äsjailmunud turbetehnoloogia raamatust : [Infosüsteemide turve, 2. osa, Turbetehnoloogia, Tallinn, 1998]

Praust, Valdo Arvutimaailm 1999 / 2, lk. 38-39