A Bibliography of Publications on Cryptography: 2020–2029

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA

Tel: +1 801 581 5254

E-mail: `beebe@math.utah.edu`, `beebe@acm.org`, `beebe@computer.org` (Internet)
WWW URL: `https://www.math.utah.edu/~beebe/`

25 January 2025
Version 1.70

Title word cross-reference

Optimized [CRSSBMR21, OLZ^{+}20, SPJ20]. **Optimizing** [HJHZ22, TRB^{+}21]. **OPTIMUS** [ODK20]. **Oracle** [RNR^{+}21]. **Oracle-guided** [RNR^{+}21]. **Order** [CCKH21, GXSC21, ZY21, CKV22, JYMP^{+}20, LLH^{+}21]. **order-preserving** [LLH^{+}21]. **Ordinal** [GXZ^{+}22]. **oriented** [Pan20]. **Origin** [GPLK22]. **ORSCA** [FNC22]. **ORSCA-GPU** [FNC22]. **Orthogonal** [XZL20]. **Oscillator** [HON21, JYMP^{+}20]. **Ostrom** [WDFN21]. **Our** [BL22b]. **Out-of-Band** [NRS20]. **output** [Lap22]. **Outsourced** [MSU^{+}20, XCV22, OK21, TWH^{+}21]. **Outsourcing** [BMV22, SZX20, RFT22]. **Over-Scaling-Based** [ZSS^{+}22]. **Overhead** [LQD22]. **Overview** [SYKL21]. **Owner** [Goo21, NBJ21]. **Owner-Custodianship** [Goo21]. **Oxymoron** [The20].

PAASH [OK21]. **PACA** [AAK^{+}21]. **Pairing** [BRPM22, WHW22]. **Pairings** [Fit22, ZYW^{+}20]. **Palm** [RA22]. **PANDA** [MSU^{+}20]. **Papers** [Lew21]. **Paradigm** [PD21]. **Parallel** [FLYL21, Lap22, KG20a, MS21a]. **Parallelization** [ZBT22]. **Parallelized** [Kad21, TSR^{+}20]. **parameters** [ESW21]. **Park** [Mar20a, Mcl20, Tur20]. **Part** [BBC^{+}20]. **Partial** [LZG^{+}21, STK20]. **partially** [ZZQ21]. **participant** [WHSX20]. **participants** [DDD21]. **Partition** [LZW^{+}21, CHJL21]. **Partitioned** [MSU^{+}20]. **Partitioning** [ODK20]. **Party** [LHY^{+}21, GJCJ20, KLC22, LLX^{+}20, SSP21, XJ20]. **Passé** [Cam20]. **passes** [Koz20]. **Passive** [LWS^{+}21, RHSH23, GL22]. **Passphrase** [LYCW20]. **Passphrase-Independent** [LYCW20]. **Password** [ASG21, JJK^{+}21, SJHL21, BBC^{+}21, WGYZ22]. **Password-Authenticated** [SJHL21, JJK^{+}21]. **Passwordless** [Cam20]. **Passwords** [AS22, Cam20]. **Path** [MMM^{+}22]. **Patient** [AS20]. **Pattern** [LLP^{+}20, NPH^{+}20, ATK^{+}22]. **Patterns** [BB22, RA22, AKM21a]. **pay** [KSS^{+}20]. **pay-TV** [KSS^{+}20]. **PBFT** [KKM21]. **Peaks** [BL22b, CGJ20]. **PEKS** [KHM20]. **PEKS-Based** [KHM20]. **Pell** [ST21, ZKY21]. **Pen** [BAR^{+}21]. **Pen-Tablet** [BAR^{+}21]. **Perceive** [WDL21]. **Perception** [FZL^{+}20b]. **Perfect** [NA20b]. **Performance** [Bis21, TSDG22, MTA^{+}22, SK20a]. **Performances** [GMD^{+}22]. **Performant** [ZHC^{+}20]. **periodicals** [TFNF21]. **Permissions** [Jak20]. **Person** [PZJL22, RA22, TTL^{+}21]. **Personal** [Dru22, JKI^{+}21, GLZZ20]. **Personalised** [AFS^{+}22]. **Personalized** [PWL^{+}22]. **Perspective** [MNR^{+}20, RMA^{+}20]. **Perturbation** [TZLZ21]. **PGP** [LP20a, LP20b]. **Pharmaceutical** [STG^{+}20]. **PharmaCrypt** [STG^{+}20]. **Phase** [LQD22]. **Phones** [BP20]. **Photo** [WWL20]. **Photo-Realistic** [WWL20]. **Physical** [DCSA22, TMG^{+}21, XZL20, XTHL21, CDG^{+}20, KSK20, LNE^{+}20, XWW^{+}20]. **Physical-Layer** [XZL20, XTHL21]. **Picture** [Ano21a]. **Pixel** [KS21a, RR21]. **PKI** [KKM21, TADS20]. **Place** [ESD^{+}22]. **Place-based** [ESD^{+}22]. **Plaintext** [HYK^{+}20]. **Platform** [CKFH22, MVBK21, RMMH22, ZHC^{+}20, GLY21, KCML20, MBK^{+}21]. **Platoon** [LNE^{+}20]. **Platoon-based** [LNE^{+}20]. **PLS** [PGCK22]. **PLS-HECC-based** [PGCK22]. **Pocket** [Vac20]. **Point** [AKM^{+}21b, MDJ20]. **Pointing** [MWVK21]. **polarization** [Koz20]. **Policies** [RRN21]. **Policy** [LYZ^{+}22, SHHM21, Sch20, SZM22, ZZQ21]. **Policy-driven** [LYZ^{+}22]. **Pollard** [VCP21]. **Polynomial** [CRSSBMR21, YDS^{+}20]. **polynomials** [ZZ21a]. **Popular** [GRA21]. **Portfolio** [JKI^{+}21]. **positives** [RIW22]. **Possible** [BL22b, RBVV22, TFNF21]. **Post**

References

Akl:2020:FHE

[AA20a] Selim G. Akl and Ibrahim Assem. Fully homomorphic encryption: a general framework and implementations. *International Journal of Parallel, Emergent and Distributed Systems: IJPEDS*, 35(5):493–498, 2020. CODEN ???? ISSN 1744-5760 (print), 1744-5779 (electronic).

Applebaum:2020:PAS

[AA20b] Benny Applebaum and Barak Arkis. On the power of amortization in secret sharing: d-uniform secret sharing and CDS with constant information rate. *ACM Transactions on Computation Theory*, 12(4):24:1–24:21, December 2020. CODEN ???? ISSN 1942-3454 (print), 1942-3462 (electronic). URL `https://dl.acm.org/doi/10.1145/3417756`.

Alzubi:2020:CDB

[AAA20] Omar A. Alzubi, Jafar A. Alzubi, and Mohammad Alsayyed. Cryptosystem design based on Hermitian curves for IoT security. *The Journal of Supercomputing*, 76(11):8566–8589, November 2020. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `https://link.springer.com/article/10.1007/s11227-020-03144-x`.

Alzoubi:2022:ITB

[AAAKJ22] Yehia Ibrahim Alzoubi, Ahmad Al-Ahmad, Hasan Kahtan, and Ashraf Jaradat. Internet of Things and blockchain integration: Security, privacy, technical, and design challenges. *Future Internet*, 14(7):216, July 21,

2022. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/14/7/216`.

Alshawish:2022:EMA

[AAH22] Islam Alshawish and Ali Al-Haj. An efficient mutual authentication scheme for IoT systems. *The Journal of Supercomputing*, 78(14):16056–16087, September 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `https://link.springer.com/article/10.1007/s11227-022-04520-5`.

Ahsan:2020:CCS

[AAI+20a] M. A. Manazir Ahsan, Ihsan Ali, Mohd Yamani Idna Bin Idris, Muhammad Imran, and Muhammad Shoaib. Correction to: Countering Statistical Attacks in Cloud-Based Searchable Encryption. *International Journal of Parallel Programming*, 48(3):580, June 2020. CODEN IJPPE5. ISSN 0885-7458 (print), 1573-7640 (electronic). URL `http://link.springer.com/content/pdf/10.1007/s10766-018-0599-1.pdf`. See [AAI+20b].

Ahsan:2020:CSA

[AAI+20b] M. A. Manazir Ahsan, Ihsan Ali, Mohd Yamani Idna Bin Idris, Muhammad Imran, and Muhammad Shoaib. Countering statistical attacks in cloud-based searchable encryption. *International Journal of Parallel Programming*, 48(3):470–495, June 2020. CODEN IJPPE5. ISSN 0885-7458 (print), 1573-7640 (electronic). See correction [AAI+20a].

Acar:2021:LPA

[AAK+21] Abbas Acar, Shoukat Ali, Koray Karabina, Cengiz Kaygusuz, Hidayet Aksu, Kemal Akkaya, and Selcuk Uluagac. A lightweight Privacy-Aware Continuous Authentication Protocol — PACA. *ACM Transactions on Privacy and Security (TOPS)*, 24(4):24:1–24:28, November 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3464690`.

Andriamilanto:2022:LSE

[AALG22] Nampoina Andriamilanto, Tristan Allard, Gaëtan Le Guelvouit, and Alexandre Garel. A large-scale empirical analysis of browser fingerprints properties for web authentication. *ACM Transactions on the Web (TWEB)*, 16(1):4:1–4:62, February 2022. CODEN ???? ISSN 1559-1131 (print), 1559-114X (electronic). URL `https://dl.acm.org/doi/10.1145/3478026`.

Applebaum:2021:CDS

[AARV21] Benny Applebaum, Barak Arkis, Pavel Raykov, and

Prashant Nalini Vasudevan. Conditional disclosure of secrets: Amplification, closure, amortization, lower-bounds, and separations. *SIAM Journal on Computing*, 50(1): 32–67, ???? 2021. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Aydin:2021:HSC

[AAT+21] Furkan Aydin, Aydin Aysu, Mohit Tiwari, Andreas Gerstlauer, and Michael Orshansky. Horizontal side-channel vulnerabilities of post-quantum key exchange and encapsulation protocols. *ACM Transactions on Embedded Computing Systems*, 20(6):110:1–110:22, November 2021. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic). URL `https://dl.acm.org/doi/10.1145/3476799`.

Azhdari:2022:CBR

[ABB22] Mohammad Sadegh Azhdari, Ali Barati, and Hamid Barati. A cluster-based routing method with authentication capability in Vehicular Ad hoc Networks (VANETs). *Journal of Parallel and Distributed Computing*, 169(??):1–23, November 2022. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0743731522001447`.

Akidau:2021:WSP

[ABC+21] Tyler Akidau, Edmon Begoli, Slava Chernyak, Fabian Hueske, Kathryn Knight, Kenneth Knowles, Daniel Mills, and Dan Sotolongo. Watermarks in stream processing systems: semantics and comparative analysis of Apache Flink and Google cloud dataflow. *Proceedings of the VLDB Endowment*, 14(12):3135–3147, July 2021. CODEN ???? ISSN 2150-8097. URL `https://dl.acm.org/doi/10.14778/3476311.3476389`.

Arfaoui:2020:CAA

[ABK+20] Amel Arfaoui, Omar Rafik Merad Boudia, Ali Kribeche, Sidi-Mohammed Senouci, and Mohamed Hamdi. Context-aware access control and anonymous authentication in WBAN. *Computers & Security*, 88(??):Article 101496, January 2020. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167404818304802`.

Alam:2021:VCS

[ABM21] Manaar Alam, Sarani Bhattacharya, and Debdeep Mukhopadhyay. Victims can be saviors: a machine learning–based detection for micro-architectural side-channel attacks. *ACM Journal on Emerging Technologies in*

Computing Systems (JETC), 17(2):14:1–14:31, April 2021. CODEN ???? ISSN 1550-4832. URL https://dl.acm.org/doi/10.1145/3439189.

Adeli:2022:CSP

[ABMPL22] Morteza Adeli, Nasour Bagheri, Honorio Martín, and Pedro Peris-Lopez. Challenging the security of "A PUF-based hardware mutual authentication protocol". *Journal of Parallel and Distributed Computing*, 169(??): 199–210, November 2022. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731522001538.

Alam:2021:NNB

[ABR+21] Manaar Alam, Arnab Bag, Debapriya Basu Roy, Dirmanto Jap, Jakub Breier, Shivam Bhasin, and Debdeep Mukhopadhyay. Neural network-based inherently fault-tolerant hardware cryptographic primitives without explicit redundancy checks. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 17(1):3:1–3:30, January 2021. CODEN ???? ISSN 1550-4832. URL https://dl.acm.org/doi/10.1145/3409594.

Ali:2020:FPS

[ACD20] Isra Mohamed Ali, Maurantonio Caprolu, and Roberto Di Pietro. Foundations, properties, and security applications of puzzles: a survey. *ACM Computing Surveys*, 53(4):72:1–72:38, September 2020. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/doi/10.1145/3396374.

Aceto:2021:DET

[ACMP21] Giuseppe Aceto, Domenico Ciuonzo, Antonio Montieri, and Antonio Pescapé. DISTILLER: Encrypted traffic classification via multimodal multitask deep learning. *Journal of Network and Computer Applications*, ??(??):??, ???? 2021. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804521000126.

Awan:2022:TMB

[ADA+22] Kamran Ahmad Awan, Ikram Ud Din, Abeer Almogren, Neeraj Kumar, and Ahmad Almogren. A taxonomy of multimedia-based graphical user authentication for green Internet of Things. *ACM Transactions on Internet Technology (TOIT)*, 22(2): 37:1–37:28, May 2022. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic). URL https://dl.acm.org/doi/10.1145/3433544.

Ali:2021:SEM

[ADS21] Guma Ali, Mussa Ally Dida, and Anael Elikana Sam. A secure and efficient multi-factor authentication algorithm for mobile money applications. *Future Internet*, 13(12):299, November 25, 2021. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/13/12/299`.

Al-Dwairi:2022:RRS

[ADSAKAD22] Mahmoud Al-Dwairi, Ahmed S. Shatnawi, Osama Al-Khaleel, and Basheer Al-Duwairi. Ransomware-resilient self-healing XML documents. *Future Internet*, 14(4):115–??, April 07, 2022. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/14/4/115`.

Alharbi:2021:SMI

[ADY+21] Ahmed Alharbi, Hai Dong, Xun Yi, Zahir Tari, and Ibrahim Khalil. Social media identity deception detection: a survey. *ACM Computing Surveys*, 54(3): 69:1–69:35, June 2021. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL `https://dl.acm.org/doi/10.1145/3446372`.

Ahamed:2022:IMB

[AFS+22] Farhad Ahamed, Farnaz Farid, Basem Suleiman, Zohaib Jan, Luay A. Wahsheh, and Seyed Shahrestani. An intelligent multimodal biometric authentication model for personalised healthcare services. *Future Internet*, 14 (8):222, July 26, 2022. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/14/8/222`.

Ahmed:2022:DDP

[AG22a] Quazi Warisha Ahmed and Shruti Garg. Double Diagonal Puzzle Encryption Standard-512 for securing data over cloud environment. *Journal of Grid Computing*, 20(4):??, December 2022. CODEN ???? ISSN 1570-7873 (print), 1572-9184 (electronic). URL `https://link.springer.com/article/10.1007/s10723-022-09612-3`.

Alam:2022:FLR

[AG22b] Tanweer Alam and Ruchi Gupta. Federated learning and its role in the privacy preservation of IoT devices. *Future Internet*, 14(9): 246, August 23, 2022. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/14/9/246`.

Andola:2022:SEC

[AGV22] Nitish Andola, Raghav Gahlot, and Shekhar Verma. Searchable encryption on the cloud: a survey. *The Journal of*

Supercomputing, 78(7):9952–9984, May 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `https://link.springer.com/article/10.1007/s11227-022-04309-6`.

Amanlou:2021:LSA

[AHB21] Sanaz Amanlou, Mohammad Kamrul Hasan, and Khairul Azmi Abu Bakar. Lightweight and secure authentication scheme for IoT network based on publish-subscribe fog computing model. *Computer Networks (Amsterdam, Netherlands: 1999)*, 199(??):??, November 9, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128621004175`.

Aloufi:2022:CBD

[AHSL22] Asma Aloufi, Peizhao Hu, Yongsoo Song, and Kristin Lauter. Computing blindfolded on data homomorphically encrypted under multiple keys: a survey. *ACM Computing Surveys*, 54(9):195:1–195:37, December 2022. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL `https://dl.acm.org/doi/10.1145/3477139`.

Au:2020:SIC

[AHWB20] Man Ho Au, Jinguang Han, Qianhong Wu, and Colin Boyd. Special issue on cryptographic currency and blockchain technology. *Future Generation Computer Systems*, 107(??):758–759, June 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X19314840`.

Alawami:2020:LFG

[AK20] Mohsen A. Alawami and Hyoungshick Kim. LocAuth: a fine-grained indoor location-based authentication system using wireless networks characteristics. *Computers & Security*, 89(??):Article 101683, February 2020. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167404819302226`.

Alyari:2020:SNR

[AKI20] Robab Alyari, Jaber Karimpour, and Habib Izadkhah. Specifying a new requirement model for secure adaptive systems. *The Computer Journal*, 63(8):1148–1167, August 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/63/8/1148/5645559`.

Akl:2020:HEG

[Akl20] Selim G. Akl. How to encrypt a graph. *International Journal of Parallel, Emergent and Distributed Systems: IJPEDS*, 35(6):668–681, 2020. CODEN ???? ISSN 1744-5760 (print), 1744-5779 (electronic).

Abdullah:2021:HAL

[AKM21a] Fatima Abdullah, Dragi Kimovski, and Kashif Munir. Handover authentication latency reduction using mobile edge computing and mobility patterns. *Computing*, 103(11):2667–2686, November 2021. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL `https://link.springer.com/article/10.1007/s00607-021-00969-z`.

Andrysco:2021:SFP

[AKM+21b] Marc Andrysco, David Kohlbrenner, Keaton Mowery, Ranjit Jhala, Sorin Lerner, and Hovav Shacham. On subnormal floating point and abnormal timing. Report, Department of Computer Science and Engineering University of California, San Diego, La Jolla, California, USA, January 2, 2021. 17 pp.

Alabdulatif:2020:TSB

[AKY20] Abdulatif Alabdulatif, Ibrahim Khalil, and Xun Yi. Towards secure big data analytic for cloud-enabled applications with fully homomorphic encryption. *Journal of Parallel and Distributed Computing*, 137(??):192–204, March 2020. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0743731519300887`.

Albeshri:2021:IHB

[Alb21] Aiiad Albeshri. An image hashing-based authentication and secure group communication scheme for IoT-enabled MANETs. *Future Internet*, 13(7):166, June 27, 2021. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/13/7/166`.

Arapinis:2021:DSQ

[ALKP21] Myrto Arapinis, Nikolaos Lamprou, Elham Kashefi, and Anna Pappa. Definitions and security of quantum electronic voting. *ACM Transactions on Quantum Computing (TQC)*, 2(1):4:1–4:33, April 2021. CODEN ???? ISSN ???? URL `https://dl.acm.org/doi/10.1145/3450144`.

Ahvanooey:2020:ANI

[ALZ+20] Milad Taleby Ahvanooey, Qianmu Li, Xuefang Zhu, Mamoun Alazab, and Jing Zhang. ANiTW: a Novel Intelligent Text Watermarking technique for forensic identification of spurious information on social media. *Computers & Security*, 90(??): Article 101702, March 2020.

CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167404819302391`.

Ahmadjee:2022:SBA

[AMGBK22] Sabreen Ahmadjee, Carlos Mera-Gómez, Rami Bahsoon, and Rick Kazman. A study on blockchain architecture design decisions and their security attacks and threats. *ACM Transactions on Software Engineering and Methodology*, 31 (2):36e:1–36e:45, April 2022. CODEN ATSMER. ISSN 1049-331X (print), 1557-7392 (electronic). URL `https://dl.acm.org/doi/10.1145/3502740`.

Aghaie:2020:IC

[AMR+20] A. Aghaie, A. Moradi, S. Rasoolzadeh, A. R. Shahmirzadi, F. Schellenberg, and T. Schneider. Impeccable circuits. *IEEE Transactions on Computers*, 69(3): 361–376, March 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Ali:2020:FDH

[AMSL20] Mohammad Ali, Javad Mohajeri, Mohammad-Reza Sadeghi, and Ximeng Liu. A fully distributed hierarchical attribute-based encryption scheme. *Theoretical Computer Science*, 815 (??):25–46, May 2, 2020. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397520301286`.

Abdul:2020:CWH

[ANG20] Wadood Abdul, Ohoud Nafea, and Sanaa Ghouzali. Combining watermarking and hyper-chaotic map to enhance the security of stored biometric templates. *The Computer Journal*, 63(3): 479–493, March 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/63/3/479/5510728`.

Anonymous:2020:DS

[Ano20] Anonymous. Demystifying stablecoins. *ACM Queue: Tomorrow's Computing Today*, 18(1):??, January 2020. CODEN AQCUAE. ISSN 1542-7730 (print), 1542-7749 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3387945.3388781`.

Anonymous:2021:BPBa

[Ano21a] Anonymous. The big picture: a big bet on crypto. *IEEE Spectrum*, 58(8):12–13, August 2021. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Anonymous:2021:BAB

[Ano21b] Anonymous. Blockchain applications beyond the cryptocurrency casino: The punishment not reward blockchain architecture. *Concurrency and Computation: Practice and Experience*, 33(1): e5749:1–e5749:??, January 10, 2021. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Anonymous:2021:DES

[Ano21c] Anonymous. A discussion of election security, cryptography, and exceptional access with Michael Alan Specter. *IEEE Security & Privacy*, 19(6):15–22, November/December 2021. ISSN 1540-7993 (print), 1558-4046 (electronic).

Anonymous:2024:GCY

[Ano24] Anonymous. GCHQ celebrates 80 years of Colossus. Web site, January 18, 2024. URL `https://www.gchq.gov.uk/news/colossus-80`.

Asharov:2021:SSE

[ANSS21] Gilad Asharov, Moni Naor, Gil Segev, and Ido Shahaf. Searchable symmetric encryption: Optimal locality in linear space via two-dimensional balanced allocations. *SIAM Journal on Computing*, 50(5):1501–1536, ???? 2021. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Al-Odat:2020:SHA

[AOAAK20] Zeyad A. Al-Odat, Mazhar Ali, Assad Abbas, and Samee U. Khan. Secure hash algorithms and the corresponding FPGA optimization techniques. *ACM Computing Surveys*, 53(5):97:1–97:36, October 2020. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL `https://dl.acm.org/doi/10.1145/3311724`.

Akmandor:2021:SSE

[AOM+21] A. O. Akmandor, J. Ortiz, I. Manotas, B. Ko, and N. K. Jha. SECRET: Semantically enhanced classification of real-world tasks. *IEEE Transactions on Computers*, 70(3):440–456, 2021. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Alsahlani:2021:LIL

[AP21] Ahmed Yaser Fahad Alsahlani and Alexandru Popa. LMAAS-IoT: Lightweight multi-factor authentication and authorization scheme for real-time data access in IoT cloud-based environment. *Journal of Network and Computer Applications*, 192(??):??, October 15, 2021. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804521001879.

Altinok:2022:GAE

[APTT22] Kaan Furkan Altinok, Afsin Peker, Cihangir Tezcan, and Alptekin Temizel. GPU accelerated 3DES encryption. *Concurrency and Computation: Practice and Experience*, 34(9):e6507:1–e6507:??, April 25, 2022. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Anand:2020:JWE

[AS20] Ashima Anand and Amit Kumar Singh. Joint watermarking–encryption–ECC for patient record security in wavelet domain. *IEEE MultiMedia*, 27(3):66–75, 2020. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic).

Alt:2022:BPC

[AS22] Florian Alt and Stefan Schneegass. Beyond passwords: Challenges and opportunities of future authentication. *IEEE Security & Privacy*, 20(1):82–86, January/February 2022. ISSN 1540-7993 (print), 1558-4046 (electronic).

Alkasasbeh:2021:WSH

[ASG21] Anas Ali Alkasasbeh, Fotios Spyridonis, and Gheorghita Ghinea. When scents help me remember my password. *ACM Transactions on Applied Perception*, 18(3):16:1–16:18, July 2021. CODEN ???? ISSN 1544-3558 (print), 1544-3965 (electronic). URL https://dl.acm.org/doi/10.1145/3469889.

Anand:2020:CTE

[ASLB20] Ashima Anand, Amit Kumar Singh, Zhihan Lv, and Guarav Bhatnagar. Compression-then-encryption-based secure watermarking technique for smart healthcare system. *IEEE MultiMedia*, 27(4):133–143, 2020. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic).

Alam:2022:NLL

[ASMK22] Manaar Alam, Sayandeep Saha, Debdeep Mukhopadhyay, and Sandip Kundu. NN-Lock: a lightweight authorization to prevent IP threats of deep learning models. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 18(3):51:1–51:19, July 2022. CODEN ???? ISSN 1550-4832. URL https://dl.acm.org/doi/10.1145/3505634.

Akbari:2021:LBC

[ASV+21] Iman Akbari, Mohammad A. Salahuddin, Leni Ven, Noura Limam, Raouf Boutaba, Bertrand Mathieu, Stephanie Moteau, and Stephane Tuffin. A look behind the curtain: Traffic classification in an increasingly encrypted Web. *ACM SIGMETRICS Performance Evaluation Review*, 49(1):23–24, June 2021. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic). URL https://dl.acm.org/doi/10.1145/3543516.3453921.

Akbari:2022:TCI

[ASV+22] Iman Akbari, Mohammad A. Salahuddin, Leni Ven, Noura Limam, Raouf Boutaba, Bertrand Mathieu, Stephanie Moteau, and Stephane Tuffin. Traffic classification in an increasingly encrypted web. *Communications of the Association for Computing Machinery*, 65(10):75–83, October 2022. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL https://dl.acm.org/doi/10.1145/3559439.

Awais:2022:NSE

[ATK+22] Muhammad Awais, Shahzaib Tahir, Fawad Khan, Hasan Tahir, Ruhma Tahir, Rabia Latif, and Mir Yasir Umair. A novel searchable encryption scheme to reduce the access pattern leakage. *Future Generation Computer Systems*, 133(??):338–350, August 2022. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X22001066.

Alizadeh:2021:STB

[ATS+21] Mojtaba Alizadeh, Mohammad Hesam Tadayon, Kouichi Sakurai, Hiroaki Anada, and Alireza Jolfaei. A secure ticket-based authentication mechanism for proxy mobile IPv6 networks in volunteer computing. *ACM Transactions on Internet Technology (TOIT)*, 21(4):82:1–82:16, July 2021. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic). URL https://dl.acm.org/doi/10.1145/3407189.

Alaca:2020:CAF

[AV20] Furkan Alaca and Paul C. Van Oorschot. Comparative analysis and framework evaluating Web single sign-on systems. *ACM Computing Surveys*, 53(5):112:1–112:34, October 2020. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/doi/10.1145/3409452.

Awad:2020:GEI

[AW20] A. Awad and R. Wang. Guest Editors' introduction to the special issue on hardware security. *IEEE Transactions on Computers*, 69(11):1556–1557, November 2020. CODEN ITCOB4. ISSN 0018-

9340 (print), 1557-9956 (electronic).

Adnan:2022:QKD

[AZH22] Mohd Hirzi Adnan, Zuriati Ahmad Zukarnain, and Nur Ziadah Harun. Quantum key distribution for 5G networks: A review, state of art and future directions. *Future Internet*, 14(3):73, February 25, 2022. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/14/3/73`.

Bhowmik:2020:EDA

[BA20] Deepayan Bhowmik and Charith Abhayaratne. Embedding distortion analysis in wavelet-domain watermarking. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 15(4):1–24, January 2020. ISSN 1551-6857 (print), 1551-6865 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3357333`.

Begum:2021:UAB

[BAR+21] Nasima Begum, Md Azim Hossain Akash, Sayma Rahman, Jungpil Shin, Md Rashedul Islam, and Md Ezharul Islam. User authentication based on handwriting analysis of pen-tablet sensor data using optimal feature selection model. *Future Internet*, 13(9):231, September 06, 2021. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/13/9/231`.

Bauer:2021:SHS

[Bau21] Craig P. Bauer. *Secret History: the Story of Cryptology*. Discrete mathematics and its applications. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, second edition, 2021. ISBN 1-315-16253-9 (e-book), 1-351-66848-X (e-book), 1-351-66849-8 (e-book), 1-351-66850-1 (e-book). xxv + 614 pp. LCCN QA76.9.A25 B38 2021. URL `https://api.pageplace.de/preview/DT0400.9781351668507_A40887288/preview-9781351668507_A40887288.pdf`.

Boucetta:2022:BAU

[BB22] Aldjia Boucetta and Leila Boussaad. Biometric authentication using finger-vein patterns with deep-learning and discriminant correlation analysis. *International Journal of Image and Graphics (IJIG)*, 22(01):??, January 2022. ISSN 0219-4678. URL `https://www.worldscientific.com/doi/10.1142/S0219467822500139`.

Baksi:2023:SFA

[BBB+23] Anubhab Baksi, Shivam Bhasin, Jakub Breier, Dirmanto Jap, and Dhiman Saha. A survey on fault attacks on symmetric key cryptosystems. *ACM Computing Surveys*, 55(4):86:1–86:??, May

2023. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/doi/10.1145/3530054.

Barthe:2020:SLN

[BBC+20] Gilles Barthe, Gustavo Betarte, Juan Diego Campo, Carlos Luna, and David Pichardie. System-level non-interference of constant-time cryptography. Part II: Verified static analysis and stealth memory. *Journal of Automated Reasoning*, 64(8):1685–1729, December 2020. CODEN JAREEW. ISSN 0168-7433 (print), 1573-0670 (electronic). URL http://link.springer.com/article/10.1007/s10817-020-09548-x.

Blazy:2021:HSS

[BBC+21] Olivier Blazy, Laura Brouilhet, Celine Chevalier, Patrick Towa, Ida Tucker, and Damien Vergnaud. Hardware security without secure hardware: How to decrypt with a password and a server. *Theoretical Computer Science*, 895(??):178–211, December 4, 2021. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397521005776.

Barthe:2020:FVC

[BBG+20] Gilles Barthe, Sandrine Blazy, Benjamin Grégoire, Rémi Hutin, Vincent Laporte, David Pichardie, and Alix Trieu. Formal verification of a constant-time preserving C compiler. *Proceedings of the ACM on Programming Languages (PACMPL)*, 4(POPL):7:1–7:30, January 2020. URL https://dl.acm.org/doi/abs/10.1145/3371075.

Behrad:2020:NSA

[BBTC20] Shanay Behrad, Emmanuel Bertin, Stéphane Tuffin, and Noel Crespi. A new scalable authentication and access control mechanism for 5g-based IoT. *Future Generation Computer Systems*, 108(??):46–61, July 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X19310143.

Busby:2020:ICC

[BCD+20] J. A. Busby, E. N. Cohen, E. A. Dames, J. Doherty, S. Dragone, D. Evans, M. J. Fisher, N. Hadzic, C. Hagleitner, A. J. Higby, M. D. Hocker, L. S. Jagich, M. J. Jordan, R. Kisley, K. D. Lamb, M. D. Marik, J. Mayfield, T. E. Morris, T. D. Needham, W. Santiago-Fernandez, V. Urban, T. Visegrady, and K. Werner. The IBM 4769 cryptographic coprocessor. *IBM Journal of Research and Development*, 64(5/6):3:1–3:11, 2020. CO-

DEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Basin:2022:TVL

[BCDS22] David Basin, Cas Cremers, Jannik Dreier, and Ralf Sasse. Tamarin: Verification of large-scale, real-world, cryptographic protocols. *IEEE Security & Privacy*, 20(3):24–32, May/June 2022. ISSN 1540-7993 (print), 1558-4046 (electronic).

Berlato:2022:FMA

[BCLR22] Stefano Berlato, Roberto Carbone, Adam J. Lee, and Silvio Ranise. Formal modelling and automated trade-off analysis of enforcement architectures for cryptographic access control in the cloud. *ACM Transactions on Privacy and Security (TOPS)*, 25(1):2:1–2:37, February 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3474056.

Brakerski:2021:CTQ

[BCM+21] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. *Journal of the ACM*, 68(5):31:1–31:47, October 2021. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL https://dl.acm.org/doi/10.1145/3441309.

Bangalore:2020:PSE

[BCP20] Laasya Bangalore, Ashish Choudhury, and Arpita Patra. The power of shunning: Efficient asynchronous Byzantine agreement revisited*. *Journal of the ACM*, 67(3):14:1–14:59, June 2020. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL https://dl.acm.org/doi/abs/10.1145/3388788.

Bultel:2020:FCC

[BDDL20] Xavier Bultel, Jannik Dreier, Jean-Guillaume Dumas, and Pascal Lafourcade. A faster cryptographer's Conspiracy Santa. *Theoretical Computer Science*, 839(??):122–134, November 2, 2020. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397520303170.

Beierle:2021:CGE

[BDL+21] Christof Beierle, Patrick Derbez, Gregor Leander, Gaëtan Leurent, Håvard Raddum, Yann Rotella, David Rupprecht, and Lukas Stennes. Cryptanalysis of the GPRS encryption algorithms GEA-1 and GEA-2. *Lecture Notes in Computer Science*,

12697:155–183, 2021. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL https://ia.cr/2021/819.

Buccafurri:2022:BBF

[BDL22] Francesco Buccafurri, Vincenzo De Angelis, and Sara Lazzaro. A blockchain-based framework to enhance anonymous services with accountability guarantees. *Future Internet*, 14(8):243, August 21, 2022. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/14/8/243.

Bernabe:2020:AER

[BDM+20] Jorge Bernal Bernabe, Martin David, Rafael Torres Moreno, Javier Presa Cordero, Sébastien Bahloul, and Antonio Skarmeta. ARIES: Evaluation of a reliable and privacy-preserving European identity management framework. *Future Generation Computer Systems*, 102 (??):409–425, January 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X1930843X.

Boyd:2021:MVF

[BG21] Colin Boyd and Kai Gellert. A modern view on forward security. *The Computer Journal*, 64(4):639–652, April 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/64/4/639/5896207.

Bian:2020:BAE

[BGCL20] Weixin Bian, Prosanta Gope, Yongqiang Cheng, and Qingde Li. Bio-AKA: an efficient fingerprint based two factor user authentication and key agreement scheme. *Future Generation Computer Systems*, 109(??):45–55, August 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X19332467.

Boudot:2022:SAI

[BGG+22] Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, and Paul Zimmermann. The state of the art in integer factoring and breaking public-key cryptography. *IEEE Security & Privacy*, 20 (2):80–86, March/April 2022. ISSN 1540-7993 (print), 1558-4046 (electronic).

Bencomo:2022:SBA

[BGH+22] Nelly Bencomo, Jin L. C. Guo, Rachel Harrison, Hans-Martin Heyn, and Tim Menzies. The secret to better AI and better software (is requirements engineering). *IEEE Software*, 39(1):105–110, February 2022. CO-

DEN IESOEG. ISSN 0740-7459 (print), 1937-4194 (electronic).

Biswas:2021:CSI

[Bis21] Arnab Kumar Biswas. Cryptographic software IP protection without compromising performance or timing side-channel leakage. *ACM Transactions on Architecture and Code Optimization*, 18 (2):20:1–20:20, March 2021. CODEN ???? ISSN 1544-3566 (print), 1544-3973 (electronic). URL `https://dl.acm.org/doi/10.1145/3443707`.

Bursztein:2023:TQR

[BK23] Elie Bursztein and Fabian Kaczmarczyck. Toward quantum resilient security keys. Google Security Blog, August 15, 2023. URL `https://security.googleblog.com/2023/08/toward-quantum-resilient-security-keys.html`. 2023.

Belguith:2020:APP

[BKL+20] Sana Belguith, Nesrine Kaaniche, Maryline Laurent, Abderrazak Jemai, and Rabah Attia. Accountable privacy preserving attribute based framework for authenticated encrypted access in clouds. *Journal of Parallel and Distributed Computing*, 135(??):1–20, January 2020. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0743731519302175`.

Binbeshr:2021:SRH

[BKM21] Farid Binbeshr, Amirrudin Kamsin, and Manal Mohammed. A systematic review on hadith authentication and classification methods. *ACM Transactions on Asian and Low-Resource Language Information Processing (TALLIP)*, 20(2): 34:1–34:17, April 2021. CODEN ???? ISSN 2375-4699 (print), 2375-4702 (electronic). URL `https://dl.acm.org/doi/10.1145/3434236`.

Barbeau:2022:AIR

[BKP22] Michel Barbeau, Evangelos Kranakis, and Nicolas Perez. Authenticity, integrity, and replay protection in quantum data communications and networking. *ACM Transactions on Quantum Computing (TQC)*, 3(2):9:1–9:22, June 2022. CODEN ???? ISSN 2643-6809 (print), 2643-6817 (electronic). URL `https://dl.acm.org/doi/10.1145/3517341`.

Baksi:2022:NAS

[BKS22] Anubhab Baksi, Satyam Kumar, and Santanu Sarkar. A new approach for side channel analysis on stream ciphers and related constructions. *IEEE Transactions on Computers*, 71(10):2527–2537, October 2022. CO-

DEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Bilami:2022:LBB

[BL22a] Karam Eddine Bilami and Pascal LORENZ. Lightweight blockchain-based scheme to secure wireless M2M area networks. *Future Internet*, 14 (5):158, May 23, 2022. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/14/5/158.

Blackburn-Lynch:2022:WEO

[BL22b] James Blackburn-Lynch. Are we ever our best possible selves? an application of bézout's identity to find coincident peaks of multiple sine curves. *College Mathematics Journal*, 53(3):183–189, 2022. CODEN ???? ISSN 0746-8342 (print), 1931-1346 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/07468342.2022.2040264.

Butler:2021:FVP

[BLG21] D. Butler, A. Lochbihler, and A. Gascón. Formalising Σ-protocols and commitment schemes using CryptHOL. *Journal of Automated Reasoning*, 65(4): 521–567, April 2021. CODEN JAREEW. ISSN 0168-7433 (print), 1573-0670 (electronic). URL https://link.springer.com/article/10.1007/s10817-020-09581-w.

Bhattacharya:2020:BPA

[BMBM20] S. Bhattacharya, C. Maurice, S. Bhasin, and D. Mukhopadhyay. Branch prediction attack on blinded scalar multiplication. *IEEE Transactions on Computers*, 69 (5):633–648, 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Bellini:2021:GLA

[BMDE21] Emanuele Bellini, Nadir Murru, Antonio J. Di Scala, and Michele Elia. Group law on affine conics and applications to cryptography. *Applied Mathematics and Computation*, 409(??): Article 125537, November 15, 2021. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300320304938.

Bouillaguet:2022:CME

[BMV22] Charles Bouillaguet, Florette Martinez, and Damien Vergnaud. Cryptanalysis of modular exponentiation outsourcing protocols. *The Computer Journal*, 65(9): 2299–2314, September 2022. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/65/9/2299/6289878.

Bahig:2022:SWF

[BNB22] Hazem M. Bahig, Dieaa I. Nassr, and Hatem M. Bahig. Speeding up wheel factoring method. *The Journal of Supercomputing*, 78(14):15730–15748, September 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-022-04470-y.

Bahig:2020:UMP

[BNBN20] Hatem M. Bahig, Dieaa I. Nassr, Ashraf Bhery, and Abderrahmane Nitaj. A unified method for private exponent attacks on RSA using lattices. *International Journal of Foundations of Computer Science (IJFCS)*, 31(2):207–231, February 2020. ISSN 0129-0541. URL https://www.worldscientific.com/doi/10.1142/S0129054120500045.

Belman:2020:DPT

[BP20] Amith K. Belman and Vir V. Phoha. Discriminative power of typing features on desktops, tablets, and phones for user identification. *ACM Transactions on Privacy and Security (TOPS)*, 23(1):4:1–4:36, February 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3377404.

Bang:2022:DEN

[BR22] A. O. Bang and Udai Pratap Rao. Design and evaluation of a novel white-box encryption scheme for resource-constrained IoT devices. *The Journal of Supercomputing*, 78(8):11111–11137, May 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-022-04322-9.

Braeken:2021:DDG

[Bra21] An Braeken. Device-to-device group authentication compatible with 5G AKA protocol. *Computer Networks (Amsterdam, Netherlands: 1999)*, 201(??):??, December 24, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128621004850.

Braeken:2022:AKA

[Bra22] An Braeken. Authenticated key agreement protocols for dew-assisted IoT systems. *The Journal of Supercomputing*, 78(10):12093–12113, July 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-022-04364-z.

Bag:2022:PFA

[BRPM22] Arnab Bag, Debapriya Basu

Roy, Sikhar Patranabis, and Debdeep Mukhopadhyay. `FlexiPair`: An automated programmable framework for pairing cryptosystems. *IEEE Transactions on Computers*, 71(3):506–519, March 2022. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Bos:2021:CCA

[BS21] Joppe W. Bos and Martijn Stam, editors. *Computational Cryptography: Algorithmic Aspects of Cryptology*, volume 469 of *London Mathematical Society lecture note series*. Cambridge University Press, Cambridge, UK, 2021. ISBN 1-108-79593-5 (paperback), 1-108-85420-6. xii + 387 pp. LCCN QA268 .C693 2021.

Bronzino:2020:ISV

[BSA+20] Francesco Bronzino, Paul Schmitt, Sara Ayoubi, Guilherme Martins, Renata Teixeira, and Nick Feamster. Inferring streaming video quality from encrypted traffic: Practical models and deployment experience. *ACM SIGMETRICS Performance Evaluation Review*, 48(3):27–32, December 2020. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic). URL `https://dl.acm.org/doi/10.1145/3453953.3453958`.

Bhatt:2022:DKG

[BSS+22] Sachin Bhatt, Prithvi Singh, Archana Sharma, Arpita Rai, Ravins Dohare, Shweta Sankhwar, Akash Sharma, and Mansoor Ali Syed. Deciphering key genes and miRNAs associated with hepatocellular carcinoma via network-based approach. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 19(2):843–853, March 2022. CODEN ITCBCY. ISSN 1545-5963 (print), 1557-9964 (electronic). URL `https://dl.acm.org/doi/10.1109/TCBB.2020.3016781`.

Bhardwaj:2022:IAU

[BVG22] Anuj Bhardwaj, Vivek Singh Verma, and Sandesh Gupta. Image authentication using block truncation coding in lifting wavelet domain. *International Journal of Image and Graphics (IJIG)*, 22(01): ??, January 2022. ISSN 0219-4678. URL `https://www.worldscientific.com/doi/10.1142/S0219467822500115`.

Campbell:2020:PPP

[Cam20] M. Campbell. Putting the passé into passwords: How passwordless technologies are reshaping digital identity. *Computer*, 53(8):89–93, 2020. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Canetti:2020:UCS

[Can20] Ran Canetti. Universally composable security. *Jour-*

nal of the ACM, 67(5):28:1–28:94, October 2020. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL https://dl.acm.org/doi/10.1145/3402457.

Chicha:2021:UCM

[CAN+21] Elie Chicha, Bechara Al Bouna, Mohamed Nassar, Richard Chbeir, Ramzi A. Haraty, Mourad Oussalah, Djamal Benslimane, and Mansour Naser Alraja. A user-centric mechanism for sequentially releasing graph datasets under Blowfish privacy. *ACM Transactions on Internet Technology (TOIT)*, 21(1):20:1–20:25, February 2021. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic). URL https://dl.acm.org/doi/10.1145/3431501.

Carnley:2022:PIT

[CB22] Renee Carnley and Sikha Bagui. A public infrastructure for a trusted wireless world. *Future Internet*, 14(7):200, June 30, 2022. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/14/7/200.

Celenk:2021:MLB

[CBE21] Özge Celenk, Thomas Bauschert, and Marcus Eckert. Machine learning based KPI monitoring of video streaming traffic for QoE estimation. *ACM SIGMETRICS Performance Evaluation Review*, 48(4):33–36, May 2021. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic). URL https://dl.acm.org/doi/10.1145/3466826.3466839.

Choudhry:2022:DEI

[CBJ22] Ajai Choudhry, Iliya Bluskov, and Alexander James. A diophantine equation inspired by Brahmagupta's identity. *International Journal of Number Theory (IJNT)*, 18(04):905–911, May 2022. ISSN 1793-0421 (print), 1793-7310 (electronic). URL https://www.worldscientific.com/doi/10.1142/S1793042122500476.

Christie:2020:MAA

[CBN+20] Marcus A. Christie, Anuj Bhandar, Supun Nakandala, Suresh Marru, Eroma Abeysinghe, Sudhakar Pamidighantam, and Marlon E. Pierce. Managing authentication and authorization in distributed science gateway middleware. *Future Generation Computer Systems*, 111(??):780–785, October 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X18314729.

Chen:2021:STF

[CC21a] Yulei Chen and Jianhua Chen. A secure three-factor-based authentication with key agreement protocol for e-health clouds. *The Journal of Supercomputing*, 77(4): 3359–3380, April 2021. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-020-03395-8.

Chi:2021:DAM

[CC21b] Po-Wen Chi and Yu-Lun Chang. Do not ask me what I am looking for: Index deniable encryption. *Future Generation Computer Systems*, 122(??):28–39, September 2021. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X21001199.

Chan:2021:CAC

[cC21c] Hei chi Chan. Chasing after cancellations: Revisiting a classic identity that implies the Rogers–Ramanujan identities. *International Journal of Number Theory (IJNT)*, 17(02):297–310, March 2021. ISSN 1793-0421 (print), 1793-7310 (electronic). URL https://www.worldscientific.com/doi/10.1142/S1793042120400266.

Chang:2021:TLR

[CCKH21] Chin-Chen Chang, Jui-Feng Chang, Wei-Jiun Kao, and Ji-Hwei Horng. Two-layer reversible data hiding for VQ-compressed images based on De-clustering and indicator-free search-order coding. *Future Internet*, 13(8):215, August 20, 2021. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/13/8/215.

Cai:2020:ESN

[CCT+20] Y. Cai, X. Chen, L. Tian, Y. Wang, and H. Yang. Enabling secure NVM-based inmemory neural network computing by sparse fast gradient encryption. *IEEE Transactions on Computers*, 69(11): 1596–1610, November 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Chen:2020:SSI

[CCX+20] G. Chen, S. Chen, Y. Xiao, Y. Zhang, Z. Lin, and T. Lai. SgxPectre: Stealing Intel secrets from SGX enclaves via speculative execution. *IEEE Security & Privacy*, 18(3):28–37, May/June 2020. ISSN 1558-4046.

Coppolino:2021:VCI

[CDF+21] L. Coppolino, S. D Antonio, V. Formicola, G. Mazzeo, and L. Romano. VISE: Combining Intel SGX and homomorphic encryption for cloud industrial control systems. *IEEE Transactions on Computers*, 70(5):711–724, 2021. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Challa:2020:DAA

[CDG+20] Sravani Challa, Ashok Kumar Das, Prosanta Gope, Neeraj Kumar, Fan Wu, and Athanasios V. Vasilakos. Design and analysis of authenticated key agreement scheme in cloud-assisted cyber-physical systems. *Future Generation Computer Systems*, 108(??): 1267–1286, July 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X17326328`.

Clark:2020:DS

[CDM20] Jeremy Clark, Didem Demirag, and Seyedehmahsa Moosavi. Demystifying stablecoins. *Communications of the Association for Computing Machinery*, 63(7):40–46, July 2020. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3386275`.

Chiesa:2022:SII

[CFGS22] Alessandro Chiesa, Michael A. Forbes, Tom Gur, and Nicholas Spooner. Spatial isolation implies zero knowledge even in a quantum world. *Journal of the ACM*, 69(2):15:1–15:44, April 2022. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `https://dl.acm.org/doi/10.1145/3511100`.

Chen:2020:TIT

[CGJ20] Liangchen Chen, Shu Gao, and Zhengwei Jiang. THS-IDPC: A three-stage hierarchical sampling method based on improved density peaks clustering algorithm for encrypted malicious traffic detection. *The Journal of Supercomputing*, 76(9):7489–7518, September 2020. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `https://link.springer.com/article/10.1007/s11227-020-03372-1`.

Cosmo:2020:RSC

[CGZ20] R. D. Cosmo, M. Gruenpeter, and S. Zacchiroli. Referencing source code artifacts: A separate concern in software citation. *Computing in Science and Engineering*, 22(2):33–43, March/April 2020. CODEN CSENFA. ISSN 1521-9615 (print), 1558-366X (electronic).

Cambou:2020:CAS

[CHA20] Bertrand Cambou, David Hély, and Sareh Assiri. Cryptography with analog scheme using memristors. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 16(4):40:1–40:30, October 2020. CODEN ???? ISSN 1550-4832. URL `https://dl.acm.org/doi/10.1145/3412439`.

Chan:2021:MTF

[CHJL21] Song Heng Chan, Nankun Hong, Jerry, and Jeremy Lovejoy. A mock theta function identity related to the partition rank modulo 3 and 9. *International Journal of Number Theory (IJNT)*, 17(02):311–327, March 2021. ISSN 1793-0421 (print), 1793-7310 (electronic). URL https://www.worldscientific.com/doi/10.1142/S1793042120400254.

Chen:2021:PAI

[CHWM21] Haixia Chen, Xinyi Huang, Wei Wu, and Yi Mu. Privacy-aware image authentication from cryptographic primitives. *The Computer Journal*, 64(8):1178–1192, August 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/64/8/1178/5943716.

Ciaurri:2022:EPG

[Cia22] Óscar Ciaurri. An "Esoteric" proof of Gelin–Cesàro identity. *American Mathematical Monthly*, 129(5):465, 2022. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Chochtoula:2022:IEC

[CISM22] Despoina Chochtoula, Aristidis Ilias, Yannis C. Stamatiou, and Christos Makris. Integrating elliptic curve cryptography with the Modbus TCP SCADA Communication Protocol. *Future Internet*, 14(8):232, July 28, 2022. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/14/8/232.

Chaudhry:2021:RBP

[CIY+21] Shehzad Ashraf Chaudhry, Azeem Irshad, Khalid Yahya, Neeraj Kumar, Mamoun Alazab, and Yousaf Bin Zikria. Rotating behind privacy: an improved lightweight authentication scheme for cloud-based IoT environment. *ACM Transactions on Internet Technology (TOIT)*, 21(3):78:1–78:19, June 2021. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic). URL https://dl.acm.org/doi/10.1145/3425707.

Chang:2020:CHS

[CJS+20] Jinyong Chang, Yanyan Ji, Bilin Shao, Maozhi Xu, and Rui Xue. Certificateless homomorphic signature scheme for network coding. *IEEE/ACM Transactions on Networking*, 28(6):2615–2628, December 2020. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic). URL https://dl.acm.org/doi/10.1109/TNET.2020.3013902.

Chaabane:2022:LPB

[CKFH22] Faten Chaabane, Jalel Ktari, Tarek Frikha, and Habib Hamam. Low power blockchained E-vote platform for university environment. *Future Internet*, 14(9):269, September 19, 2022. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/14/9/269.

Cuzzocrea:2022:EES

[CKV22] Alfredo Cuzzocrea, Panagiotis Karras, and Akrivi Vlachou. Effective and efficient skyline query processing over attribute-order-preserving-free encrypted data in cloud-enabled databases. *Future Generation Computer Systems*, 126(??):237–251, January 2022. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X21003137.

Chen:2021:LBU

[CLH+21] Wenbin Chen, Jin Li, Zhengan Huang, Chongzhi Gao, Siuming Yiu, and Zoe L. Jiang. Lattice-based unidirectional infinite-use proxy re-signatures with private re-signature key. *Journal of Computer and System Sciences*, 120(??):137–148, September 2021. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000021000398.

Cao:2021:CED

[CLLR21] Xinle Cao, Jian Liu, Hao Lu, and Kui Ren. Cryptanalysis of an encrypted database in SIGMOD '14. *Proceedings of the VLDB Endowment*, 14(10):1743–1755, June 2021. CODEN ???? ISSN 2150-8097. URL https://dl.acm.org/doi/10.14778/3467861.3467865.

Castagnos:2022:TPC

[CLT22] Guilhem Castagnos, Fabien Laguillaumie, and Ida Tucker. A tighter proof for CCA secure inner product functional encryption: Genericity meets efficiency. *Theoretical Computer Science*, 914(??):84–113, May 7, 2022. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397522000913.

Chen:2022:ECA

[CLZG22] Ningyu Chen, Jiguo Li, Yichen Zhang, and Yuyan Guo. Efficient CP-ABE scheme with shared decryption in cloud storage. *IEEE Transactions on Computers*, 71(1):175–184, January 2022. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Caviglione:2021:KLT

[CMR+21] Luca Caviglione, Wojciech Mazurczyk, Matteo Repetto, Andreas Schaffhauser, and Marco Zuppelli. Kernel-level tracing for detecting stego-malware and covert channels in Linux environments. *Computer Networks (Amsterdam, Netherlands: 1999)*, 191(??):??, May 22, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128621001249`.

Choudhary:2021:MBB

[CN21] Swati K. Choudhary and Ameya K. Naik. Multimodal biometric-based authentication with secured templates. *International Journal of Image and Graphics (IJIG)*, 21 (02):??, April 2021. ISSN 0219-4678. URL `https://www.worldscientific.com/doi/10.1142/S0219467821500182`.

Chen:2020:NES

[CNL+20] Jiahui Chen, Jianting Ning, Jie Ling, Terry Shue Chien Lau, and Yacheng Wang. A new encryption scheme for multivariate quadratic systems. *Theoretical Computer Science*, 809(??):372–383, February 24, 2020. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397520300025`.

Cui:2021:TFD

[CPN+21] Hui Cui, Russell Paulet, Surya Nepal, Xun Yi, and Butrus Mbimbi. Two-factor decryption: a better way to protect data security and privacy. *The Computer Journal*, 64(4):550–563, April 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/64/4/550/5868155`.

Cui:2020:RDS

[CQSN20] Hui Cui, Baodong Qin, Willy Susilo, and Surya Nepal. Robust digital signature revisited. *Theoretical Computer Science*, 844(??):87–96, December 6, 2020. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S030439752030445X`.

Chang:2022:SMD

[CRJ+22] Jinyong Chang, Qiaochuan Ren, Yanyan Ji, Maozhi Xu, and Rui Xue. Secure medical data management with privacy-preservation and authentication properties in smart healthcare system. *Computer Networks (Amsterdam, Netherlands: 1999)*, 212(??):??, July 20, 2022. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http:`

//www.sciencedirect.com/science/article/pii/S1389128622001736.

Camacho-Ruiz:2021:TOH

[CRSSBMR21] Eros Camacho-Ruiz, Santiago Sánchez-Solano, Piedad Brox, and Macarena C. Martínez-Rodríguez. Timing-optimized hardware implementation to accelerate polynomial multiplication in the NTRU algorithm. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 17(3):35:1–35:16, July 2021. CODEN ???? ISSN 1550-4832. URL https://dl.acm.org/doi/10.1145/3445979.

Cui:2021:PPD

[CSA+21] Shujie Cui, Xiangfu Song, Muhammad Rizwan Asghar, Steven D. Galbraith, and Giovanni Russello. Privacy-preserving dynamic symmetric searchable encryption with controllable leakage. *ACM Transactions on Privacy and Security (TOPS)*, 24(3):18:1–18:35, April 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3446920.

Cocco:2021:BSS

[CTM21] Luisanna Cocco, Roberto Tonelli, and Michele Marchesi. Blockchain and self sovereign identity to support quality in the food supply chain. *Future Internet*, 13(12):301, November 26, 2021. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/13/12/301.

Cocco:2022:SPI

[CTM22] Luisanna Cocco, Roberto Tonelli, and Michele Marchesi. A system proposal for information management in building sector based on BIM, SSI, IoT and blockchain. *Future Internet*, 14(5):140, April 30, 2022. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/14/5/140.

Cheng:2021:MLN

[CWE+21] Jin Cheng, Yulei Wu, Yuepeng E, Junling You, Tong Li, Hui Li, and Jingguo Ge. MATEC: a lightweight neural network for online encrypted traffic classification. *Computer Networks (Amsterdam, Netherlands: 1999)*, 199(??):??, November 9, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128621004217.

Cheng:2021:SNQ

[CWS+21] Ke Cheng, Liangmin Wang, Yulong Shen, Hua Wang, Yongzhi Wang, Xiaohong Jiang, and Hong Zhong. Secure k-NN query on encrypted cloud data with multiple keys. *IEEE Transac-*

tions on Big Data, 7(4):689–702, 2021. ISSN 2332-7790.

Cao:2022:FSE

[CXC+22] Yibo Cao, Shiyuan Xu, Xue Chen, Yunhua He, and Shuo Jiang. A forward-secure and efficient authentication protocol through lattice-based group signature in VANETs scenarios. *Computer Networks (Amsterdam, Netherlands: 1999)*, 214(??):??, September 4, 2022. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128622002626`.

Chen:2021:CFV

[CXZ+21] Yanjiao Chen, Meng Xue, Jian Zhang, Qianyun Guan, Zhiyuan Wang, Qian Zhang, and Wei Wang. ChestLive: Fortifying voice-based authentication with chest motion biometric on smart devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 5(4):148:1–148:25, December 2021. CODEN ???? ISSN 2474-9567 (electronic). URL `https://dl.acm.org/doi/10.1145/3494962`.

Chowdhuryy:2022:LST

[CY22] Md Hafizul Islam Chowdhuryy and Fan Yao. Leaking secrets through modern branch predictors in the speculative world. *IEEE Transactions on Computers*, 71(9): 2059–2072, September 2022. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Chen:2022:NCB

[CZC22] Siyuan Chen, Peng Zeng, and Kim-Kwang Raymond Choo. A new code-based blind signature scheme. *The Computer Journal*, 65(7): 1776–1786, July 2022. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/65/7/1776/6236090`.

Dar:2020:CAE

[DAK+20a] Zaineb Dar, Adnan Ahmad, Farrukh Aslam Khan, Furkh Zeshan, Razi Iqbal, Hafiz Husnain Raza Sherazi, and Ali Kashif Bashir. A context-aware encryption protocol suite for edge computing-based IoT devices. *The Journal of Supercomputing*, 76(4): 2548–2567, April 2020. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Dhanasekaran:2020:RIS

[DAK20b] K. Dhanasekaran, P. Anandan, and N. Kumaratharan. A robust image steganography using teaching learning based optimization based edge detection model for smart cities. *Computa-*

tional Intelligence, 36(3): 1275–1289, August 2020. CODEN COMIE6. ISSN 0824-7935 (print), 1467-8640 (electronic).

Datta:2020:CPF

[Dat20] Pratish Datta. Constrained pseudorandom functions from functional encryption. *Theoretical Computer Science*, 809 (??):137–170, February 24, 2020. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397519307662`.

Devi:2020:TPP

[DC20] R. Ramya Devi and V. Vijaya Chamundeeswari. Triple DES: Privacy preserving in big data healthcare. *International Journal of Parallel Programming*, 48(3):515–533, June 2020. CODEN IJPPE5. ISSN 0885-7458 (print), 1573-7640 (electronic).

Dubey:2022:GML

[DCSA22] Anuj Dubey, Rosario Cammarota, Vikram Suresh, and Aydin Aysu. Guarding machine learning hardware against physical side-channel attacks. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 18(3):56:1–56:31, July 2022. CODEN ???? ISSN 1550-4832. URL `https://dl.acm.org/doi/10.1145/3465377`.

Dhir:2020:UBF

[DD20] S. Dhir and S. K. A. Devi. The use of biometric fingerprints for on-the-fly digital signing of documents. *Computer*, 53(2):57–67, February 2020. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

DArco:2021:SSS

[DDD21] Paolo D'Arco, Roberto De Prisco, and Alfredo De Santis. Secret sharing schemes for infinite sets of participants: a new design technique. *Theoretical Computer Science*, 859(??):149–161, March 6, 2021. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397521000347`.

Dottling:2021:IBE

[DG21] Nico Döttling and Sanjam Garg. Identity-based encryption from the Diffie–Hellman assumption. *Journal of the ACM*, 68(3):14:1–14:46, May 2021. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `https://dl.acm.org/doi/10.1145/3422370`.

Dhanuskodi:2020:TRS

[DH20] S. N. Dhanuskodi and D. Holcomb. Techniques to reduce switching and leakage energy in unrolled block ciphers. *IEEE Transactions on Computers*, 69(10):1414–1423,

2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Diffie:2021:HCW

[DH21] Whitfield Diffie and Martin Hellman. New directions in cryptography (1976). In *Ideas That Created the Future: Classic Papers of Computer Science* [Lew21], chapter 42, pages 421–440. ISBN 0-262-04530-3. LCCN Q124.6-127.2.

Dong:2020:RNF

[DJ20] Shi Dong and Raj Jain. Retraction notice to "Flow online identification method for the encrypted Skype" [YJNCA (2019) 75–85]. *Journal of Network and Computer Applications*, 161(??):??, July 1, 2020. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804520301399`.

Devi:2021:HCW

[DK21] V. Anusuya Devi and V. Kalaivani. Hybrid cryptosystem in wireless body area networks using message authentication code and modified and enhanced lattice-based cryptography (MAC-MELBC) in healthcare applications. *Concurrency and Computation: Practice and Experience*, 33 (9):e6132:1–e6132:??, May 10, 2021. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Dong:2021:SCL

[DKJ+21] Xingbo Dong, Soohyong Kim, Zhe Jin, Jung Yeon Hwang, Sangrae Cho, and Andrew Beng Jin Teoh. Secure chaffless fuzzy vault for face identification systems. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 17 (3):79:1–79:22, August 2021. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL `https://dl.acm.org/doi/10.1145/3442198`.

Drusinsky:2020:OTE

[DM20] D. Drusinsky and J. B. Michael. Obtaining trust in executable derivatives using crowdsourced critiques with blind signatures. *Computer*, 53(4):51–56, April 2020. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Dodds:2022:FVI

[Dod22] Mike Dodds. Formally verifying industry cryptography. *IEEE Security & Privacy*, 20 (3):65–70, May/June 2022. ISSN 1540-7993 (print), 1558-4046 (electronic).

Debnath:2020:UAS

[DR20] Saswati Debnath and Pinki Roy. User authentication system based on speech and cascade hybrid facial feature. *International Journal of Image and Graphics (IJIG)*, 20(03): ??, July 2020. ISSN 0219-4678. URL `https://www.worldscientific.com/doi/10.1142/S0219467820500229`.

Duong:2022:CCL

[DRS+22] Dung Hoang Duong, Partha Sarathi Roy, Willy Susilo, Kazuhide Fukushima, Shinsaku Kiyomoto, and Arnaud Sipasseuth. Chosen-ciphertext lattice-based public key encryption with equality test in standard model. *Theoretical Computer Science*, 905(??): 31–53, February 22, 2022. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397521007210`.

Drusinsky:2021:WAM

[Dru21] D. Drusinsky. Who is authenticating my e-commerce logins? *Computer*, 54(4): 49–54, April 2021. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Drusinsky:2022:CBS

[Dru22] Doron Drusinsky. Cryptographic–biometric self-sovereign personal identities. *Computer*, 55 (6):96–102, June 2022. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Dutta:2021:CRI

[DSDR21] Priyanka Dutta, Willy Susilo, Dung Hoang Duong, and Partha Sarathi Roy. Collusion-resistant identity-based Proxy Re-encryption: Lattice-based constructions in Standard Model. *Theoretical Computer Science*, 871(??):16–29, June 6, 2021. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397521002127`.

Dutta:2022:PIB

[DSDR22] Priyanka Dutta, Willy Susilo, Dung Hoang Duong, and Partha Sarathi Roy. Puncturable identity-based and attribute-based encryption from lattices. *Theoretical Computer Science*, 929(??): 18–38, September 11, 2022. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397522003954`.

Dehshibi:2020:RIB

[DSP20] Mohammad Mahdi Dehshibi, Jamshid Shanbehzadeh, and Mir Mohsen Pedram. A robust image-based cryptology scheme based on cellular non-linear network and local image descriptors. *International Journal of Parallel, Emergent and Distributed Systems: IJPEDS*, 35(5):514–534, 2020. CODEN ????

ISSN 1744-5760 (print), 1744-5779 (electronic).

Duong:2020:MBR

[DST20] Dung Hoang Duong, Willy Susilo, and Ha Thanh Nguyen Tran. A multivariate blind ring signature scheme. *The Computer Journal*, 63(8): 1194–1202, August 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/63/8/1194/5643521.

Dimitrov:2022:FGR

[DVA22] Vassil Dimitrov, Luigi Vigneri, and Vidal Attias. Fast generation of RSA keys using smooth integers. *IEEE Transactions on Computers*, 71(7):1575–1585, July 2022. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Dong:2020:CCE

[DZL+20] Cong Dong, Chen Zhang, Zhigang Lu, Baoxu Liu, and Bo Jiang. CETAnalytics: Comprehensive effective traffic information analytics for encrypted traffic classification. *Computer Networks (Amsterdam, Netherlands: 1999)*, 176 (??):Article 107258, July 20, 2020. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128619309466.

Dong:2022:EEA

[DZL+22] Jiankuo Dong, Fangyu Zheng, Jingqiang Lin, Zhe Liu, Fu Xiao, and Guang Fan. EC-ECC: Accelerating elliptic curve cryptography for edge computing on embedded GPU TX2. *ACM Transactions on Embedded Computing Systems*, 21(2):16:1–16:25, March 2022. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic). URL https://dl.acm.org/doi/10.1145/3492734.

Ding:2021:MSA

[DZW+21] Yaoling Ding, Liehuang Zhu, An Wang, Yuan Li, Yongjuan Wang, Siu Ming Yiu, and Keke Gai. A multiple sieve approach based on artificial intelligent techniques and correlation power analysis. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 17(2s):71:1–71:21, June 2021. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL https://dl.acm.org/doi/10.1145/3433165.

ElGhanam:2021:ABD

[EAHO21] Eiman ElGhanam, Ibtihal Ahmed, Mohamed Hassan, and Ahmed Osman. Authentication and billing for dynamic wireless EV charging in an Internet of Electric Vehicles. *Future Internet*, 13(10):257, October 08,

2021. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/13/10/257.

Elkoumy:2022:PCP

[EFPS+22] Gamal Elkoumy, Stephan A. Fahrenkrog-Petersen, Mohammadreza Fani Sani, Agnes Koschmider, Felix Mannhardt, Saskia Nuñez Von Voigt, Majid Rafiei, and Leopold Von Waldthausen. Privacy and confidentiality in process mining: Threats and research challenges. *ACM Transactions on Management Information Systems (TMIS)*, 13 (1):11:1–11:17, March 2022. CODEN ???? ISSN 2158-656X (print), 2158-6578 (electronic). URL https://dl.acm.org/doi/10.1145/3468877.

Emura:2020:SCF

[EIO20] Keita Emura, Katsuhiko Ito, and Toshihiro Ohigashi. Secure-channel free searchable encryption with multiple keywords: a generic construction, an instantiation, and its implementation. *Journal of Computer and System Sciences*, 114(??):107–125, December 2020. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000018304598.

Eriguchi:2020:SSL

[EK20] Reo Eriguchi and Noboru Kunihiro. Strong security of linear ramp secret sharing schemes with general access structures. *Information Processing Letters*, 164 (??):Article 106018, December 2020. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019020301058.

Ekhall:2024:TDC

[Ekh24] Magnus Ekhall. The TICOM DF-114 cryptanalytic device — a theory of operation and computer simulation. Report ??, ????, ????, June 2024. 10 pp. URL https://dspace.ut.ee/server/api/core/bitstreams/f707e86c-a7d6-421b-b904-267439ee1cee/content. Presented at HistoCrypt 2024, June 25–27, 2024, Oxford/Bletchley Park, UK.

Emura:2022:IBE

[EKW22] Keita Emura, Shuichi Katsumata, and Yohei Watanabe. Identity-based encryption with security against the KGC: a formal model and its instantiations. *Theoretical Computer Science*, 900 (??):97–119, January 8, 2022. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S030439752100699X.

Eltaief:2022:FCF

[Elt22] Hamdi Eltaief. Flex-CC:

a flexible connected chains scheme for multicast source authentication in dynamic SDN environment. *Computer Networks (Amsterdam, Netherlands: 1999)*, 214 (??):??, September 4, 2022. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128622002766.

Eyyunni:2021:IBF

[EMS21] Pramod Eyyunni, Bibekananda Maji, and Garima Sood. An inequality between finite analogues of rank and crank moments. *International Journal of Number Theory (IJNT)*, 17(02):405–423, March 2021. ISSN 1793-0421 (print), 1793-7310 (electronic). URL https://www.worldscientific.com/doi/10.1142/S1793042120400217.

Erbsen:2020:SHL

[EPG+20] Andres Erbsen, Jade Philipoom, Jason Gross, Robert Sloan, and Adam Chlipala. Simple high-level code for cryptographic arithmetic: With proofs, without compromises. *Operating Systems Review*, 54(1):23–30, August 2020. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic). URL https://dl.acm.org/doi/10.1145/3421473.3421477.

Er-rajy:2020:NSR

[ErEE20] Latifa Er-rajy, My Ahmed El Kiram, and Mohamed El Ghazouani. New security risk value estimate method for Android applications. *The Computer Journal*, 63(4):593–603, April 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/63/4/593/5618854.

Esfahani:2021:ECA

[ESA21] Mahdi Esfahani, Hadi Soleimany, and Mohammad Reza Aref. Enhanced cache attack on AES applicable on ARM-based devices with new operating systems. *Computer Networks (Amsterdam, Netherlands: 1999)*, 198 (??):??, October 24, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128621003790.

Echavarria:2022:CEE

[ESD+22] Karina Rodriguez Echavarria, Myrsini Samaroudi, Laurie Dibble, Edward Silverton, and Sophie Dixon. Creative experiences for engaging communities with cultural heritage through place-based narratives. *Journal on Computing and Cultural Heritage (JOCCH)*, 15(2):33:1–33:19, June 2022. CODEN ???? ISSN 1556-4673 (print), 1556-4711 (electronic). URL https://dl.acm.org/doi/10.1145/3479007.

Emura:2021:ERI

[ESW21] Keita Emura, Jae Hong Seo, and Yohei Watanabe. Efficient revocable identity-based encryption with short public parameters. *Theoretical Computer Science*, 863 (??):127–155, April 8, 2021. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397521001134.

El-Zawawy:2022:SSB

[EZBC22] Mohamed A. El-Zawawy, Alessandro Brighente, and Mauro Conti. SETCAP: Service-based energy-efficient temporal credential authentication protocol for Internet of Drones. *Computer Networks (Amsterdam, Netherlands: 1999)*, 206(??):??, April 7, 2022. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128622000305.

Fotohi:2021:SCB

[FA21] Reza Fotohi and Fereidoon Shams Aliee. Securing communication between things using blockchain technology based on authentication and SHA-256 to improving scalability in large-scale IoT. *Computer Networks (Amsterdam, Netherlands: 1999)*, 197(??):??, October 9, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128621003303.

Fagin:2020:IFC

[Fag20] Barry S. Fagin. Idempotent factorizations in the cryptography classroom. *Two-Year College Mathematics Journal*, 51(3):195–203, 2020. CODEN ???? ISSN 0049-4925 (print), 2325-9116 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/07468342.2020.1724495.

Fomichev:2022:NRC

[FAlS+22] Mikhail Fomichev, Luis F. Abanto-leon, Max Stiegler, Alejandro Molina, Jakob Link, and Matthias Hollick. Next2You: Robust copresence detection based on channel state information. *ACM Transactions on Internet of Things (TIOT)*, 3(2):11:1–11:31, May 2022. CODEN ???? ISSN 2691-1914 (print), 2577-6207 (electronic). URL https://dl.acm.org/doi/10.1145/3491244.

Fang:2021:PPM

[Fan21] Haokun Fang. Privacy preserving machine learning with homomorphic encryption and federated learning. *Future Internet*, 13(4):94, April 08, 2021. CODEN ???? ISSN

1999-5903. URL https://www.mdpi.com/1999-5903/13/4/94.

Fotouhi:2020:LST

[FBD+20] Mahdi Fotouhi, Majid Bayat, Ashok Kumar Das, Hossein Abdi Nasib Far, S. Morteza Pournaghi, and M. A. Doostari. A lightweight and secure two-factor authentication scheme for wireless body area networks in healthcare IoT. *Computer Networks (Amsterdam, Netherlands: 1999)*, 177(??):Article 107333, August 4, 2020. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128619316457.

Francq:2022:NTS

[FBH+22] Julien Francq, Loïc Besson, Paul Huynh, Philippe Guillot, Gilles Millerioux, and Marine Minier. Non-triangular self-synchronizing stream ciphers. *IEEE Transactions on Computers*, 71(1): 134–145, January 2022. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Ferdous:2021:SCA

[FCH21] Md Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, and Mohammad A. Hoque. A survey of consensus algorithms in public blockchain systems for crypto-currencies. *Journal of Network and Computer Applications*, 182(??):??, May 15, 2021. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804521000618.

Ferretti:2021:HSI

[Fer21] Marco Ferretti. H2O: Secure interactions in IoT via behavioral fingerprinting. *Future Internet*, 13(5):117, April 30, 2021. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/13/5/117.

Fischer:2022:CED

[FFK+22] Andreas Fischer, Benny Fuhry, Jörn Kußmaul, Jonas Janneck, Florian Kerschbaum, and Eric Bodden. Computation on encrypted data using dataflow authentication. *ACM Transactions on Privacy and Security (TOPS)*, 25(3):21:1–21:36, August 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3513005.

Feng:2022:BTE

[FGC22] Shengyuan Feng, Junqing Gong, and Jie Chen. Binary tree encryption with constant-size public key in the standard model. *The Computer Journal*, 65(6): 1489–1511, June 2022. CO-

DEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/65/6/1489/6154510`.

Fitzgerald:2022:ECP

[Fit22] Joshua Brian Fitzgerald. Elliptic curve pairings. *Computer*, 55(4):74–77, April 2022. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Fan:2020:FGA

[FLTQ20] Yongkai Fan, Shengle Liu, Gang Tan, and Fei Qiao. Fine-grained access control based on Trusted Execution Environment. *Future Generation Computer Systems*, 109 (??):551–561, August 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X17319362`.

Fei:2021:VAP

[FLYL21] Xiongwei Fei, Kenli Li, Wangdong Yang, and Keqin Li. Velocity-aware parallel encryption algorithm with low energy consumption for streams. *IEEE Transactions on Big Data*, 7(4):619–631, 2021. ISSN 2332-7790.

Fanfakh:2022:OGO

[FNC22] Ahmed Fanfakh, Hassan Noura, and Raphaël Couturier. ORSCA-GPU: one round stream cipher algorithm for GPU implementation. *The Journal of Supercomputing*, 78(9):11744–11767, June 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `https://link.springer.com/article/10.1007/s11227-022-04335-4`.

Freeman:2021:FAP

[Fre21] Peter E. Freeman. Facilitating authentic practice for early undergraduate statistics students. *The American Statistician*, 75 (4):433–444, 2021. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/00031305.2020.1844293`.

Feldmann:2022:AAC

[FSK+22] Axel Feldmann, Nikola Samardzic, Aleksandar Krastev, Srinivas Devadas, Ron Dreslinski, Chris Peikert, and Daniel Sanchez. An architecture to accelerate computation on encrypted data. *IEEE Micro*, 42(4):59–68, July/August 2022. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Farzadnia:2021:NID

[FSN21] Ehsan Farzadnia, Hossein Shirazi, and Alireza Nowroozi. A new intrusion detection system using the improved dendritic cell algorithm. *The*

Computer Journal, 64(8): 1193–1214, August 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/64/8/1193/6015901.

Fu:2022:PFS

[FWCB22] Junsong Fu, Na Wang, Baojiang Cui, and Bharat K. Bhargava. A practical framework for secure document retrieval in encrypted cloud file systems. *IEEE Transactions on Parallel and Distributed Systems*, 33(5):1246–1261, May 2022. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Fyrbiak:2020:GSA

[FWR+20] M. Fyrbiak, S. Wallat, S. Reinhard, N. Bissantz, and C. Paar. Graph similarity and its applications to hardware security. *IEEE Transactions on Computers*, 69(4): 505–519, April 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Fan:2020:HVS

[FWZ+20] Xingyue Fan, Ting Wu, Qiuhua Zheng, Yuanfang Chen, Muhammad Alam, and Xiaodong Xiao. HSE-Voting: a secure high-efficiency electronic voting scheme based on homomorphic signcryption. *Future Generation Computer Systems*, 111(??): 754–762, October 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X1931951X.

Fei:2021:SVS

[FYDX21] Shufan Fei, Zheng Yan, Wenxiu Ding, and Haomeng Xie. Security vulnerabilities of SGX and countermeasures: a survey. *ACM Computing Surveys*, 54(6): 126:1–126:36, July 2021. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/doi/10.1145/3456631.

Fu:2021:FAA

[FYY+21] Yunfei Fu, Hongchuan Yu, Chih-Kuo Yeh, Tong-Yee Lee, and Jian J. Zhang. Fast accurate and automatic brushstroke extraction. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 17 (2):44:1–44:24, June 2021. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL https://dl.acm.org/doi/10.1145/3429742.

Faghihi:2021:RDC

[FZ21] Farnood Faghihi and Mohammad Zulkernine. RansomCare: Data-centric detection and mitigation against smartphone crypto-ransomware.

Computer Networks (Amsterdam, Netherlands: 1999), 191(??):??, May 22, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128621001250`.

Fang:2021:CCE

[FZH21] Yong Fang, Yuchi Zhang, and Cheng Huang. CyberEyes: Cybersecurity entity recognition model based on graph convolutional network. *The Computer Journal*, 64(8): 1215–1225, August 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/64/8/1215/6012869`.

Fang:2020:HHR

[FZL+20a] Liming Fang, Hongwei Zhu, Boqing Lv, Zhe Liu, Weizhi Meng, Yu Yu, Shouling Ji, and Zehong Cao. HandiText: Handwriting recognition based on dynamic characteristics with incremental LSTM. *ACM Transactions on Data Science (TDS)*, 1(4): 25:1–25:18, December 2020. CODEN ???? ISSN 2691-1922. URL `https://dl.acm.org/doi/10.1145/3385189`.

Feng:2020:MIM

[FZL+20b] H. Feng, J. Zhou, W. Lin, Y. Zhang, and Z. Qu. Multiple-input, multilayer-perception-based classification of traces from side-channel attacks. *Computer*, 53(8):40–48, 2020. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Gajabe:2022:SKB

[GA22] Rajashree Gajabe and Syed Taqi Ali. Secret key-based image steganography in spatial domain. *International Journal of Image and Graphics (IJIG)*, 22(02):??, April 2022. CODEN ???? ISSN 0219-4678. URL `https://www.worldscientific.com/doi/10.1142/S0219467822500140`.

Garcia:2021:DRT

[GAGV+21] Norberto Garcia, Tomas Alcaniz, Aurora González-Vidal, Jorge Bernal Bernabe, Diego Rivera, and Antonio Skarmeta. Distributed real-time SlowDoS attacks detection over encrypted traffic using Artificial Intelligence. *Journal of Network and Computer Applications*, 173(??):??, January 1, 2021. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804520303362`.

Garske:2021:DCL

[Gar21] D. Garske. Deprecate CyaSSL library #151. GitHub document, 2021. URL `https://github.com/cyassl/cyassl/pull/151`.

Gomez-Barrero:2020:RIS

[GBG20] Marta Gomez-Barrero and Javier Galbally. Reversing the irreversible: a survey on inverse biometrics. *Computers & Security*, 90(??): Article 101700, March 2020. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167404819302378`.

Garriga:2021:BCC

[GDA+21] Martin Garriga, Stefano Dalla Palma, Maxmiliano Arias, Alan De Renzis, Remo Pareschi, and Damian Andrew Tamburri. Blockchain and cryptocurrencies: a classification and comparison of architecture drivers. *Concurrency and Computation: Practice and Experience*, 33 (8):e5992:1–e5992:??, April 25, 2021. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Guo:2021:PSE

[GDZL21] Junyan Guo, Ye Du, Yahang Zhang, and Meihong Li. A provably secure ECC-based access and handover authentication protocol for space information networks. *Journal of Network and Computer Applications*, 193(??):??, November 1, 2021. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804521001922`.

Gutterman:2020:RRT

[GGA+20] Craig Gutterman, Katherine Guo, Sarthak Arora, Trey Gilliland, Xiaoyang Wang, Les Wu, Ethan Katz-Bassett, and Gil Zussman. Requet: Real-time QoE metric detection for encrypted YouTube traffic. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 16(2s):71:1–71:28, July 2020. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3394498`.

Guo:2020:RDS

[GJCJ20] Cheng Guo, Xueru Jiang, Kim-Kwang Raymond Choo, and Yingmo Jie. R-Dedup: Secure client-side deduplication for encrypted data without involving a third-party entity. *Journal of Network and Computer Applications*, 162(??):??, July 15, 2020. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804520301387`.

Ghahramani:2020:SBB

[GJS20] Meysam Ghahramani, Reza Javidan, and Mohammad Shojafar. A secure biometric-based authentication protocol for global mobility networks in smart cities. *The Journal of Supercomputing*, 76(11):8729–8755, November 2020. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-020-03160-x.

Gao:2022:UNU

[GL22] Ming Gao and YuBin Lu. URAP: a new ultra-lightweight RFID authentication protocol in passive RFID system. *The Journal of Supercomputing*, 78(8):10893–10905, May 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-021-04252-y.

Goey:2021:ANT

[GLY21] Jia-Zheng Goey, Wai-Kong Lee, and Wun-She Yap. Accelerating number theoretic transform in GPU platform for fully homomorphic encryption. *The Journal of Supercomputing*, 77(2):1455–1474, February 2021. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-020-03156-7.

Guo:2020:ABE

[GLZZ20] Rui Guo, Xiong Li, Dong Zheng, and Yinghui Zhang. An attribute-based encryption scheme with multiple authorities on hierarchical personal health record in cloud. *The Journal of Supercomputing*, 76(7):4884–4903, July 2020. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Gentile:2022:VPA

[GMD+22] Antonio Francesco Gentile, Davide Macrì, Floriano De Rango, Mauro Tropea, and Emilio Greco. A VPN performances analysis of constrained hardware open source infrastructure deploy in IoT environment. *Future Internet*, 14(9):264, September 13, 2022. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/14/9/264.

Gupta:2020:ABS

[GMS+20] Nishu Gupta, Ravikanti Manaswini, Bongaram Saikrishna, Francisco Silva, and Ariel Teles. Authentication-based secure data dissemination protocol and framework for 5G-enabled VANET. *Future Internet*, 12(4):63, April 01, 2020. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/12/4/63.

Ganesh:2021:CRF

[GMV21] Chaya Ganesh, Bernardo Magri, and Daniele Venturi. Cryptographic reverse firewalls for interactive proof systems. *Theoretical Computer Science*, 855(??): 104–132, February 6, 2021. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397520306927.

Gnad:2021:VBC

[GNGT21] Dennis R. E. Gnad, Cong Dang Khoa Nguyen, Syed Hashim Gillani, and Mehdi B. Tahoori. Voltage-based covert channels using FPGAs. *ACM Transactions on Design Automation of Electronic Systems*, 26(6): 43:1–43:25, November 2021. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic). URL https://dl.acm.org/doi/10.1145/3460229.

Gokulkumari:2022:MEA

[Gok22] G. Gokulkumari. Metaheuristic-enabled artificial neural network framework for multimodal biometric recognition with local fusion visual features. *The Computer Journal*, 65(6):1586–1597, June 2022. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/65/6/1586/6167838.

Goodell:2021:DCA

[Goo21] Geoffrey Goodell. A digital currency architecture for privacy and owner-custodianship. *Future Internet*, 13(5):130, May 14, 2021. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/13/5/130.

Goodin:2023:FCK

[Goo23] Dan Goodin. In a first, cryptographic keys protecting SSH connections stolen in new attack. Ars Technica Web site, November 13, 2023. URL https://arstechnica.com/security/2023/11/hackers-can-steal-ssh-cryptographic-keys-in-new-cutting-edge-attack/. Details are in the technical paper [RHSH23].

Goudosis:2021:AOR

[Gou21] Athanasios Goudosis. ARIBC: Online reporting based on identity-based cryptography. *Future Internet*, 13(2):53, February 21, 2021. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/13/2/53.

Giannakoulopoulos:2022:ICO

[GPLK22] Andreas Giannakoulopoulos, Minas Pergantis, Laida Limniati, and Alexandros Kouretsis. Investigating the country of origin and the role of the `.eu` TLD in external trade of European Union member states. *Future Internet*, 14(6):174, June 04, 2022.

CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/14/6/174.

Gangwani:2021:SEI

[GPPB+21] Pranav Gangwani, Alexander Perez-Pons, Tushar Bhardwaj, Himanshu Upadhyay, Santosh Joshi, and Leonel Lagos. Securing environmental IoT data using masked authentication messaging protocol in a DAG-based blockchain: IOTA tangle. *Future Internet*, 13(12): 312, December 06, 2021. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/13/12/312.

Gai:2021:PPD

[GQZ21] Keke Gai, Meikang Qiu, and Hui Zhao. Privacy-preserving data encryption strategy for big data in mobile cloud computing. *IEEE Transactions on Big Data*, 7(4):678–688, 2021. ISSN 2332-7790.

Gwyn:2021:FRU

[GRA21] Tony Gwyn, Kaushik Roy, and Mustafa Atay. Face recognition using popular deep net architectures: a brief comparative study. *Future Internet*, 13(7):164, June 25, 2021. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/13/7/164.

Giti:2020:SCA

[GSS+20] J. E. Giti, A. Sakzad, B. Srinivasan, J. Kamruzzaman, and R. Gaire. Secrecy capacity against adaptive eavesdroppers in a random wireless network using friendly jammers and protected zone. *Journal of Network and Computer Applications*, 165(??):??, September 1, 2020. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804520301727.

Guan:2021:LKA

[Gua21] Albert Guan. A lightweight key agreement protocol with authentication capability. *International Journal of Foundations of Computer Science (IJFCS)*, 32(04):389–404, June 2021. ISSN 0129-0541. URL https://www.worldscientific.com/doi/10.1142/S0129054121500222.

Guerar:2020:CNA

[GVM+20] Meriem Guerar, Luca Verderame, Alessio Merlo, Francesco Palmieri, Mauro Migliardi, and Luca Vallerini. CirclePIN: a novel authentication mechanism for smartwatches to prevent unauthorized access to IoT devices. *ACM Transactions on Cyber-Physical Systems (TCPS)*, 4 (3):34:1–34:19, March 2020. CODEN ???? ISSN 2378-962X (print), 2378-9638 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3365995.

Guan:2021:ASS

[GWF+21] Zhitao Guan, Naiyu Wang, Xunfeng Fan, Xueyan Liu, Longfei Wu, and Shaohua Wan. Achieving secure search over encrypted data for e-commerce: a blockchain approach. *ACM Transactions on Internet Technology (TOIT)*, 21(1):12:1–12:17, February 2021. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic). URL https://dl.acm.org/doi/10.1145/3408309.

Gong:2022:SLC

[GWW+22] Bei Gong, Yong Wu, Qian Wang, Yu heng Ren, and Chong Guo. A secure and lightweight certificateless hybrid signcryption scheme for Internet of Things. *Future Generation Computer Systems*, 127(??):23–30, February 2022. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X21003356.

Guo:2020:MSC

[GWZ+20] Shaoyong Guo, Fengning Wang, Neng Zhang, Feng Qi, and Xuesong Qiu. Master-slave chain based trusted cross-domain authentication mechanism in IoT. *Journal of Network and Computer Applications*, 172(??):??, December 15, 2020. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804520302836.

Gao:2022:FVM

[GXS+22] Pengfei Gao, Hongyi Xie, Pu Sun, Jun Zhang, Fu Song, and Taolue Chen. Formal verification of masking countermeasures for arithmetic programs. *IEEE Transactions on Software Engineering*, 48(3):973–1000, March 2022. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic).

Gao:2021:HAF

[GXSC21] Pengfei Gao, Hongyi Xie, Fu Song, and Taolue Chen. A hybrid approach to formal verification of higher-order masked arithmetic programs. *ACM Transactions on Software Engineering and Methodology*, 30(3):26:1–26:42, May 2021. CODEN ATSMER. ISSN 1049-331X (print), 1557-7392 (electronic). URL https://dl.acm.org/doi/10.1145/3428015.

Guo:2022:DFE

[GXZ+22] Mengzhuo Guo, Zhongzhi Xu, Qingpeng Zhang, Xiuwu Liao, and Jiapeng Liu. Deciphering feature effects on decision-making in ordinal regression problems: an explainable ordinal factorization model. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 16(3):59:1–59:26, June 2022. CODEN ???? ISSN 1556-4681 (print), 1556-472X (electronic). URL https://dl.acm.org/doi/10.1145/3487048.

Gyongyosi:2020:SVD

[Gyo20] Laszlo Gyongyosi. Singular value decomposition assisted multicarrier continuous-variable quantum key distribution. *Theoretical Computer Science*, 801(??):35–63, January 1, 2020. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397519304645.

Guo:2020:AAS

[GZG20] Nan Guo, Cong Zhao, and Tianhan Gao. An anonymous authentication scheme for edge computing-based car–home connectivity services in vehicular networks. *Future Generation Computer Systems*, 106(??):659–671, May 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X19323179.

Guo:2022:SSR

[GZG22] Yimin Guo, Zhenfeng Zhang, and Yajun Guo. SecFHome: Secure remote authentication in fog-enabled smart home environment. *Computer Networks (Amsterdam, Netherlands: 1999)*, 207(??):??, April 22, 2022. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S138912862200041X.

Hammami:2021:LAA

[HBO21] Hamza Hammami, Sadok Ben Yahia, and Mohammad S. Obaidat. A lightweight anonymous authentication scheme for secure cloud computing services. *The Journal of Supercomputing*, 77(2):1693–1713, February 2021. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-020-03313-y.

Hu:2020:LKE

[HBS+20] J. Hu, M. Baldi, P. Santini, N. Zeng, S. Ling, and H. Wang. Lightweight key encapsulation using LDPC codes on FPGAs. *IEEE Transactions on Computers*, 69(3):327–341, March 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Hughes:2022:CIT

[HD22] James P. Hughes and Whitfield Diffie. The challenges of IoT, TLS, and random number generators in the real world: Bad random numbers are still with us and are proliferating in modern systems. *ACM Queue: Tomorrow's Computing Today*, 20(3):18–40, May 2022. CODEN AQCUAE. ISSN 1542-7730 (print), 1542-7749 (electronic). URL https://dl.acm.org/doi/10.1145/3546933.

Hayouni:2021:NEE

[HH21] Haythem Hayouni and Mohamed Hamdi. A novel energy-efficient encryption algorithm for secure data in WSNs. *The Journal of Supercomputing*, 77(5):4754–4777, May 2021. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-020-03465-x.

Huang:2021:ABT

[HHO+21] Jun Huang, Debiao He, Mohammad S. Obaidat, Pandi Vijayakumar, Min Luo, and Kim-Kwang Raymond Choo. The application of the blockchain technology in voting systems: a review. *ACM Computing Surveys*, 54 (3):60:1–60:28, June 2021. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/doi/10.1145/3439725.

Hameed:2020:LCE

[HIMM20] Mustafa Emad Hameed, Masrullizam Mat Ibrahim, Nurulfajar Abd Manap, and Ali A. Mohammed. A lossless compression and encryption mechanism for remote monitoring of ECG data using Huffman coding and CBC–AES. *Future Generation Computer Systems*, 111 (??):829–840, October 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X19313950.

Huang:2022:OEI

[HJHZ22] Yan Huang, Yan Jin, Zhi Hu, and Fangguo Zhang. Optimizing the evaluation of l-isogenous curve for isogeny-based cryptography. *Information Processing Letters*, 178(??):Article 106301, November 2022. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019022000588.

Han:2020:SMF

[HKC+20] Juhyeng Han, Seongmin Kim, Daeyang Cho, Byungkwon Choi, Jaehyeong Ha, and Dongsu Han. A secure middlebox framework for enabling visibility over multiple encryption protocols. *IEEE/ACM Transactions on Networking*, 28(6):

2727–2740, December 2020. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic). URL https://dl.acm.org/doi/10.1109/TNET.2020.3016785.

Hamada:2021:SCL

[HLG21] Louiza Hamada, Pascal Lorenz, and Marc Gilg. Security challenges for light emitting systems. *Future Internet*, 13(11):276, October 28, 2021. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/13/11/276.

Hu:2020:TEC

[HLH+20] Yang Hu, John C. S. Lui, Wenjun Hu, Xiaobo Ma, Jianfeng Li, and Xiao Liang. Taming energy cost of disk encryption software on data-intensive mobile devices. *Future Generation Computer Systems*, 107(??):681–691, June 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X17320113.

Hu:2022:NDP

[HLJW22] Xichao Hu, Yongqiang Li, Lin Jiao, and Mingsheng Wang. New division property propagation table: Applications to block ciphers with large S-boxes. *The Computer Journal*, 65(6):1560–1573, June 2022. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/65/6/1560/6134263.

Herzberg:2021:SMA

[HLS+21] Amir Herzberg, Hemi Leibowitz, Kent Seamons, Elham Vaziripour, Justin Wu, and Daniel Zappala. Secure messaging authentication ceremonies are broken. *IEEE Security & Privacy*, 19(2):29–37, 2021. ISSN 1540-7993 (print), 1558-4046 (electronic).

Han:2020:CSA

[HLSC20a] Jiawei Han, Yanheng Liu, Xin Sun, and Aiping Chen. Correction to: A self-adjusting quantum key renewal management scheme in classical network symmetric cryptography. *The Journal of Supercomputing*, 76(6):4231, June 2020. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/content/pdf/10.1007/s11227-018-2373-y.pdf. See [HLSC20b].

Han:2020:SAQ

[HLSC20b] Jiawei Han, Yanheng Liu, Xin Sun, and Aiping Chen. A self-adjusting quantum key renewal management scheme in classical network symmetric cryptography. *The Journal of Supercomputing*, 76(6):4212–4230, June 2020.

CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). See correction [HLSC20a].

Hu:2021:FSM

[HLZ21] Zhi Hu, Dongdai Lin, and Chang-An Zhao. Fast scalar multiplication of degenerate divisors for hyperelliptic curve cryptosystems. *Applied Mathematics and Computation*, 404(??):Article 126239, September 1, 2021. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0096300321003295`.

He:2021:GCF

[HMLZ21] Jiaji He, Haocheng Ma, Yanjiang Liu, and Yiqiang Zhao. Golden chip-free Trojan detection leveraging Trojan Trigger's side-channel fingerprinting. *ACM Transactions on Embedded Computing Systems*, 20(1):6:1–6:18, January 2021. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic). URL `https://dl.acm.org/doi/10.1145/3419105`.

Heydari:2020:KUI

[HMT+20] Mohammad Heydari, Alexios Mylonas, Vahid Heydari Fami Tafreshi, Elhadj Benkhelifa, and Surjit Singh. Known unknowns: Indeterminacy in authentication in IoT. *Future Generation Computer Systems*, 111 (??):278–287, October 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X1931982X`.

Halder:2022:EST

[HN22] Subir Halder and Thomas Newe. Enabling secure time-series data sharing via homomorphic encryption in cloud-assisted IIoT. *Future Generation Computer Systems*, 133 (??):351–363, August 2022. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X22001078`.

Hazari:2021:MLV

[HON21] Noor Ahmad Hazari, Ahmed Oun, and Mohammed Niamat. Machine learning vulnerability analysis of FPGA-based ring oscillator PUFs and counter measures. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 17(3):36:1–36:20, July 2021. CODEN ???? ISSN 1550-4832. URL `https://dl.acm.org/doi/10.1145/3445978`.

Hong:2022:MTC

[Hon22] Jason Hong. Modern tech can't shield your secret identity. *Communications of the Association for Computing Machinery*, 65(5):24–25, May 2022. CODEN CACMA2.

ISSN 0001-0782 (print), 1557-7317 (electronic). URL https://dl.acm.org/doi/10.1145/3524013.

Huaman:2020:AIS

[HOV20] Carlos Quinto Huamán, Ana Lucila Sandoval Orozco, and Luis Javier García Villalba. Authentication and integrity of smartphone videos through multimedia container structure analysis. *Future Generation Computer Systems*, 108(??):15–33, July 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X20300078.

Heuser:2020:LCT

[HPGM20] A. Heuser, S. Picek, S. Guilley, and N. Mentens. Lightweight ciphers and their side-channel resilience. *IEEE Transactions on Computers*, 69 (10):1434–1448, 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Hao:2021:ACF

[HRX+21] Xiaohan Hao, Wei Ren, Ruoting Xiong, Tianqing Zhu, and Kim-Kwang Raymond Choo. Asymmetric cryptographic functions based on generative adversarial neural networks for Internet of Things. *Future Generation Computer Systems*, 124(??): 243–253, November 2021. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X21001801.

Hurley-Smith:2020:QLC

[HSHC20] Darren Hurley-Smith and Julio Hernandez-Castro. Quantum leap and crash: Searching and finding bias in quantum random number generators. *ACM Transactions on Privacy and Security (TOPS)*, 23(3):16:1–16:25, July 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3398726.

Hughes:2021:BEM

[Hug21] James Prescott Hughes. *BadRandom: the effect and mitigations for low entropy random numbers in TLS*. Ph.D. dissertation, University of California, Santa Cruz, Santa Cruz, CA, 2021. xv + 101 pp. URL https://escholarship.org/uc/item/9528885m.

Howard:2020:BCF

[HV20] J. P. Howard and M. E. Vachino. Blockchain compliance with federal cryptographic information-processing standards. *IEEE Security & Privacy*, 18(1):65–70, January 2020. ISSN 1540-7993 (print), 1558-4046 (electronic).

Hubacek:2020:HCL

[HY20] Pavel Hubácek and Eylon Yogev. Hardness of continuous local search: Query complexity and cryptographic lower bounds. *SIAM Journal on Computing*, 49(6): 1128–1172, ???? 2020. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Hoque:2020:HPO

[HYK+20] Tamzidul Hoque, Kai Yang, Robert Karam, Shahin Tajik, Domenic Forte, Mark Tehranipoor, and Swarup Bhunia. Hidden in plaintext: an obfuscation-based countermeasure against FPGA bitstream tampering attacks. *ACM Transactions on Design Automation of Electronic Systems*, 25(1):4:1–4:32, January 2020. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3361147.

Huang:2020:ULT

[HYZ+20a] Meijuan Huang, Bo Yang, Mingwu Zhang, Lina Zhang, and Hongxia Hou. Updatable lossy trapdoor functions under consecutive leakage. *The Computer Journal*, 63(4):648–656, April 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/63/4/648/5667451.

Huang:2020:GCC

[HYZ+20b] Meijuan Huang, Bo Yang, Yi Zhao, Xin Wang, Yanwei Zhou, and Zhe Xia. A generic construction of CCA-secure deterministic encryption. *Information Processing Letters*, 154(??):Article 105865, February 2020. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019019301486.

Huang:2022:CLR

[HYZH22] Meijuan Huang, Bo Yang, Yanwei Zhou, and Xuewei Hu. Continual leakage-resilient hedged public-key encryption. *The Computer Journal*, 65(6):1574–1585, June 2022. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/65/6/1574/6134264.

Islam:2021:HLS

[ISK21] Sheikh Ariful Islam, Love Kumar Sah, and Srinivas Katkoori. High-level synthesis of key-obfuscated RTL IP with design lockout and camouflaging. *ACM Transactions on Design Automation of Electronic Systems*, 26 (1):6:1–6:35, January 2021. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic). URL https://dl.acm.org/doi/10.1145/3410337.

Ibrahim:2021:MFU

[ISOD21] Omar Adel Ibrahim, Savio Sciancalepore, Gabriele Oligeri, and Roberto Di Pietro. MAGNETO: Fingerprinting USB flash drives via unintentional magnetic emissions. *ACM Transactions on Embedded Computing Systems*, 20(1):8:1–8:26, January 2021. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic). URL https://dl.acm.org/doi/10.1145/3422308.

Jamshidpour:2020:SAD

[JA20] Sadegh Jamshidpour and Zahra Ahmadian. Security analysis of a dynamic threshold secret sharing scheme using linear subspace method. *Information Processing Letters*, 163 (??):Article 105994, November 2020. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019020300818.

Jakobsson:2020:PP

[Jak20] M. Jakobsson. Permissions and privacy. *IEEE Security & Privacy*, 18(2):46–55, March/April 2020. ISSN 1558-4046.

Jin:2022:ESC

[JCKH22] Sunghyun Jin, Sung Min Cho, HeeSeok Kim, and Seokhie Hong. Enhanced side-channel analysis on ECDSA employing fixed-base comb method. *IEEE Transactions on Computers*, 71(9):2341–2350, September 2022. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Ji:2022:DFM

[JCZ+22] Xiaoyu Ji, Yushi Cheng, Juchuan Zhang, Yuehan Chi, Wenyuan Xu, and Yi-Chao Chen. Device fingerprinting with magnetic induction signals radiated by CPU modules. *ACM Transactions on Sensor Networks*, 18(2):23:1–23:28, May 2022. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic). URL https://dl.acm.org/doi/10.1145/3495158.

Jin:2021:FSL

[JDZ+21] Xin Jin, Yuwei Duan, Ying Zhang, Yating Huang, Mengdong Li, Ming Mao, Amit Kumar Singh, and Yujie Li. Fast search of lightweight block cipher primitives via swarm-like metaheuristics for cyber security. *ACM Transactions on Internet Technology (TOIT)*, 21(4):93:1–93:15, July 2021. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic). URL https://dl.acm.org/doi/10.1145/3417296.

Jiang:2020:EBC

[JFK20] Zhen Hang Jiang, Yunsi

Fei, and David Kaeli. Exploiting bank conflict-based side-channel timing leakage of GPUs. *ACM Transactions on Architecture and Code Optimization*, 16(4): 1–24, January 2020. CODEN ???? ISSN 1544-3566 (print), 1544-3973 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3361870`.

Ji:2021:CSS

[JHS+21] Sai Ji, Rui Huang, Jian Shen, Xin Jin, and Youngju Cho. A certificateless signcryption scheme for smart home networks. *Concurrency and Computation: Practice and Experience*, 33(7):1, April 10, 2021. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Jayasinghe:2021:QQB

[JIR+21] Darshana Jayasinghe, Aleksandar Ignjatovic, Roshan Ragel, Jude Angelo Ambrose, and Sri Parameswaran. QuadSeal: Quadruple balancing to mitigate power analysis attacks with variability effects and electromagnetic fault injection attacks. *ACM Transactions on Design Automation of Electronic Systems*, 26(5):33:1–33:36, June 2021. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic). URL `https://dl.acm.org/doi/10.1145/3443706`.

Jarecki:2021:TFP

[JJK+21] Stanislaw Jarecki, Mohammed Jubur, Hugo Krawczyk, Nitesh Saxena, and Maliheh Shirvanian. Two-factor password-authenticated key exchange with end-to-end security. *ACM Transactions on Privacy and Security (TOPS)*, 24(3):17:1–17:37, April 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3446807`.

John:2020:SUT

[JJKJ20] B. John, S. Jörg, S. Koppal, and E. Jain. The security-utility trade-off for iris authentication and eye animation for social virtual avatars. *IEEE Transactions on Visualization and Computer Graphics*, 26(5): 1880–1890, 2020. CODEN ITVGEA. ISSN 1077-2626.

Jacomme:2021:EFA

[JK21a] Charlie Jacomme and Steve Kremer. An extensive formal analysis of multi-factor authentication protocols. *ACM Transactions on Privacy and Security (TOPS)*, 24(2):13:1–13:34, February 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3440712`.

Ju:2021:RNC

[JK21b] GwangSu Ju and UnGwang Ko. Research on a novel construction of probabilistic visual cryptography scheme $(k, n, 0, 1, 1)$-PVCS for threshold access structures. *Theoretical Computer Science*, 863(??):19–39, April 8, 2021. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397521000840.

Jeong:2021:MPP

[JKI+21] Junho Jeong, Donghyo Kim, Sun-Young Ihm, Yangsun Lee, and Yunsik Son. Multilateral personal portfolio authentication system based on hyperledger fabric. *ACM Transactions on Internet Technology (TOIT)*, 21(1):14:1–14:17, February 2021. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic). URL https://dl.acm.org/doi/10.1145/3423554.

Joshi:2021:SDI

[JKM21] Anand B. Joshi, Dhanesh Kumar, and D. C. Mishra. Security of digital images based on 3D Arnold cat map and elliptic curve. *International Journal of Image and Graphics (IJIG)*, 21(01):??, January 2021. ISSN 0219-4678. URL https://www.worldscientific.com/doi/10.1142/S0219467821500066.

Ji:2020:ASH

[JLZ+20] Xiaoyu Ji, Chaohao Li, Xinyan Zhou, Juchuan Zhang, Yanmiao Zhang, and Wenyuan Xu. Authenticating smart home devices via home limited channels. *ACM Transactions on Internet of Things (TIOT)*, 1(4):24:1–24:24, October 2020. CODEN ???? ISSN 2691-1914 (print), 2577-6207 (electronic). URL https://dl.acm.org/doi/10.1145/3399432.

Jha:2021:DED

[JMKM21] Nandan Kumar Jha, Sparsh Mittal, Binod Kumar, and Govardhan Mattela. DeepPeep: Exploiting design ramifications to decipher the architecture of compact DNNs. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 17(1):5:1–5:25, January 2021. CODEN ???? ISSN 1550-4832. URL https://dl.acm.org/doi/10.1145/3414552.

Jover:2020:SAS

[Jov20] Roger Piqueras Jover. Security analysis of SMS as a second factor of authentication: The challenges of multifactor authentication based on SMS, including cellular security deficiencies, SS7 exploits, and SIM swapping. *ACM Queue: Tomorrow's Computing Today*, 18(4):37–60, August 2020. URL https:/

/dl.acm.org/doi/10.1145/3424302.3425909.

Jauernig:2020:TEE

[JSS20] P. Jauernig, A. Sadeghi, and E. Stapf. Trusted execution environments: Properties, applications, and challenges. *IEEE Security & Privacy*, 18(2):56–60, March/April 2020. ISSN 1558-4046.

Sun:2020:NAC

[jSZyW+20] Yu jie Sun, Hao Zhang, Xing yuan Wang, Xiao qing Wang, and Peng fei Yan. 2D non-adjacent coupled map lattice with q and its applications in image encryption. *Applied Mathematics and Computation*, 373(??): Article 125039, May 15, 2020. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300320300084.

Jiang:2020:SCR

[JTGJ20] Jiafu Jiang, Linyu Tang, Ke Gu, and WeiJia Jia. Secure computing resource allocation framework for open fog computing. *The Computer Journal*, 63(4):567–592, April 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/63/4/567/5717858.

Jiang:2020:SLW

[JYH+20] Shunzhi Jiang, Dengpan Ye, Jiaqing Huang, Yueyun Shang, and Zhuoyuan Zheng. SmartSteganogaphy: Lightweight generative audio steganography model for smart embedding application. *Journal of Network and Computer Applications*, 165 (??):??, September 1, 2020. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804520301636.

Jahanshahi:2020:NFO

[JYMP+20] Hadi Jahanshahi, Amin Yousefpour, Jesus M. Munoz-Pacheco, Sezgin Kacar, Viet-Thanh Pham, and Fawaz E. Alsaadi. A new fractional-order hyperchaotic memristor oscillator: Dynamic analysis, robust adaptive synchronization, and its application to voice encryption. *Applied Mathematics and Computation*, 383(??): Article 125310, October 15, 2020. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300320302769.

Ji:2021:IMS

[JZD21] Fulei Ji, Wentao Zhang, and Tianyou Ding. Improving Matsui's search algorithm for the best differential/linear trails and its applications for DES, DESL and GIFT. *The Computer Journal*, 64(4):610–627, April 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/64/4/610/5880463.

Jiang:2020:EAP

[JZWX20] Yan Jiang, Youwen Zhu, Jian Wang, and Yong Xiang. Efficient authentication protocol with anonymity and key protection for mobile Internet users. *Journal of Parallel and Distributed Computing*, 137(??):179–191, March 2020. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731519303107.

Karabulut:2022:EFC

[KAA22] Emre Karabulut, Erdem Alkim, and Aydin Aysu. Efficient, flexible, and constant-time Gaussian sampling hardware for lattice cryptography. *IEEE Transactions on Computers*, 71(8):1810–1823, August 2022. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Kaddoura:2021:PDD

[Kad21] Sanaa Kaddoura. A parallelized database damage assessment approach after cyberattack for healthcare systems. *Future Internet*, 13(4):90, March 31, 2021. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/13/4/90.

Khanal:2022:UBI

[KAS+22] Yurika Pant Khanal, Abeer Alsadoon, Khurram Shahzad, Ahmad B. Al-Khalil, Penatiyana W. C. Prasad, Sabih Ur Rehman, and Rafiqul Islam. Utilizing blockchain for IoT privacy through enhanced ECIES with secure hash function. *Future Internet*, 14(3):77, February 28, 2022. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/14/3/77.

Ku-Cauich:2020:LCB

[KCML20] Juan Carlos Ku-Cauich and Guillermo Morales-Luna. A linear code based on resilient Boolean maps whose dual is a platform for a robust secret sharing scheme. *Linear Algebra and its Applications*, 596(??):216–229, July 1, 2020. CODEN LAAPAW. ISSN 0024-3795 (print), 1873-1856 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0024379520301312.

Khadem:2020:IAP

[KG20a] Behrooz Khadem and Reza Ghasemi. Improved algorithms in parallel evaluation of large cryptographic S-boxes. *International*

Journal of Parallel, Emergent and Distributed Systems: IJPEDS, 35(4):461–472, 2020. CODEN ???? ISSN 1744-5760 (print), 1744-5779 (electronic).

Kumar:2020:EDC

[KG20b] Priyan Malarvizhi Kumar and Usha Devi Gandhi. Enhanced DTLS with CoAP-based authentication scheme for the Internet of Things in healthcare application. *The Journal of Supercomputing*, 76(6):3963–3983, June 2020. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Khan:2021:SCL

[Kha21] Shawal Khan. Security challenges of location privacy in VANETs and state-of-the-art solutions: a survey. *Future Internet*, 13(4):96, April 10, 2021. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/13/4/96`.

Ko:2020:PBN

[KHM20] Kyi Thar Ko, Htet Htet Hlaing, and Masahiro Mambo. A PEKS-based NDN strategy for name privacy. *Future Internet*, 12(8):130, July 31, 2020. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/12/8/130`.

Khan:2020:MAS

[KHV20] Hassan Khan, Urs Hengartner, and Daniel Vogel. Mimicry attacks on smartphone keystroke authentication. *ACM Transactions on Privacy and Security (TOPS)*, 23(1):2:1–2:34, February 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3372420`.

Krishnan:2021:SEQ

[KJJ+21] Prabhakar Krishnan, Kurunandan Jain, Pramod George Jose, Krishnashree Achuthan, and Rajkumar Buyya. SDN enabled QoE and security framework for multimedia applications in 5G networks. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 17(2):39:1–39:29, June 2021. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL `https://dl.acm.org/doi/10.1145/3377390`.

Kaur:2020:PPR

[KK20] Harkeerat Kaur and Pritee Khanna. Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing. *Future Generation Computer Systems*, 102(??):30–41, January 2020. CODEN FGSEVI. ISSN

0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X18330553.

Kim:2020:RAA

[KKBL20] Hokeun Kim, Eunsuk Kang, David Broman, and Edward A. Lee. Resilient authentication and authorization for the Internet of Things (IoT) using edge computing. *ACM Transactions on Internet of Things (TIOT)*, 1 (1):4:1–4:27, February 2020. CODEN ???? ISSN 2691-1914 (print), 2577-6207 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3375837.

Kubilay:2021:KEP

[KKM21] Murat Yasin Kubilay, Mehmet Sabir Kiraz, and Haci Ali Mantar. KORGAN: an efficient PKI architecture based on PBFT through dynamic threshold signatures. *The Computer Journal*, 64(4):564–574, April 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/64/4/564/5890396.

Kaboli:2021:GCH

[KKP21] Reza Kaboli, Shahram Khazaei, and Maghsoud Parviz. On group-characterizability of homomorphic secret sharing schemes. *Theoretical Computer Science*, 891(??):116–130, November 4, 2021. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397521005090.

Kim:2022:PPE

[KLC22] Hyeong-Jin Kim, Hyunjo Lee, and Jae-Woo Chang. Privacy-preserving k NN query processing algorithms via secure two-party computation over encrypted database in cloud computing. *The Journal of Supercomputing*, 78(7):9245–9284, May 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-021-04286-2.

Kim:2020:TRO

[KLP20] Eunkyung Kim, Hyang-Sook Lee, and Jeongeun Park. Towards round-optimal secure multiparty computations: Multikey FHE without a CRS. *International Journal of Foundations of Computer Science (IJFCS)*, 31(2):157–174, February 2020. CODEN IFCSEN. ISSN 0129-0541. URL https://www.worldscientific.com/doi/10.1142/S012905412050001X.

Krishnankutty:2020:ISI

[KLR+20] D. Krishnankutty, Z. Li, R. Robucci, N. Banerjee, and C. Patel. Instruction sequence identification and disassembly using power supply side-channel analysis. *IEEE Transactions on Computers*, 69(11):1639–1653, November 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Kim:2021:TER

[KLZ+21] H. M. Kim, M. Laskowski, M. Zargham, H. Turesson, M. Barlin, and D. Kabanov. Token economics in real life: Cryptocurrency and incentives design for Insolar's blockchain network. *Computer*, 54(1):70–80, 2021. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Kumar:2022:RRA

[KMK22] Vinod Kumar, Mahmoud Shuker Mahmoud, and Adesh Kumari. RAPCHI: Robust authentication protocol for IoMT-based cloud-healthcare infrastructure. *The Journal of Supercomputing*, 78 (14):16167–16196, September 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-022-04513-4.

Katsumata:2020:LBR

[KMT20] Shuichi Katsumata, Takahiro Matsuda, and Atsushi Takayasu. Lattice-based revocable (hierarchical) IBE with decryption key exposure resistance. *Theoretical Computer Science*, 809(??):103–136, February 24, 2020. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397519307650.

Koot:2020:FNC

[Koo20] Matthijs Koot. Field note on CVE-2019-11510: Pulse connect secure SSL-VPN in The Netherlands. *Digital Threats: Research and Practice (DTRAP)*, 1(2):13:1–13:7, July 2020. CODEN ???? ISSN ???? URL https://dl.acm.org/doi/abs/10.1145/3382765.

Koutsos:2021:DSS

[Kou21] Adrien Koutsos. Decidability of a sound set of inference rules for computational indistinguishability. *ACM Transactions on Computational Logic*, 22(1):3:1–3:44, January 2021. CODEN ???? ISSN 1529-3785 (print), 1557-945X (electronic). URL https://dl.acm.org/doi/10.1145/3423169.

Koziol:2020:NES

[Koz20] M. Koziol. New encryption strategy passes early test: Ghost polarization harnesses ultrafast fluctuations that occur in a light wave. *IEEE Spectrum*, 57(7):11, 2020. CODEN IEEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Khan:2020:BSU

[KPG+20] Saad Khan, Simon Parkinson, Liam Grant, Na Liu, and Stephen Mcguire. Biometric systems utilising health data from wearable devices: Applications and future challenges in computer security. *ACM Computing Surveys*, 53(4): 85:1–85:29, September 2020. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/doi/10.1145/3400030.

Kumaresan:2020:TVA

[KS20] S. Kumaresan and Vijayaragavan Shanmugam. Time-variant attribute-based multitype encryption algorithm for improved cloud data security using user profile. *The Journal of Supercomputing*, 76(8):6094–6112, August 2020. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

K:2021:PPB

[KS21a] Reshma V. K and Vinod Kumar R. S. Pixel prediction-based image steganography by support vector neural network. *The Computer Journal*, 64(5):731–748, May 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/64/5/731/5819403.

Karbasi:2021:SLS

[KS21b] Amir Hassani Karbasi and Siyamak Shahpasand. SINGLETON: A lightweight and secure end-to-end encryption protocol for the sensor networks in the Internet of Things based on cryptographic ratchets. *The Journal of Supercomputing*, 77(4): 3516–3554, April 2021. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-020-03411-x.

Karacay:2020:IDE

[KSA20] Leyli Karaçay, Erkay Savaş, and Halit Alptekin. Intrusion detection over encrypted network data. *The Computer Journal*, 63(4):604–619, April 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/63/4/604/5618960.

Kruger:2021:CEA

[KSA+21] Stefan Krüger, Johannes Späth, Karim Ali, Eric Bodden, and Mira Mezini. CrySL: An extensible approach to validating the correct usage of cryptographic APIs. *IEEE Transactions on Software Engineering*, 47(11): 2382–2400, November 2021. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic).

Krol:2021:PPU

[KSAB+21] Michał Król, Alberto Sonnino, Mustafa Al-Bassam, Argyrios G. Tasiopoulos, Etienne Rivière, and Ioannis Psaras. Proof-of-prestige: a useful work reward system for unverifiable tasks. *ACM Transactions on Internet Technology (TOIT)*, 21(2):44:1–44:27, June 2021. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic). URL `https://dl.acm.org/doi/10.1145/3419483`.

Kumar:2022:CSA

[KSC+22] Ashish Kumar, Rahul Saha, Mauro Conti, Gulshan Kumar, William J. Buchanan, and Tai Hoon Kim. A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions. *Journal of Network and Computer Applications*, 204(??):??, August 2022. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804522000716`.

Kansal:2022:EMS

[KSD22] Meenakshi Kansal, Amit Kumar Singh, and Ratna Dutta. Efficient multi-signature scheme using lattice. *The Computer Journal*, 65(9):2421–2429, September 2022. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/65/9/2421/6289877`.

Ko:2020:DWB

[KSK20] Woo-Hyun Ko, Bharadwaj Satchidanandan, and P. R. Kumar. Dynamic watermarking-based defense of transportation cyber-physical systems. *ACM Transactions on Cyber-Physical Systems (TCPS)*, 4(1):12:1–12:21, January 2020. CODEN ???? ISSN 2378-962X (print), 2378-9638 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3361700`.

Kumar:2022:NAT

[KSM22] Sunil Kumar, Harshdeep Singh, and Gaurav Mittal. A novel approach towards degree and Walsh-transform of Boolean functions. *International Journal of Foundations of Computer Science (IJFCS)*, 33(05):453–479, August 2022. ISSN 0129-0541. URL `https://www.worldscientific.com/doi/10.1142/S0129054122500101`.

Kumaravelu:2020:CES

[KSS+20] Ramesh Kumaravelu, Rajakumar Sadaiyandi, Anandamurugan Selvaraj, Jeeva Selvaraj, and Gayathiri Karthick. Computationally efficient and secure anonymous authentication scheme for IoT-based mobile pay-TV systems. *Computational Intelligence*, 36(3):994–1009, August 2020. CODEN COMIE6. ISSN 0824-7935 (print), 1467-8640 (electronic).

Kaur:2020:CIE

[KSSR20] Manjit Kaur, Dilbag Singh, Kehui Sun, and Umashankar Rawat. Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map. *Future Generation Computer Systems*, 107(??):333–350, June 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X19324707`.

Kapassa:2021:BAI

[KTCI21] Evgenia Kapassa, Marinos Themistocleous, Klitos Christodoulou, and Elias Iosif. Blockchain application in Internet of Vehicles: Challenges, contributions and current limitations. *Future Internet*, 13(12):313, December 10, 2021. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/13/12/313`.

Levi:2022:NCN

[LA22] Anthony F. J. Levi and Gabriel Aeppli. The naked chip: No trade secret or hardware trojan can hide from ptychographic X-ray laminography. *IEEE Spectrum*, 59(5):38–43, May 2022. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Liu:2020:ESI

[LAKS20] Z. Liu, R. Azarderakhsh, H. Kim, and H. Seo. Efficient software implementation of ring-LWE encryption on IoT processors. *IEEE Transactions on Computers*, 69(10):1424–1433, 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Luo:2021:ABP

[LAKWC21] Fucai Luo, Saif Al-Kuwari, Fuqun Wang, and Kefei Chen. Attribute-based proxy re-encryption from standard lattices. *Theoretical Computer Science*, 865 (??):52–62, April 14, 2021. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397521001201`.

LaMacchia:2022:SLR

[LaM22] Brian LaMacchia. Security: The long road ahead to transition to post-quantum cryptography. *Communications of the Association for Computing Machinery*, 65(1):28–30, January 2022. CODEN CACMA2. ISSN

0001-0782 (print), 1557-7317 (electronic). URL https://dl.acm.org/doi/10.1145/3498706.

Lapworth:2022:PEI

[Lap22] Leigh Lapworth. Parallel encryption of input and output data for HPC applications. *The International Journal of High Performance Computing Applications*, 36 (2):231–250, March 1, 2022. CODEN IHPCFL. ISSN 1094-3420 (print), 1741-2846 (electronic). URL https://journals.sagepub.com/doi/full/10.1177/10943420211016516.

Li:2021:EPK

[LB21] Qinyi Li and Xavier Boyen. Efficient public-key encryption with equality test from lattices. *Theoretical Computer Science*, 892(??):85–107, November 12, 2021. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397521005259.

Li:2022:IMM

[LC22] Manman Li and Shaozhen Chen. Improved meet-in-the-middle attacks on reduced-round tweakable block cipher Deoxys-BC. *The Computer Journal*, 65(9):2411–2420, September 2022. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/65/9/2411/6291059.

Li:2021:FGA

[LCZL21] Guangsong Li, Wei Chen, Bin Zhang, and Siqi Lu. A fine-grained anonymous handover authentication protocol based on consortium blockchain for wireless networks. *Journal of Parallel and Distributed Computing*, 157(??):157–167, November 2021. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731521001362.

Luo:2022:FDF

[LDX22] Yukui Luo, Shijin Duan, and Xiaolin Xu. FPGAPRO: a defense framework against crosstalk-induced secret leakage in FPGA. *ACM Transactions on Design Automation of Electronic Systems*, 27(3):24:1–24:31, May 2022. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic). URL https://dl.acm.org/doi/10.1145/3491214.

Lachtar:2020:CSA

[LEBM20] Nada Lachtar, Abdulrahman Abu Elkhail, Anys Bacha, and Hafiz Malik. A cross-stack approach towards defending against cryptojacking. *IEEE Computer Architecture Letters*, 19(2): 126–129, 2020. ISSN 1556-

6056 (print), 1556-6064 (electronic).

Lee:2021:RHI

[Lee21] Kwangsu Lee. Revocable hierarchical identity-based encryption with adaptive security. *Theoretical Computer Science*, 880(??):37–68, August 3, 2021. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397521003376.

Lemire:2024:ESP

[Lem24] Daniel Lemire. Exact short products from truncated multipliers. *The Computer Journal*, 67(4):1514–1520, April 2024. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/67/4/1514/7306807; https://arxiv.org/abs/2303.14321v1.

Lewis:2020:MHP

[Lew20] P. Lewis. Make a hack-proof garage door opener: A new breakout board offers cryptographic security — [hands on]. *IEEE Spectrum*, 57(3):16–18, March 2020. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Lewis:2021:ICF

[Lew21] Harry R. Lewis. *Ideas That Created the Future: Classic Papers of Computer Science*. MIT Press, Cambridge, MA, USA, 2021. ISBN 0-262-04530-3. xxii + 495 pp. LCCN Q124.6-127.2.

Li:2020:EAI

[LFJ+20] Liandeng Li, Jiarui Fang, Jinlei Jiang, Lin Gan, Weijie Zheng, Haohuan Fu, and Guangwen Yang. Efficient AES implementation on Sunway TaihuLight supercomputer: a systematic approach. *Journal of Parallel and Distributed Computing*, 138(??):178–189, April 2020. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731519301108.

Liao:2022:BBI

[LGCY22] Chia-Hung Liao, Xue-Qin Guan, Jen-Hao Cheng, and Shyan-Ming Yuan. Blockchain-based identity management and access control framework for open banking ecosystem. *Future Generation Computer Systems*, 135(??):450–466, October 2022. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X22001868.

Larrucea:2020:AEM

[LGNEAO20] Xabier Larrucea, Pablo González-Nalda, Ismael Etxeberria-Agiriano, and Mari Carmen

Otero. Analysing encryption mechanisms and functional safety in a ROS-based architecture. *Journal of Software: Evolution and Process*, 32(2): e2224:1–e2224:??, February 2020. CODEN ???? ISSN 2047-7473 (print), 2047-7481 (electronic).

Luo:2020:HTI

[LGT+20] Entao Luo, Kehua Guo, Yayuan Tang, Xiangdong Ying, and Wen Huang. Hidden the true identity and dating characteristics based on quick private matching in mobile social networks. *Future Generation Computer Systems*, 109 (??):633–641, August 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X17320149`.

Lai:2020:CSC

[LHAM20] Junzuo Lai, Zhengan Huang, Man Ho Au, and Xianping Mao. Constant-size CCA-secure multi-hop unidirectional proxy re-encryption from indistinguishability obfuscation. *Theoretical Computer Science*, 847(??):1–16, December 22, 2020. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397520305302`.

Lai:2022:PSO

[LHHW22] Jianchang Lai, Xinyi Huang, Debiao He, and Wei Wu. Provably secure online/offline identity-based signature scheme based on SM9. *The Computer Journal*, 65 (7):1692–1701, July 2022. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/65/7/1692/6189769`.

Liu:2020:BBI

[LHO+20] Yang Liu, Debiao He, Mohammad S. Obaidat, Neeraj Kumar, Muhammad Khurram Khan, and Kim-Kwang Raymond Choo. Blockchain-based identity management systems: a review. *Journal of Network and Computer Applications*, 166(??): ??, September 15, 2020. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804520302058`.

Li:2022:ESS

[LHR+22] Jingwei Li, Suyu Huang, Yanjing Ren, Zuoru Yang, Patrick P. C. Lee, Xiaosong Zhang, and Yao Hao. Enabling secure and space-efficient metadata management in encrypted deduplication. *IEEE Transactions on Computers*, 71(4): 959–970, April 2022. CODEN ITCOB4. ISSN 0018-

9340 (print), 1557-9956 (electronic).

Li:2022:TCC

[LHS+22] Ying Li, Yi Huang, Suranga Seneviratne, Kanchana Thilakarathna, Adriel Cheng, Guillaume Jourjon, Darren Webb, David B. Smith, and Richard Yi Da Xu. From traffic classes to content: a hierarchical approach for encrypted traffic classification. *Computer Networks (Amsterdam, Netherlands: 1999)*, 212(??):??, July 20, 2022. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S138912862200175X`.

Liu:2021:EAB

[LHW21] Zhen Liu, Qiong Huang, and Duncan S Wong. On enabling attribute-based encryption to be traceable against traitors. *The Computer Journal*, 64(4):575–598, April 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/64/4/575/5874143`.

Liu:2021:LFD

[LHY+21] Jianghua Liu, Jingyu Hou, Wenjie Yang, Yang Xiang, Wanlei Zhou, Wei Wu, and Xinyi Huang. Leakage-free dissemination of authenticated tree-structured data with multi-party control. *IEEE Transactions on Computers*, 70(7):1120–1131, 2021. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Li:2020:SSB

[LHZZ20] Yantao Li, Hailong Hu, Zhangqian Zhu, and Gang Zhou. SCANet: Sensor-based continuous authentication with two-stream convolutional neural networks. *ACM Transactions on Sensor Networks*, 16(3):29:1–29:27, August 2020. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3397179`.

Lindner:2020:IDA

[LIJ20] Sebastian Lindner, Laurent Imbert, and Michael J. Jacobson. Improved divisor arithmetic on generic hyperelliptic curves. *ACM Communications in Computer Algebra*, 54(3):95–99, September 2020. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic). URL `https://dl.acm.org/doi/10.1145/3457341.3457345`.

Lee:2020:SBP

[LIS20] Jaekyu Lee, Yasuo Ishii, and Dam Sunwoo. Securing branch predictors with two-level encryption. *ACM Transactions on Architecture and Code Optimization*, 17

(3):21:1–21:25, August 2020. CODEN ???? ISSN 1544-3566 (print), 1544-3973 (electronic). URL https://dl.acm.org/doi/10.1145/3404189.

Liu:2020:CCB

[LKX20] Hongjun Liu, Abdurahman Kadir, and Chengbo Xu. Cryptanalysis and constructing S-Box based on chaotic map and backtracking. *Applied Mathematics and Computation*, 376(??): Article 125153, July 1, 2020. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300320301223.

Liu:2021:DVV

[LLA+21] Yanwei Liu, Jinxia Liu, Antonios Argyriou, Siwei Ma, Liming Wang, and Zhen Xu. 360-degree VR video watermarking based on spherical wavelet transform. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 17 (1):38:1–38:23, April 2021. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL https://dl.acm.org/doi/10.1145/3425605.

Lu:2022:EKE

[LLAL22] Jinyu Lu, Yunwen Liu, Tomer Ashur, and Chao Li. On the effect of the key-expansion algorithm in Simon-like ciphers. *The Computer Journal*, 65(9): 2454–2469, September 2022. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/65/9/2454/6314722.

Li:2021:FHO

[LLH+21] Dongjie Li, Siyi Lv, Yanyu Huang, Yijing Liu, Tong Li, Zheli Liu, and Liang Guo. Frequency-hiding order-preserving encryption with small client storage. *Proceedings of the VLDB Endowment*, 14(13):3295–3307, September 2021. CODEN ???? ISSN 2150-8097. URL https://dl.acm.org/doi/10.14778/3484224.3484228.

Liu:2022:TCS

[LLHG22] Xiangyu Liu, Shengli Liu, Shuai Han, and Dawu Gu. Tightly CCA-secure inner product functional encryption scheme. *Theoretical Computer Science*, 898 (??):1–19, January 4, 2022. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397521006009.

Li:2021:SIB

[LLLZ21] Xiong Li, Shanpeng Liu, Rongxing Lu, and Xiaosong Zhang. On security of an identity-based dynamic data auditing protocol for big data storage. *IEEE Transactions on Big Data*, 7(6):975–977, December 2021. CODEN ???? ISSN 2332-7790.

Liu:2020:DPS

[LLP+20] Yue Liu, Qinghua Lu, Hye-Young Paik, Xiwei Xu, Shiping Chen, and Liming Zhu. Design pattern as a service for blockchain-based self-sovereign identity. *IEEE Software*, 37(5):30–36, September/October 2020. CODEN IESOEG. ISSN 0740-7459 (print), 1937-4194 (electronic).

Li:2020:ILE

[LLT+20] Jingwei Li, Patrick P. C. Lee, Chufeng Tan, Chuan Qin, and Xiaosong Zhang. Information leakage in encrypted deduplication via frequency analysis: Attacks and defenses. *ACM Transactions on Storage*, 16(1):4:1–4:30, April 2020. CODEN ???? ISSN 1553-3077 (print), 1553-3093 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3365840`.

Li:2020:PPS

[LLX+20] Dong Li, Xiaofeng Liao, Tao Xiang, Jiahui Wu, and Junqing Le. Privacy-preserving self-serviced medical diagnosis scheme based on secure multi-party computation. *Computers & Security*, 90(??):Article 101701, March 2020. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S016740481930238X`.

Li:2020:MUD

[LMG20] Juyan Li, Chunguang Ma, and Zhen Gu. Multi-use deterministic public key proxy re-encryption from lattices in the auxiliary-input setting. *International Journal of Foundations of Computer Science (IJFCS)*, 31(05):551–567, August 2020. ISSN 0129-0541. URL `https://www.worldscientific.com/doi/10.1142/S0129054120500252`.

Ling:2021:EGI

[LMH+21] Yunhao Ling, Sha Ma, Qiong Huang, Ximing Li, Yijian Zhong, and Yunzhi Ling. Efficient group ID-based encryption with equality test against insider attack. *The Computer Journal*, 64(4):661–674, April 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/64/4/661/5910102`.

Li:2022:DDV

[LMM+22] Yingying Li, Jianfeng Ma, Yinbin Miao, Huizhong Li, Qiang Yan, Yue Wang, Ximeng Liu, and Kim-Kwang Raymond Choo. DVREI: Dynamic verifiable retrieval over encrypted images. *IEEE Transactions* on *Computers*, 71(8):1755–1769, August 2022. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Li:2020:DIS

[LNE+20] Kai Li, Wei Ni, Yousef Emami, Yiran Shen, Ricardo Severino, David Pereira, and Eduardo Tovar. Design and implementation of secret key agreement for platoon-based vehicular cyber-physical systems. *ACM Transactions on Cyber-Physical Systems (TCPS)*, 4(2):22:1–22:20, February 2020. CODEN ???? ISSN 2378-962X (print), 2378-9638 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3365996.

Leurent:2020:SSF

[LP20a] Gaëtan Leurent and Thomas Peyrin. SHA-1 is a shambles — first chosen-prefix collision on SHA-1and application to the PGP Web of Trust. Report, Inria and Nanyang Technological University and Temasek Laboratories, France and Singapore, July 26, 2020. URL https://eprint.iacr.org/2020/014.pdf.

Peyrin:2020:SSF

[LP20b] Gaëtan Leurent and Thomas Peyrin. SHA-1 is a shambles: First chosen-prefix collision on SHA-1 and application to the PGP Web of Trust. Report, Inria and Nanyang Technological University and Temasek Laboratories, France and Singapore, January 7, 2020.

Lee:2020:TSG

[LPLL20] Youngkyung Lee, Jong Hwan Park, Kwangsu Lee, and Dong Hoon Lee. Tight security for the generic construction of identity-based signature (in the multi-instance setting). *Theoretical Computer Science*, 847(??):122–133, December 22, 2020. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397520305557.

Liu:2022:LOH

[LQD22] Yanjiang Liu, Tongzhou Qu, and Zibin Dai. A low-overhead and high-security cryptographic circuit design utilizing the TIGFET-based three-phase single-rail pulse register against side-channel attacks. *ACM Transactions on Design Automation of Electronic Systems*, 27(4):36:1–36:13, July 2022. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic). URL https://dl.acm.org/doi/10.1145/3498339.

Lin:2020:LFI

[LSQ20] Xi-Jun Lin, Lin Sun, and Haipeng Qu. Leakage-free

ID-based signature, revisited. *The Computer Journal*, 63 (8):1263–1270, August 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/63/8/1263/5716157.

Li:2021:LUC

[LSX+21] Cong Li, Qingni Shen, Zhikang Xie, Xinyu Feng, Yuejian Fang, and Zhonghai Wu. Large universe CCA2 CP-ABE with equality and validity test in the standard model. *The Computer Journal*, 64(4):509–533, April 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/64/4/509/5872129.

Lin:2020:SCS

[LSY+20] Xi-Jun Lin, Lin Sun, Zhen Yan, Xiaoshuai Zhang, and Haipeng Qu. On the security of a certificateless signcryption with known session-specific temporary information security in the standard model. *The Computer Journal*, 63(8):1259–1262, August 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/63/8/1259/5699818.

Scala:2022:SBC

[LT22] Roberto La Scala and Sharwan K. Tiwari. Stream/block ciphers, difference equations and algebraic attacks. *Journal of Symbolic Computation*, 109(??):177–198, March/April 2022. CODEN JSYCEH. ISSN 0747-7171 (print), 1095-855X (electronic). URL http://www.sciencedirect.com/science/article/pii/S0747717121000584.

Li:2022:DCB

[LTDZ22] Yantao Li, Peng Tao, Shaojiang Deng, and Gang Zhou. DeFFusion: CNN-based continuous authentication using deep feature fusion. *ACM Transactions on Sensor Networks*, 18(2):18:1–18:20, May 2022. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic). URL https://dl.acm.org/doi/10.1145/3485060.

Lloret-Talavera:2022:EHE

[LTJS+22] Guillermo Lloret-Talavera, Marc Jorda, Harald Servat, Fabian Boemer, Chetan Chauhan, Shigeki Tomishima, Nilesh N. Shah, and Antonio J. Peña. Enabling homomorphically encrypted inference for large DNN models. *IEEE Transactions on Computers*, 71(5):1145–1155, May 2022. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Le:2020:CCM

[LTTT20] Minh Ha Le, Vinh Duc Tran, Van Anh Trinh, and

Viet Cuong Trinh. Compacting ciphertext in multi-channel broadcast encryption and attribute-based encryption. *Theoretical Computer Science*, 804(??):219–235, January 12, 2020. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397519307601.

Luengo:2021:RSR

[LV21] Elena Almaraz Luengo and Luis Javier García Villalba. Recommendations on statistical randomness test batteries for cryptographic purposes. *ACM Computing Surveys*, 54(4):80:1–80:34, July 2021. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/doi/10.1145/3447773.

Loffi:2021:MAM

[LWGW21] Leandro Loffi, Carla Merkle Westphall, Lukas Derner Grüdtner, and Carlos Becker Westphall. Mutual authentication with multi-factor in IoT–Fog–Cloud environment. *Journal of Network and Computer Applications*, 176(??):??, February 15, 2021. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S108480452030391X.

Lu:2022:SSK

[LWH+22] Youjing Lu, Fan Wu, Qianyi Huang, Shaojie Tang, Linghe Kong, and Guihai Chen. Shared secret key generation by exploiting inaudible acoustic channels. *ACM Transactions on Sensor Networks*, 18(1):13:1–13:26, February 2022. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic). URL https://dl.acm.org/doi/10.1145/3480461.

Li:2021:DMS

[LWL+21] Songbin Li, Jingang Wang, Peng Liu, Miao Wei, and Qiandong Yan. Detection of multiple steganography methods in compressed speech based on code element embedding, Bi-LSTM and CNN with attention mechanisms. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 29(??):1556–1569, 2021. CODEN ???? ISSN 2329-9290.

Lv:2020:SAP

[LWS+20] Jiaxian Lv, Yi Wang, Jinshu Su, Rongmao Chen, and Wenjun Wu. Security of auditing protocols against subversion attacks. *International Journal of Foundations of Computer Science (IJFCS)*, 31(2):193–206, February 2020. ISSN 0129-0541. URL https://www.worldscientific.com/doi/10.1142/S0129054120500033.

Lin:2021:SAF

[LWS+21] Xi-Jun Lin, Qihui Wang, Lin Sun, Zhen Yan, and Peishun Liu. Security analysis of the first certificateless proxy signature scheme against malicious-but-passive KGC attacks. *The Computer Journal*, 64(4):653–660, April 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/64/4/653/5880730.

Lin:2021:IBE

[LWSQ21] Xi-Jun Lin, Qihui Wang, Lin Sun, and Haipeng Qu. Identity-based encryption with equality test and datestamp-based authorization mechanism. *Theoretical Computer Science*, 861(??): 117–132, March 12, 2021. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397521000815.

Liu:2021:FSC

[LWZ+21] Kunlin Liu, Ping Wang, Wenbo Zhou, Zhenyu Zhang, Yanhao Ge, Honggu Liu, Weiming Zhang, and Nenghai Yu. Face swapping consistency transfer with neural identity carrier. *Future Internet*, 13(11):298, November 22, 2021. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/13/11/298.

Lin:2021:TNC

[LXG21] Kunda Lin, Xiaolong Xu, and Honghao Gao. TSCRNN: a novel classification scheme of encrypted traffic based on flow spatiotemporal features for efficient management of IIoT. *Computer Networks (Amsterdam, Netherlands: 1999)*, 190(??):??, May 8, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128621001067.

Liang:2022:MSA

[LXZ+22] Wei Liang, Songyou Xie, Dafang Zhang, Xiong Li, and Kuan ching Li. A mutual security authentication method for RFID-PUF circuit based on deep learning. *ACM Transactions on Internet Technology (TOIT)*, 22(2):34:1–34:20, May 2022. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic). URL https://dl.acm.org/doi/10.1145/3426968.

Lu:2020:VSV

[LYCW20] Li Lu, Jiadi Yu, Yingying Chen, and Yan Wang. VocalLock: Sensing vocal tract for passphrase-independent user authentication leveraging acoustic signals on smartphones. *Proceedings of the*

ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT), 4(2):51:1–51:24, June 2020. CODEN ???? ISSN 2474-9567 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3397320.

Liang:2021:IAH

[LYDZ21] X. Liang, Z. Yan, R. H. Deng, and Q. Zheng. Investigating the adoption of hybrid encrypted cloud data deduplication with game theory. *IEEE Transactions on Parallel and Distributed Systems*, 32(3): 587–600, March 2021. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Lalouani:2022:CMA

[LYEK22] Wassila Lalouani, Mohamed Younis, Mohammad Ebrahimabadi, and Naghmeh Karimi. Countering modeling attacks in PUF-based IoT security solutions. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 18(3):46:1–46:28, July 2022. CODEN ???? ISSN 1550-4832. URL https://dl.acm.org/doi/10.1145/3491221.

Li:2021:IEB

[LYSC21] Yinghua Li, He Yu, Bin Song, and Jinjun Chen. Image encryption based on a single-round dictionary and chaotic sequences in cloud computing. *Concurrency and Computation: Practice and Experience*, 33(7):1, April 10, 2021. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Luo:2022:MEO

[LYX+22] Meng Luo, Yepeng Yao, Liling Xin, Zhengwei Jiang, Qiuyun Wang, and Wenchang Shi. Measurement for encrypted open resolvers: Applications and security. *Computer Networks (Amsterdam, Netherlands: 1999)*, 213(??):??, August 4, 2022. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128622002183.

Liu:2021:CCS

[LYY+21] Jinhui Liu, Yong Yu, Bo Yang, Jianwei Jia, and Qiqi Lai. Cryptanalysis of Cramer–Shoup like cryptosystems based on index exchangeable family. *International Journal of Foundations of Computer Science (IJFCS)*, 32(01):73–91, January 2021. ISSN 0129-0541. URL https://www.worldscientific.com/doi/10.1142/S0129054121500040.

Lu:2022:PDD

[LYZ+22] Hai Lu, Ruyun Yu, Yan Zhu, Xiao He, Kaitai Liang, and William Cheng-Chung Chu. Policy-driven data sharing over attribute-based encryption supporting dual membership. *The Journal of Systems and Software*, 188(??):??, June 2022. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0164121222000346`.

Liu:2020:ASF

[LZ20] Muhua Liu and Ping Zhang. An adaptively secure functional encryption for randomized functions. *The Computer Journal*, 63(8):1247–1258, August 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/63/8/1247/5699816`.

Li:2022:ESA

[LZ22] Sujuan Li and Futai Zhang. eCK-secure authenticated key exchange against auxiliary input leakage. *The Computer Journal*, 65(8): 2063–2072, August 2022. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/65/8/2063/6269133`.

Lin:2021:LPK

[LZG+21] Hao Lin, Zhen Zhao, Fei Gao, Willy Susilo, Qiaoyan Wen, Fuchun Guo, and Yijie Shi. Lightweight public key encryption with equality test supporting partial authorization in cloud storage. *The Computer Journal*, 64 (8):1226–1238, August 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/64/8/1226/6025507`.

Lou:2021:SMS

[LZJZ21] Xiaoxuan Lou, Tianwei Zhang, Jun Jiang, and Yinqian Zhang. A survey of microarchitectural side-channel vulnerabilities, attacks, and defenses in cryptography. *ACM Computing Surveys*, 54 (6):122:1–122:37, July 2021. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL `https://dl.acm.org/doi/10.1145/3456629`.

Liu:2021:NKT

[LZW+21] Zuquan Liu, Guopu Zhu, Yuan-Gen Wang, Jianquan Yang, and Sam Kwong. A novel (t, s, k, n)-threshold visual secret sharing scheme based on access structure partition. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 16(4):118:1–118:21, January 2021. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL `https://dl.acm.org/doi/10.1145/3418212`.

Liu:2022:NLN

[LZX+22] Zeyi Liu, Weijuan Zhang, Ji Xiang, Daren Zha, and

Lei Wang. NP-LFA: Non-profiled leakage fingerprint attacks against improved rotating S-box masking scheme. *The Computer Journal*, 65 (6):1598–1610, June 2022. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/65/6/1598/6178973.

Li:2021:TAN

[LZYZ21] Yamin Li, Jun Zhang, Zhongliang Yang, and Ru Zhang. Topic-aware neural linguistic steganography based on knowledge graphs. *ACM Transactions on Data Science (TDS)*, 2(2):10:1–10:13, May 2021. CODEN ???? ISSN 2691-1922. URL https://dl.acm.org/doi/10.1145/3418598.

Mall:2021:CPB

[MAOH21] Priyanka Mall, Ruhul Amin, Mohammad S. Obaidat, and Kuei-Fang Hsiao. CoMSeC++: PUF-based secured light-weight mutual authentication protocol for drone-enabled WSN. *Computer Networks (Amsterdam, Netherlands: 1999)*, 199 (??):??, November 9, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128621004230.

Marsh:2020:HFB

[Mar20a] Allison Marsh. The hidden figures behind Bletchley Park's code-breaking Colossus. *IEEE Spectrum*, 57 (1):??, January 2020. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic). URL https://spectrum.ieee.org/tech-history/dawn-of-electronics/the-hidden-figures-behind-bletchley-parks-codebreaking-colossus. Online supplement to 1-page story.

Marsh:2020:HFC

[Mar20b] Allison Marsh. The hidden figures of Colossus. *IEEE Spectrum*, 57(1):64, January 2020. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic). URL https://spectrum.ieee.org/tech-history/dawn-of-electronics/the-hidden-figures-behind-bletchley-parks-codebreaking-colossus.

Martin:2024:GCA

[Mar24] Alexander Martin. GCHQ celebrates 80th anniversary of world's first digital computer, used to crack Nazi ciphers. Web site, January 18, 2024. URL https://therecord.media/80th-anniversary-colossus-digital-computer-uk-wwii-nazi-codebreaking.

Mirsaraei:2022:STF

[MGB22] AmirHossein Ghafouri Mirsaraei, Ali Barati, and Hamid Barati. A secure three-factor authentication scheme for IoT environments. *Journal of Parallel and Distributed Computing*, 169(??): 87–105, November 2022. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731522001460.

Manzoor:2021:PRE

[MBK+21] Ahsan Manzoor, An Braeken, Salil S. Kanhere, Mika Ylianttila, and Madhsanka Liyanage. Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain. *Journal of Network and Computer Applications*, 176 (??):??, February 15, 2021. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804520303763.

McCallum:2024:UIC

[McC24] Shiona McCallum. Unseen images of code breaking computer that helped win WW2. Web site, January 18, 2024. URL https://www.bbc.com/news/technology-67997406.

Ma:2022:RAS

[MCF+22] Ruhui Ma, Jin Cao, Dengguo Feng, Hui Li, Xiaowei Li, and Yang Xu. A robust authentication scheme for remote diagnosis and maintenance in 5G V2N. *Journal of Network and Computer Applications*, 198(??):??, February 2022. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804521002770.

McIntire:2021:SCS

[McI21] Brenda McIntire. The secret career of Solomon Kullback. *Chance*, 34(2):18–23, 2021. CODEN CNDCE4. ISSN 0933-2480 (print), 1867-2280 (electronic).

Mclaughlin:2020:BPC

[Mcl20] Martyn Mclaughlin. Bletchley Park codebreaker who helped change course of World War II dies aged 97. Web site, May 17, 2020. URL https://www.scotsman.com/news/people/bletchley-park-codebreaker-who-helped-change-course-world-war-ii-dies-aged-97-2855511.

Moussaileb:2021:SWB

[MCLL21] Routa Moussaileb, Nora Cuppens, Jean-Louis Lanet, and Hélène Le Bouder. A survey on Windows-based ransomware taxonomy and detection mechanisms. *ACM Computing Surveys*, 54(6): 117:1–117:36, July 2021. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/doi/10.1145/3453153.

Mitra:2021:CIA

[MDD+21] Shyamali Mitra, Nibaran Das, Soumyajyoti Dey, Sukanta Chakraborty, Mita Nasipuri, and Mrinal Kanti Naskar. Cytology image analysis techniques toward automation: Systematically revisited. *ACM Computing Surveys*, 54(3):52:1–52:41, June 2021. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/doi/10.1145/3447238.

Mehrabi:2020:ECC

[MDJ20] M. A. Mehrabi, C. Doche, and A. Jolfaei. Elliptic curve cryptography point multiplication core for hardware security module. *IEEE Transactions on Computers*, 69(11): 1707–1718, November 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Ma:2021:IKR

[MG21] Sudong Ma and Jie Guan. Improved key recovery attacks on simplified version of K2 stream cipher. *The Computer Journal*, 64(8): 1253–1263, August 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/64/8/1253/6042244.

Ma:2021:CAF

[MH21a] Sha Ma and Qiong Huang. CCA-almost-full anonymous group signature with verifier local revocation in the standard model. *The Computer Journal*, 64(8):1239–1252, August 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/64/8/1239/6029314.

Mouha:2021:AFM

[MH21b] N. Mouha and A. Hailane. The application of formal methods to real-world cryptographic algorithms, protocols, and systems. *Computer*, 54(1):29–38, 2021. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Meng:2020:BSC

[MHS+20] D. Meng, R. Hou, G. Shi, B. Tu, A. Yu, Z. Zhu, X. Jia, Y. Wen, and Y. Yang. Built-in security computer: Deploying security-first architecture using active security processor. *IEEE Transactions on Computers*, 69(11): 1571–1583, November 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Meshram:2022:ERU

[MIB22] Chandrashekhar Meshram, Rabha W. Ibrahim, and

Sharad Kumar Barve. An efficient remote user authentication with key agreement procedure based on convolution-Chebyshev chaotic maps using biometric. *The Journal of Supercomputing*, 78(10): 12792–12814, July 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-021-04280-8.

Meshram:2022:EAK

[MII22] Chandrashekhar Meshram, Rabha W. Ibrahim, and Agbotiname Lucky Imoize. An efficient authentication with key agreement procedure using Mittag-Leffler–Chebyshev summation chaotic map under the multi-server architecture. *The Journal of Supercomputing*, 78(4):4938–4959, March 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-021-04039-1.

Ma:2020:SAR

[ML20] Xuecheng Ma and Dongdai Lin. Server-aided revocable IBE with identity reuse. *The Computer Journal*, 63(4):620–632, April 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/63/4/620/5625927.

Meng:2020:TCS

[MMHX20] Keju Meng, Fuyou Miao, Wenchao Huang, and Yan Xiong. Threshold changeable secret sharing with secure secret reconstruction. *Information Processing Letters*, 157(??):Article 105928, May 2020. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019020300156.

Mahalat:2022:ICA

[MMM+22] Mahabub Hasan Mahalat, Suraj Mandal, Anindan Mondal, Bibhash Sen, and Rajat Subhra Chakraborty. Implementation, characterization and application of path changing switch based arbiter PUF on FPGA as a lightweight security primitive for IoT. *ACM Transactions on Design Automation of Electronic Systems*, 27(3):26:1–26:26, May 2022. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic). URL https://dl.acm.org/doi/10.1145/3491212.

Mehic:2020:QKD

[MNR+20] Miralem Mehic, Marcin Niemiec, Stefan Rass, Jiajun Ma, Momtchil Peev, Alejandro Aguado, Vicente Martin, Stefan Schauer, Andreas Poppe, Christoph Pacher, and Miroslav Voznak. Quantum key distribution: a networking perspective. *ACM Computing Surveys*, 53(5): 96:1–96:41, October 2020. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/doi/10.1145/3402192.

Mogensen:2022:HRL

[Mog22] Torben Ægidius Mogensen. `Hermes`: a reversible language for lightweight encryption. *Science of Computer Programming*, 215(??):??, March 1, 2022. CODEN SCPGD4. ISSN 0167-6423 (print), 1872-7964 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167642321001398.

Mone:2020:NQT

[Mon20] Gregory Mone. News: The quantum threat. *Communications of the Association for Computing Machinery*, 63 (7):12–14, July 2020. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3398388.

Misra:2021:SSR

[MOP21] Sudip Misra, Tamoghna Ojha, and Madhusoodhanan P. SecRET: Secure range-based localization with evidence theory for underwater sensor networks. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, 15 (1):2:1–2:26, February 2021. CODEN ???? ISSN 1556-4665 (print), 1556-4703 (electronic). URL https://dl.acm.org/doi/10.1145/3431390.

Mazza:2021:HEV

[MPV21] S. Mazza, D. Patel, and I. Viola. Homomorphic-encrypted volume rendering. *IEEE Transactions on Visualization and Computer Graphics*, 27(2):635–644, 2021. CODEN ITVGEA. ISSN 1077-2626.

Maniam:2021:AEH

[MS21a] Senthil Murugan Maniam and T. Sasilatha. Area-efficient and high-speed hardware structure of hybrid cryptosystem (AES-RC4) for maximizing key lifetime using parallel subpipeline architecture. *Concurrency and Computation: Practice and Experience*, 33(3):e5287:1–e5287:??, February 10, 2021. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Menezes:2021:AES

[MS21b] Alfred Menezes and Douglas Stebila. The Advanced Encryption Standard: 20 years later. *IEEE Security & Privacy*, 19(6):98–102, November/December 2021. ISSN 1540-7993 (print), 1558-4046 (electronic).

Menezes:2021:CC

[MS21c] Alfred Menezes and Douglas Stebila. Challenges in cryptography. *IEEE Security & Privacy*, 19(2):70–73, 2021. ISSN 1540-7993 (print), 1558-4046 (electronic).

Mayrhofer:2022:AMM

[MS22a] René Mayrhofer and Stephan Sigg. Adversary models for mobile device authentication. *ACM Computing Surveys*, 54 (9):198:1–198:35, December 2022. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/doi/10.1145/3477601.

Mobarhan:2022:RAS

[MS22b] Mostafa Ayoubi Mobarhan and Mohammed Salamah. REPS-AKA3: a secure authentication and re- authentication protocol for LTE networks. *Journal of Network and Computer Applications*, 201(??):??, May 2022. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804522000145.

Mehrotra:2020:PPD

[MSU+20] Sharad Mehrotra, Shantanu Sharma, Jeffrey D. Ullman, Dhrubajyoti Ghosh, Peeyush Gupta, and Anurag Mishra. PANDA: Partitioned data security on outsourced sensitive and non-sensitive data. *ACM Transactions on Management Information Systems (TMIS)*, 11(4):23:1–23:41, December 2020. CODEN ???? ISSN 2158-656X (print), 2158-6578 (electronic). URL https://dl.acm.org/doi/10.1145/3397521.

Meftah:2022:THP

[MTA+22] Souhail Meftah, Benjamin Hong Meng Tan, Khin Mi Mi Aung, Lu Yuxiao, Lin Jie, and Bharadwaj Veeravalli. Towards high performance homomorphic encryption for inference tasks on CPU: an MPI approach. *Future Generation Computer Systems*, 134 (??):13–21, September 2022. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X22001145.

Mary:2022:VTS

[MUK22] Narla John Metilda Sagaya Mary, Srinivasan Umesh, and Sandesh Varadaraju Katta. S-vectors and TESA: Speaker embeddings and a speaker authenticator based on transformer encoder. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 30(??):404–413, 2022. CODEN ???? ISSN 2329-9290.

Mayrhofer:2021:APS

[MVBK21] René Mayrhofer, Jeffrey Vander Stoep, Chad Brubaker, and Nick Kralevich. The Android platform security model. *ACM Transactions on Privacy and Security (TOPS)*, 24(3):19:1–19:35, April 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3448609.

Mathis:2021:FSA

[MWVK21] Florian Mathis, John H. Williamson, Kami Vaniea, and Mohamed Khamis. Fast and secure authentication in virtual reality using coordinated 3D manipulation and pointing. *ACM Transactions on Computer-Human Interaction*, 28(1):6:1–6:44, February 2021. CODEN ATCIF4. ISSN 1073-0516 (print), 1557-7325 (electronic). URL https://dl.acm.org/doi/10.1145/3428121.

Mabodi:2020:MLT

[MYF20] Kobra Mabodi, Mehdi Yusefi, and Reza Fotohi. Multi-level trust-based intelligence schema for securing of Internet of Things (IoT) against security threats using cryptographic authentication. *The Journal of Supercomputing*, 76(9):7081–7106, September 2020. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-019-03137-5.

Narasimhan:2020:BPM

[NA20a] Sivasankari Narasimhan and Muthukumar Arunachalam. Bio-Puf-Mac authenticated encryption for iris biometrics. *Computational Intelligence*, 36(3):1221–1241, August 2020. CODEN COMIE6. ISSN 0824-7935 (print), 1467-8640 (electronic).

Nikooghadam:2020:PFS

[NA20b] Mahdi Nikooghadam and Haleh Amintoosi. Perfect forward secrecy via an ECC-based authentication scheme for SIP in VoIP. *The Journal of Supercomputing*, 76(4):3086–3104, April 2020. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Nassr:2022:ISP

[NAB22] Dieaa I. Nassr, M. Anwar, and Hatem M. Bahig. Improving small private exponent attack on the Murru–Saettone cryptosystem. *Theoretical Computer Science*, 923(??):222–234, June 26, 2022. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397522003085.

Nabeel:2020:RTS

[NAP+20] M. Nabeel, M. Ashraf, S. Patnaik, V. Soteriou, O. Sinanoğlu, and J. Knechtel. 2.5D root of trust: Secure system-level integration of untrusted chiplets. *IEEE Transactions on Computers*, 69(11):1611–1625, November 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Narasimhulu:2022:NBW

[Nar22] C. Venkata Narasimhulu. A new blind watermark embedding model: Spiral updated rider optimization algorithm. *The Computer Journal*, 65 (6):1365–1385, June 2022. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/65/6/1365/6124657.

Najafi:2021:FMO

[NBJ21] Aniseh Najafi, Majid Bayat, and Hamid Haj Seyyed Javadi. Fair multi-owner search over encrypted data with forward and backward privacy in cloud-assisted Internet of Things. *Future Generation Computer Systems*, 124(??):285–294, November 2021. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X21002053.

Noura:2022:DGB

[NCM22] Hassan N. Noura, Raphaël Couturier, and Kamel Mazouzi. DKEMA: GPU-based and dynamic key-dependent efficient message authentication algorithm. *The Journal of Supercomputing*, 78(12):14034–14071, August 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-022-04433-3.

Nanda:2020:HET

[NNH+20] Ashish Nanda, Priyadarsi Nanda, Xiangjian He, Aruna Jamdagni, and Deepak Puthal. A hybrid encryption technique for Secure-GLOR: the adaptive secure routing protocol for dynamic wireless mesh networks. *Future Generation Computer Systems*, 109(??):521–530, August 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X17322409.

Natgunanathan:2022:BBA

[NPG+22] Iynkaran Natgunanathan, Purathani Praitheeshan, Longxiang Gao, Yong Xiang, and Lei Pan. Blockchain-based audio watermarking technique for multimedia copyright protection in distribution networks. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 18 (3):86:1–86:23, August 2022. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL https://dl.acm.org/doi/10.1145/3492803.

Nahiyan:2020:SCF

[NPH+20] Adib Nahiyan, Jungmin Park, Miao He, Yousef Iskander, Farimah Farahmandi, Domenic Forte, and Mark Tehranipoor. SCRIPT: a CAD framework for power side-channel vulnerability assessment using information flow tracking and pattern generation. *ACM Transactions on Design Automation of Electronic Systems*, 25(3):26:1–26:27, May 2020. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3383445.

Naor:2020:SLU

[NRS20] Moni Naor, Lior Rotem, and Gil Segev. The security of lazy users in out-of-band authentication. *ACM Transactions on Privacy and Security (TOPS)*, 23(2):9:1–9:32, May 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3377849.

Nath:2022:EWV

[NS22] Kaushik Nath and Palash Sarkar. Efficient 4-way vectorizations of the Montgomery ladder. *IEEE Transactions on Computers*, 71(3):712–723, March 2022. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Nejatollahi:2020:SFA

[NVB+20] Hamid Nejatollahi, Felipe Valencia, Subhadeep Banik, Francesco Regazzoni, Rosario Cammarota, and Nikil Dutt. Synthesis of flexible accelerators for early adoption of ring-LWE post-quantum cryptography. *ACM Transactions on Embedded Computing Systems*, 19(2):11:1–11:17, March 2020. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3378164.

Omar:2020:OSC

[ODK20] H. Omar, B. D'Agostino, and O. Khan. OPTIMUS: A security-centric dynamic hardware partitioning scheme for processors that prevent microarchitecture state attacks. *IEEE Transactions on Computers*, 69(11):1558–1570, November 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Ogundoyin:2021:PPP

[OK21] Sunday Oyinlola Ogundoyin and Ismaila Adeniyi Kamil. PAASH: a privacy-preserving authentication and fine-grained access control of outsourced data for secure smart health in smart cities. *Journal of Parallel and Distributed Computing*, 155(??): 101–119, September 2021. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S074373152100099X`.

Oden:2022:ICA

[OK22] Lena Oden and Jörg Keller. Improving cryptanalytic applications with stochastic runtimes on GPUs and multicores. *Parallel Computing*, 112(??):??, September 2022. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167819122000412`.

Oviatt:2021:KWY

[OLS21] Sharon Oviatt, Jionghao Lin, and Abishek Sriramulu. I know what you know: What hand movements reveal about domain expertise. *ACM Transactions on Interactive Intelligent Systems (TIIS)*, 11(1):4:1–4:26, April 2021. CODEN ???? ISSN 2160-6455 (print), 2160-6463 (electronic). URL `https://dl.acm.org/doi/10.1145/3423049`.

Ou:2020:LDA

[OLZ+20] C. Ou, S. K. Lam, C. Zhou, G. Jiang, and F. Zhang. A lightweight detection algorithm for collision-optimized divide-and-conquer attacks. *IEEE Transactions on Computers*, 69(11):1694–1706, November 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Ono:2022:PPF

[OTK+22] Shinji Ono, Jun Takata, Masaharu Kataoka, Tomohiro I, Kilho Shin, and Hiroshi Sakamoto. Privacy-preserving feature selection with fully homomorphic encryption. *Algorithms (Basel)*, 15(7), July 2022. CODEN ALGOCH. ISSN 1999-4893 (electronic). URL `https://www.mdpi.com/1999-4893/15/7/229`.

Pulagara:2021:IRC

[PA21] Seshu Babu Pulagara and P. J. A. Alphonse. An intelligent and robust conditional privacy preserving authentication and group-key management scheme for vehicular ad hoc networks using elliptic curve cryptosystem. *Concurrency and Computation: Practice and Experience*, 33(3):e5153:1–e5153:??, February 10, 2021. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Pandey:2020:SMD

[Pan20] Hari Mohan Pandey. Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography. *Future Generation Computer Systems*, 111 (??):213–225, October 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X20303848.

Paul:2021:TEE

[Pau21a] Jon D. Paul. In the twilight of electromechanical encryption, an exceptional machine figured in a major spy scandal. *IEEE Spectrum*, 58(9):32–52, 2021. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Paul:2021:SHL

[Pau21b] Jon D. Paul. The scandalous history of the last rotor cipher machine: How this gadget figured in the shady Rubicon spy case. *IEEE Spectrum*, 58(??):??, August 31, 2021. URL https://spectrum.ieee.org/the-scandalous-history-of-the-last-rotor-cipher-machine.

Palit:2022:ABB

[PCC22] Sudip Kumar Palit, Mohuya Chakraborty, and Subhalaxmi Chakraborty. AUGChain: blockchain-based mobile user authentication scheme in global mobility network. *The Journal of Supercomputing*, 78(5):6788–6816, April 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-021-04139-y.

Patsakis:2020:ECD

[PCK20] Constantinos Patsakis, Fran Casino, and Vasilios Katos. Encrypted and covert DNS queries for botnets: Challenges and countermeasures. *Computers & Security*, 88 (??):Article 101614, January 2020. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S016740481831321X.

Payeras-Capella:2020:IEM

[PCMPCA+20] M Magdalena Payeras-Capella, Macia Mut-Puigserver, Pau Conejero-Alberola, Jordi Castella-Roca, and Llorenç Huguet-Rotger. Implementation and evaluation of the mCity-PASS protocol for secure and private access to associated touristic services. *The Computer Journal*, 63 (8):1168–1193, August 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/63/8/1168/5670506.

Paskin-Cherniavsky:2020:CAU

[PCO20] Anat Paskin-Cherniavsky and Ruxandra F. Olimid. On cryptographic anonymity and unpredictability in secret sharing. *Information Processing Letters*, 161(??): Article 105965, September 2020. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019020300521.

Peng:2021:EDD

[PCV+21] Cong Peng, Jianhua Chen, Pandi Vijayakumar, Neeraj Kumar, and Debiao He. Efficient distributed decryption scheme for IoT gateway-based applications. *ACM Transactions on Internet Technology (TOIT)*, 21(1): 19:1–19:23, February 2021. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic). URL https://dl.acm.org/doi/10.1145/3414475.

Patel:2021:SLK

[PD21] Chintan Patel and Nishant Doshi. Secure lightweight key exchange using ECC for user-gateway paradigm. *IEEE Transactions on Computers*, 70(11):1789–1803, November 2021. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Pirayesh:2022:PHB

[PGCK22] Jamshid Pirayesh, Alberto Giaretta, Mauro Conti, and Parviz Keshavarzi. A PLS-HECC-based device authentication and key agreement scheme for smart home networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 216(??):??, October 24, 2022. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S138912862200216X.

Papadogiannaki:2021:SEN

[PI21] Eva Papadogiannaki and Sotiris Ioannidis. A survey on encrypted network traffic analysis applications, techniques, and countermeasures. *ACM Computing Surveys*, 54 (6):123:1–123:35, July 2021. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/doi/10.1145/3457904.

Prabhakaran:2021:IRC

[PK21] Varun Prabhakaran and Ashokkumar Kulandasamy. Integration of recurrent convolutional neural network and optimal encryption scheme for intrusion detection with secure data storage in the cloud. *Computational Intelligence*, 37(1):344–370, February 2021. CODEN COMIE6. ISSN 0824-7935 (print), 1467-8640 (electronic).

Pedone:2022:QKD

[PL22] Ignazio Pedone and Antonio Lioy. Quantum key distribution in Kubernetes clusters. *Future Internet*, 14(6):

160, May 25, 2022. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/14/6/160.

Platt:2021:SAI

[PM21] Moritz Platt and Peter McBurney. Sybil attacks on identity-augmented proof-of-stake. *Computer Networks (Amsterdam, Netherlands: 1999)*, 199(??):??, November 9, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128621003893.

Pham:2022:WIB

[PNJ+22] Minh Thuy Truc Pham, Ngoc Ai Van Nguyen, Mei Jiang, Dung Hoang Duong, and Willy Susilo. Wildcarded identity-based encryption from lattices. *Theoretical Computer Science*, 902 (??):41–53, January 18, 2022. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397521007167.

Poulter:2020:ESU

[POC20] Andrew John Poulter, Steven J. Ossont, and Simon J. Cox. Enabling the secure use of dynamic identity for the Internet of Things — using the Secure Remote Update Protocol (SRUP). *Future Internet*, 12(8):138, August 18, 2020. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/12/8/138.

Paez:2020:ABE

[PPR+20] Rafael Páez, Manuel Pérez, Gustavo Ramírez, Juan Montes, and Lucas Bouvarel. An architecture for biometric electronic identification document system based on blockchain. *Future Internet*, 12(1):10, January 11, 2020. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/12/1/10.

Panwar:2021:FES

[PPS21] Kirtee Panwar, Ravindra Kumar Purwar, and Garima Srivastava. A fast encryption scheme suitable for video surveillance applications using SHA-256 hash function and 1D sine–sine chaotic map. *International Journal of Image and Graphics (IJIG)*, 21(02):??, April 2021. ISSN 0219-4678. URL https://www.worldscientific.com/doi/10.1142/S0219467821500224.

Perillo:2022:SSE

[PPT22] Angelo Massimo Perillo, Giuseppe Persiano, and Alberto Trombetta. Secure selections on encrypted multi-writer streams. *ACM Transactions on Privacy and Security (TOPS)*, 25(1):7:1–7:33, February 2022. CODEN

???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3485470.

Przytarski:2022:QPB

[PSGM22] Dennis Przytarski, Christoph Stach, Clémentine Gritti, and Bernhard Mitschang. Query processing in blockchain systems: Current state and future challenges. *Future Internet*, 14(1):1, December 21, 2022. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/14/1/1.

Pilania:2022:FVS

[PTZM22] Urmila Pilania, Rohit Tanwar, Mazdak Zamani, and Azizah Abdul Manaf. Framework for video steganography using integer wavelet transform and JPEG compression. *Future Internet*, 14(9):254, August 25, 2022. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/14/9/254.

Pang:2022:TPP

[PWL+22] Xiaoyi Pang, Zhibo Wang, Defang Liu, John C. S. Lui, Qian Wang, and Ju Ren. Towards personalized privacy-preserving truth discovery over crowdsourced data streams. *IEEE/ACM Transactions on Networking*, 30(1):327–340, February 2022. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic). URL https://dl.acm.org/doi/10.1109/TNET.2021.3110052.

Piao:2021:DSS

[PYC21] Yangheran Piao, Kai Ye, and Xiaohui Cui. A data sharing scheme for GDPR-compliance based on consortium blockchain. *Future Internet*, 13(8):217, August 21, 2021. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/13/8/217.

Panoff:2022:RCA

[PYSJ22] Max Panoff, Honggang Yu, Haoqi Shan, and Yier Jin. A review and comparison of AI-enhanced side channel analysis. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 18(3):62:1–62:20, July 2022. CODEN ???? ISSN 1550-4832. URL https://dl.acm.org/doi/10.1145/3517810.

Pang:2022:FUP

[PZJL22] Bo Pang, Deming Zhai, Junjun Jiang, and Xianming Liu. Fully unsupervised person re-identification via selective contrastive learning. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 18(2):64:1–64:15, May 2022. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL https://dl.acm.org/doi/10.1145/3485061.

Qasaimeh:2021:SDE

[QAQA21] Malik Qasaimeh, Raad S. Al-Qassas, and Mohammad Ababneh. Software design and experimental evaluation of a reduced AES for IoT applications. *Future Internet*, 13(11):273, October 27, 2021. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/13/11/273.

Qi:2022:AKE

[QC22a] Mingping Qi and Jianhua Chen. Authentication and key establishment protocol from supersingular isogeny for mobile environments. *The Journal of Supercomputing*, 78(5): 6371–6385, April 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-021-04121-8.

Qi:2022:PSP

[QC22b] Mingping Qi and Jianhua Chen. Provably secure post-quantum authenticated key exchange from supersingular isogenies. *The Journal of Supercomputing*, 78(10): 12815–12833, July 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-022-04378-7.

Qi:2022:RRV

[QGL+22] Wenfa Qi, Sirui Guo, Yuxin Liu, Xiang Wang, and Zongming Guo. Research on reversible visible watermarking algorithms based on vectorization compression method. *The Computer Journal*, 65 (5):1320–1337, May 2022. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/65/5/1320/6120302.

Qiao:2021:NPK

[QYZ+21] Zirui Qiao, Qiliang Yang, Yanwei Zhou, Zhe Xia, and Mingwu Zhang. Novel public-key encryption with continuous leakage amplification. *The Computer Journal*, 64 (8):1163–1177, August 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/64/8/1163/5921729.

Rajalakshmi:2022:EVP

[RA22] M. Rajalakshmi and K. Annapurani. Enhancement of vascular patterns in palm images using various image enhancement techniques for person identification. *International Journal of Image and Graphics (IJIG)*, 22(04): ??, July 2022. ISSN 0219-4678. URL https://www.worldscientific.com/doi/10.1142/S0219467822500322.

Ramezanpour:2020:SPS

[RAD20] K. Ramezanpour, P. Ampadu, and W. Diehl. SCAUL: Power side-channel analysis with unsupervised learning. *IEEE Transactions on Computers*, 69(11):1626–1638, November 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Ramkumar:2022:IBC

[RAN22] D. Ramkumar, C. Annadurai, and I. Nelson. Iris-based continuous authentication in mobile ad hoc network. *Concurrency and Computation: Practice and Experience*, 34 (8):e5542:1–e5542:??, April 10, 2022. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Rashid:2020:FED

[Ras20] F. Y. Rashid. The fight over encrypted DNS — [news]. *IEEE Spectrum*, 57(1):11–12, January 2020. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Rawal:2020:PRE

[Raw20] Bharat S. Rawal. Proxy re-encryption architect for storing and sharing of cloud contents. *International Journal of Parallel, Emergent and Distributed Systems: IJPEDS*, 35(3):219–235, 2020. CODEN ???? ISSN 1744-5760 (print), 1744-5779 (electronic).

Roy:2021:DFA

[RBM21] Dibyendu Roy, Bhagwan Bathe, and Subhamoy Maitra. Differential fault attack on Kreyvium & FLIP. *IEEE Transactions on Computers*, 70(12):2161–2167, December 2021. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Raheman:2022:WZV

[RBVV22] Fazal Raheman, Tejas Bhagat, Brecht Vermeulen, and Peter Van Daele. Will zero vulnerability computing (ZVC) ever be possible? Testing the hypothesis. *Future Internet*, 14(8):238, July 30, 2022. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/14/8/238`.

Russinovich:2021:TCC

[RCF+21] Mark Russinovich, Manuel Costa, Cédric Fournet, David Chisnall, Antoine Delignat-Lavaud, Sylvan Clebsch, Kapil Vaswani, and Vikas Bhatia. Toward confidential cloud computing. *Communications of the Association for Computing Machinery*, 64(6):54–61, June 2021. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `https://dl.acm.org/doi/10.1145/3453930`.

Rahman:2021:CGO

[RDM+21] M. Tanjidur Rahman, Nusrat Farzana Dipu, Dhwani Mehta, Shahin Tajik, Mark Tehranipoor, and Navid Asadizanjani. CONCEALING-Gate: Optical contactless probing resilient design. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 17(3):39:1–39:25, July 2021. CODEN ???? ISSN 1550-4832. URL https://dl.acm.org/doi/10.1145/3446998.

Roy:2022:LBP

[RDS+22] Partha Sarathi Roy, Dung Hoang Duong, Willy Susilo, Arnaud Sipasseuth, Kazuhide Fukushima, and Shinsaku Kiyomoto. Lattice-based public-key encryption with equality test supporting flexible authorization in standard model. *Theoretical Computer Science*, 929(??):124–139, September 11, 2022. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397522004091.

Rahmani:2022:NAS

[RFT22] Peyman Rahmani, Seyed Mostafa Fakhrahmad, and Mohammad Taheri. New attacks on secret sharing-based data outsourcing: toward a resistant scheme. *The Journal of Supercomputing*, 78 (14):15749–15785, September 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-022-04467-7.

Rjaibi:2020:ESD

[RH20] Walid Rjaibi and Mohammad Hammoudeh. Enhancing and simplifying data security and privacy for multitiered applications. *Journal of Parallel and Distributed Computing*, 139(??):53–64, May 2020. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S074373151930632X.

Ravi:2021:LBK

[RHCB21] Prasanna Ravi, James Howe, Anupam Chattopadhyay, and Shivam Bhasin. Lattice-based key-sharing schemes: a survey. *ACM Computing Surveys*, 54(1):9:1–9:39, April 2021. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/doi/10.1145/3422178.

Ryan:2023:PSK

[RHSH23] Keegan Ryan, Kaiwen He, George Arnold Sullivan, and Nadia Heninger. Passive SSH key compromise via lattices. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and*

Communications Security: [CCS '23, November 26–30, 2023, Copenhagen, Denmark]. ACM Press, New York, NY 10036, USA, 2023. URL `https://eprint.iacr.org/2023/1711.pdf`.

Rahman:2022:WSD

[RIW22] Md Rayhanur Rahman, Nasif Imtiaz, and Laurie Williams. Why secret detection tools are not enough: It's not just about false positives — an industrial case study. *Empirical Software Engineering*, 27(3):??, May 2022. CODEN ESENFW. ISSN 1382-3256 (print), 1573-7616 (electronic). URL `https://link.springer.com/article/10.1007/s10664-021-10109-y`.

Rafiee:2021:PSO

[RK21] Mojtaba Rafiee and Shahram Khazaei. Private set operations over encrypted cloud dataset and applications. *The Computer Journal*, 64 (8):1145–1162, August 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/64/8/1145/5921321`.

Rathore:2021:SHB

[RLZ+21] Aditya Singh Rathore, Zhengxiong Li, Weijin Zhu, Zhanpeng Jin, and Wenyao Xu. A survey on heart biometrics. *ACM Computing Surveys*, 53 (6):114:1–114:38, February 2021. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL `https://dl.acm.org/doi/10.1145/3410158`.

Raza:2020:ESI

[RMA+20] Abdur Rehman Raza, Khawir Mahmood, Muhammad Faisal Amjad, Haider Abbas, and Mehreen Afzal. On the efficiency of software implementations of lightweight block ciphers from the perspective of programming languages. *Future Generation Computer Systems*, 104(??):43–59, March 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X19310519`.

Rana:2022:LCI

[RMI22] Muhammad Rana, Quazi Mamun, and Rafiqul Islam. Lightweight cryptography in IoT networks: a survey. *Future Generation Computer Systems*, 129(??):77–89, April 2022. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X21004404`.

Rawal:2022:MTS

[RMMH22] Bharat S. Rawal, Poongodi M., Gunasekaran Manogaran, and Mounir Hamdi. Multi-tier stack of block chain with proxy re-encryption method scheme on the Internet of Things platform. *ACM Transactions on Internet Technology (TOIT)*, 22(2):41:1–41:20, May 2022. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic). URL https://dl.acm.org/doi/10.1145/3421508.

Raju:2022:SEM

[RN22] Konduru Upendra Raju and Amutha Prabha Nagarajan. A steganography embedding method based on CDF-DWT technique for reversible data hiding application using Elgamal algorithm. *International Journal of Foundations of Computer Science (IJFCS)*, 33(6–7):489–512, September–November 2022. ISSN 0129-0541. URL https://www.worldscientific.com/doi/10.1142/S0129054122420011.

Rahman:2021:SAD

[RNR+21] M. Sazadur Rahman, Adib Nahiyan, Fahim Rahman, Saverio Fazzari, Kenneth Plaks, Farimah Farahmandi, Domenic Forte, and Mark Tehranipoor. Security assessment of dynamically obfuscated scan chain against oracle-guided attacks. *ACM Transactions on Design Automation of Electronic Systems*, 26(4):29:1–29:27, April 2021. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic). URL https://dl.acm.org/doi/10.1145/3444960.

Rangwani:2022:FFM

[RO22] Diksha Rangwani and Hari Om. Four-factor mutual authentication scheme for health-care based on wireless body area network. *The Journal of Supercomputing*, 78(4):5744–5778, March 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-021-04099-3.

Raja:2020:CPB

[RR20] J. Raja and M. Ramakrishnan. Confidentiality-preserving based on attribute encryption using auditable access during encrypted records in cloud location. *The Journal of Supercomputing*, 76(8):6026–6039, August 2020. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Ravikumar:2021:PPB

[RR21] K. P. Ravikumar and H. S. Manjunatha Reddy. Pixel prediction-based image steganography using crow search algorithm-based deep belief network approach. *International Journal of Image and Graphics (IJIG)*, 21(01):??, January 2021. ISSN 0219-4678. URL https://www.worldscientific.com/doi/10.1142/S0219467821500029.

Ranathunga:2021:MRM

[RRN21] Dinesha Ranathunga, Matthew Roughan, and Hung Nguyen. Mathematical reconciliation of medical privacy policies. *ACM Transactions on Management Information Systems (TMIS)*, 12(1):5:1–5:18, March 2021. CODEN ???? ISSN 2158-656X (print), 2158-6578 (electronic). URL https://dl.acm.org/doi/10.1145/3397520.

Roy:2022:FFH

[RSB22] Prasanta Kumar Roy, Prashant Sahu, and Ansuman Bhattacharya. FastHand: a fast handover authentication protocol for densely deployed small-cell networks. *Journal of Network and Computer Applications*, 205(??):??, September 2022. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804522000893.

Ren:2021:AIB

[RYM21] Qiuning Ren, Chao Yang, and Jianfeng Ma. App identification based on encrypted multi-smartphone sources traffic fingerprints. *Computer Networks (Amsterdam, Netherlands: 1999)*, 201(??):??, December 24, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S138912862100493X.

Sadri:2021:ATF

[SA21] Mohammad Javad Sadri and Maryam Rajabzadeh Asaar. An anonymous two-factor authentication protocol for IoT-based applications. *Computer Networks (Amsterdam, Netherlands: 1999)*, 199(??):??, November 9, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128621004151.

Seo:2020:MMP

[SAKH20] Hwajeong Seo, Kyuhwang An, Hyeokdong Kwon, and Zhi Hu. Montgomery multiplication for public key cryptography on MSP430X. *ACM Transactions on Embedded Computing Systems*, 19(3):20:1–20:15, July 2020. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3387919.

Setty:2020:VSM

[SAL20] Srinath Setty, Sebastian Angel, and Jonathan Lee. Verifiable state machines: Proofs that untrusted services operate correctly. *Operating Systems Review*, 54(1):40–46, August 2020. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic). URL https://dl.acm.org/doi/10.1145/3421473.3421479.

Sarier:2021:CBB

[Sar21] Neyire Deniz Sarier. Comments on biometric-based non-transferable credentials and their application in blockchain-based identity management. *Computers & Security*, 105(??):Article 102243, June 2021. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167404821000675.

Sharma:2021:BSD

[SAS21] N. Sharma, A. Anand, and A. K. Singh. Bio-signal data sharing security through watermarking: a technical survey. *Computing*, 103(9):1883–1917, September 2021. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL https://link.springer.com/article/10.1007/s00607-020-00881-y.

Salem:2020:ELB

[SAY20] Fatima K. Abu Salem, Mira Al Arab, and Laurence T. Yang. Extending the limits for big data RSA cracking: Towards cache-oblivious TU decomposition. *Journal of Parallel and Distributed Computing*, 138(??):65–77, April 2020. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731519300425.

Schneier:2020:TVP

[Sch20] B. Schneier. Technologists vs. policy makers. *IEEE Security & Privacy*, 18(1):72–71, January 2020. ISSN 1540-7993 (print), 1558-4046 (electronic).

Schnorr:2021:FFI

[Sch21] Claus Peter Schnorr. Fast factoring integers by SVP algorithms. Report, Fachbereich Informatik und Mathematik, Goethe-Universität Frankfurt, PSF 111932, D-60054 Frankfurt am Main, Germany, March 11, 2021. URL https://eprint.iacr.org/2021/232.pdf.

Sciarretta:2020:FAM

[SCRV20] Giada Sciarretta, Roberto Carbone, Silvio Ranise, and Luca Viganò. Formal analysis of mobile multi-factor authentication with single sign-on login. *ACM Transactions on Privacy and Security (TOPS)*, 23(3):13:1–13:37, July 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3386685.

Shi:2021:TMO

[SCW+21] Xiaofeng Shi, Haofan Cai, Minmei Wang, Ge Wang, Baiwen Huang, Junjie Xie, and Chen Qian. TagAttention: Mobile object tracing with zero appearance knowledge by vision-RFID fusion. *IEEE/ACM Transactions on Networking*, 29(2): 890–903, April 2021. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic). URL https://dl.acm.org/doi/10.1109/TNET.2021.3052805.

Shen:2020:CBM

[SCZ+20] Meng Shen, Guohua Cheng, Liehuang Zhu, Xiaojiang Du, and Jiankun Hu. Content-based multi-source encrypted image retrieval in clouds with privacy preservation. *Future Generation Computer Systems*, 109(??):621–632, August 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X17321969.

Sakib:2020:RDB

[SGB20] Mohammad Nazmus Sakib, Shuvashis Das Gupta, and Satyendra N. Biswas. A robust DWT-based compressed domain video watermarking technique. *International Journal of Image and Graphics (IJIG)*, 20(01):??, January 2020. ISSN 0219-4678. URL https://www.worldscientific.com/doi/10.1142/S0219467820500047.

Sepulveda:2021:BCA

[SGZS21] Johanna Sepúlveda, Mathieu Gross, Andreas Zankl, and Georg Sigl. Beyond cache attacks: Exploiting the bus-based communication structure for powerful on-chip microarchitectural attacks. *ACM Transactions on Embedded Computing Systems*, 20(2):17:1–17:23, March 2021. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic). URL https://dl.acm.org/doi/10.1145/3433653.

Souvignet:2020:LLL

[SHB20] T. R. Souvignet, T. Heckmann, and T. Bolle. From Lucky Luke to lock bits. *IEEE Security & Privacy*, 18 (2):61–66, March/April 2020. ISSN 1558-4046.

Sellami:2022:DRL

[SHB22] Bassem Sellami, Akram Hakiri, and Sadok Ben Yahia. Deep Reinforcement Learning for energy-aware task offloading in join SDN-Blockchain 5G massive IoT edge network. *Future Generation Computer Systems*, 137(??): 363–379, December 2022. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X22002588.

Satar:2021:TVC

[SHHM21] Siti Dhalila Mohd Satar,

Masnida Hussin, Zurina Mohd Hanapi, and Mohamad Afendee Mohamed. Towards virtuous cloud data storage using access policy hiding in ciphertext policy attribute-based encryption. *Future Internet*, 13(11):279, October 30, 2021. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/13/11/279`.

Shinagawa:2022:QAS

[SI22] Kazuo Shinagawa and Tetsu Iwata. Quantum attacks on sum of even-Mansour pseudorandom functions. *Information Processing Letters*, 173(??):Article 106172, January 2022. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019021000879`.

Shin:2021:VBP

[SJHL21] Ji Sun Shin, Minjae Jo, Jung Yeon Hwang, and Jaehwan Lee. A verifier-based password-authenticated key exchange using tamper-proof hardware. *The Computer Journal*, 64(8):1293–1302, August 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/64/8/1293/6064819`.

S:2020:SPE

[SK20a] Ajish S. and K. S. Anil Kumar. Security and performance enhancement of fingerprint biometric template using symmetric hashing. *Computers & Security*, 90(??): Article 101714, March 2020. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S016740482030002X`.

Shahid:2020:SDS

[SK20b] Furqan Shahid and Abid Khan. Smart Digital Signatures (SDS): a post-quantum digital signature scheme for distributed ledgers. *Future Generation Computer Systems*, 111(??):241–253, October 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X19319892`.

Siddiqui:2021:CBV

[SK21] Tanveer J. Siddiqui and Ashish Khare. Chaos-based video steganography method in discrete cosine transform domain. *International Journal of Image and Graphics (IJIG)*, 21(02): ??, April 2021. ISSN 0219-4678. URL `https://www.worldscientific.com/doi/10.1142/S0219467821500157`.

Streit:2022:DET

[SKB+22] Franz-Josef Streit, Paul Krüger, Andreas Becher, Stefan Wildermann, and Jürgen

Teich. Design and evaluation of a tunable PUF architecture for FPGAs. *ACM Transactions on Reconfigurable Technology and Systems*, 15(1):7:1–7:27, March 2022. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic). URL `https://dl.acm.org/doi/10.1145/3491237`.

Savvides:2020:ECP

[SKE20] Savvas Savvides, Darshika Khandelwal, and Patrick Eugster. Efficient confidentiality-preserving data analytics over symmetrically encrypted datasets. *Proceedings of the VLDB Endowment*, 13 (8):1290–1303, April 2020. CODEN ???? ISSN 2150-8097. URL `https://dl.acm.org/doi/abs/10.14778/3389133.3389144`.

Sakalis:2020:USD

[SKR+20] C. Sakalis, S. Kaxiras, A. Ros, A. Jimborean, and M. Själander. Understanding selective delay as a method for efficient secure speculative execution. *IEEE Transactions on Computers*, 69(11): 1584–1595, November 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Sasongko:2021:HCS

[SKW+21] Arif Sasongko, I. M. Narendra Kumara, Arief Wicaksana, Frédéric Rousseau, and Olivier Muller. Hardware context switch-based cryptographic accelerator for handling multiple streams. *ACM Transactions on Reconfigurable Technology and Systems*, 14(3):14:1–14:25, September 2021. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic). URL `https://dl.acm.org/doi/10.1145/3460941`.

Slayton:2022:DCW

[Sla22] Rebecca Slayton. *Democratizing Cryptography: The Work of Whiteld Diffie and Martin Hellman*, volume 42 of *ACM books*. ACM Press, New York, NY 10036, USA, 2022. ISBN 1-4503-9825-1 (paperback), 1-4503-9826-X (epub), 1-4503-9827-8 (hardcover), 1-4503-9828-6 (ebook). ISSN 2374-6777. xx + 538 pp. LCCN ????

Shen:2021:SAC

[SLL+21] Jian Shen, Dengzhi Liu, Qi Liu, Xingming Sun, and Yan Zhang. Secure authentication in cloud big data with hierarchical attribute authorization structure. *IEEE Transactions on Big Data*, 7(4):668–677, 2021. ISSN 2332-7790.

Shi:2021:WEU

[SLLC21] Cong Shi, Jian Liu, Hongbo Liu, and Yingying Chen. WiFi-enabled user authentication through deep learning in daily activities. *ACM*

Transactions on Internet of Things (TIOT), 2(2):13:1–13:25, May 2021. CODEN ???? ISSN 2691-1914 (print), 2577-6207 (electronic). URL `https://dl.acm.org/doi/10.1145/3448738`.

Shen:2020:ECA

[SLS+20] Jian Shen, Dengzhi Liu, Xingming Sun, Fushan Wei, and Yang Xiang. Efficient cloud-aided verifiable secret sharing scheme with batch verification for smart cities. *Future Generation Computer Systems*, 109 (??):450–456, August 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X17318629`.

Shao:2021:EBR

[SLZ+21] Huiru Shao, Jing Li, Jia Zhang, Hui Yu, and Jiande Sun. Eye-based recognition for user identification on mobile devices. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 16(4):117:1–117:19, January 2021. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL `https://dl.acm.org/doi/10.1145/3399659`.

Sun:2020:RIB

[SMS+20] Yinxia Sun, Yi Mu, Willy Susilo, Futai Zhang, and Anmin Fu. Revocable identity-based encryption with server-aided ciphertext evolution. *Theoretical Computer Science*, 815(??):11–24, May 2, 2020. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397520301298`.

Sainani:2020:IRS

[SNS+20] Henanksha Sainani, Josephine M. Namayanja, Guneeti Sharma, Vasundhara Misal, and Vandana P. Janeja. IP reputation scoring with geo-contextual feature augmentation. *ACM Transactions on Management Information Systems (TMIS)*, 11(4):26:1–26:29, December 2020. CODEN ???? ISSN 2158-656X (print), 2158-6578 (electronic). URL `https://dl.acm.org/doi/10.1145/3419373`.

Shuaieb:2020:RRF

[SOA+20] Wafa Shuaieb, George Oguntala, Ali AlAbdullah, Huthaifa Obeidat, Rameez Asif, Raed A. Abd-Alhameed, Mohammed S. Bin-Melha, and Chakib Kara-Zaïtri. RFID RSS fingerprinting system for wearable human activity recognition. *Future Internet*, 12 (2):33, February 12, 2020. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/12/2/33`.

Shanmugam:2020:TLA

[SP20a] Anitha Shanmugam and Jayanthi Paramasivam. A two-level authentication scheme for clone node detection in smart cities using Internet of Things. *Computational Intelligence*, 36(3):1200–1220, August 2020. CODEN COMIE6. ISSN 0824-7935 (print), 1467-8640 (electronic).

Singh:2020:IBB

[SP20b] Sonika Singh and Sahadeo Padhye. Identity based blind signature scheme over NTRU lattices. *Information Processing Letters*, 155 (??):Article 105898, March 2020. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019019301814`.

Shaikh:2021:STB

[SP21] Ayesha S. Shaikh and Vibha D. Patel. Significance of the transition to biometric template protection: Explore the future. *International Journal of Image and Graphics (IJIG)*, 21(02):??, April 2021. ISSN 0219-4678. URL `https://www.worldscientific.com/doi/10.1142/S021946782150025X`.

Salvakkam:2022:MLM

[SP22a] Dilli Babu Salvakkam and Rajendra Pamula. MESSB-LWE: multi-extractable somewhere statistically binding and learning with error-based integrity and authentication for cloud storage. *The Journal of Supercomputing*, 78(14):16364–16393, September 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `https://link.springer.com/article/10.1007/s11227-022-04497-1`.

Shukla:2022:NEB

[SP22b] Shivangi Shukla and Sankita J. Patel. A novel ECC-based provably secure and privacy-preserving multi-factor authentication protocol for cloud computing. *Computing*, 104(5):1173–1202, May 2022. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL `https://link.springer.com/article/10.1007/s00607-021-01041-6`.

S:2020:SMB

[SPJ20] Anguraj S, Shantharajah S P, and Jeba Emilyn J. A steganographic method based on optimized audio embedding technique for secure data communication in the Internet of Things. *Computational Intelligence*, 36(2): 557–573, May 2020. CODEN COMIE6. ISSN 0824-7935 (print), 1467-8640 (electronic).

Sadhukhan:2021:LRU

[SRD21] Dipanwita Sadhukhan, Sangram Ray, and Mou Das-gupta. A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography. *The Journal of Supercomputing*, 77(2):1114–1151, February 2021. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-020-03318-7.

Singh:2022:TII

[SS22] Kedar Nath Singh and Amit Kumar Singh. Towards integrating image encryption with compression: a survey. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 18 (3):89:1–89:21, August 2022. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL https://dl.acm.org/doi/10.1145/3498342.

Sahu:2021:LMP

[SSP21] Amiya Kumar Sahu, Suraj Sharma, and Deepak Puthal. Lightweight multi-party authentication and key agreement protocol in IoT-based e-healthcare service. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 17 (2s):64:1–64:20, June 2021. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL https://dl.acm.org/doi/10.1145/3398039.

Szigeti:2020:PCH

[SSvW20] Jenő Szigeti, Szilvia Szilágyi, and Leon van Wyk. A power Cayley–Hamilton identity for $n \times n$ matrices over a Lie nilpotent ring of index k. *Linear Algebra and its Applications*, 584(??): 153–163, January 1, 2020. CODEN LAAPAW. ISSN 0024-3795 (print), 1873-1856 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0024379519303994.

Sanzo:2021:DKC

[SSW21] Karen L. Sanzo, Jay Paredes Scribner, and Hongyi Wu. Designing a K-16 cybersecurity collaborative: CIPHER. *IEEE Security & Privacy*, 19 (2):56–59, 2021. ISSN 1540-7993 (print), 1558-4046 (electronic).

Schneider:2020:CPP

[ST20] T. Schneider and A. Treiber. A comment on privacy-preserving scalar product protocols as proposed in SPOC. *IEEE Transactions on Parallel and Distributed Systems*, 31(3):543–546, March 2020. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Susilo:2021:WTA

[ST21] Willy Susilo and Joseph Tonien. A Wiener-type attack on an RSA-like cryptosystem constructed from cubic Pell equations. *Theoretical Computer Science*, 885(??):125–130, September 11, 2021. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S030439752100390X.

Saxena:2020:PBC

[STG+20] Neetesh Saxena, Ieuan Thomas, Prosante Gope, Pete Burnap, and Neeraj Kumar. PharmaCrypt: Blockchain for critical pharmaceutical industry to counterfeit drugs. *Computer*, 53(7):29–44, July 2020. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Singh:2021:JEC

[STJ+21] A. K. Singh, S. Thakur, Alireza Jolfaei, Gautam Srivastava, MD. Elhoseny, and A. Mohan. Joint encryption and compression-based watermarking technique for security of digital documents. *ACM Transactions on Internet Technology (TOIT)*, 21(1):18:1–18:20, February 2021. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic). URL https://dl.acm.org/doi/10.1145/3414474.

Suzuki:2020:EPK

[STK20] Kaichi Suzuki, Atsushi Takayasu, and Noboru Kunihiro. Extended partial key exposure attacks on RSA: Improvement up to full size decryption exponents. *Theoretical Computer Science*, 841(??):62–83, November 12, 2020. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397520303820.

Saini:2023:CNF

[STK23] A. Saini, A. Tsokanos, and R. Kirner. CryptoQNRG: a new framework for evaluation of cryptographic strength in quantum and pseudorandom number generation for key-scheduling algorithms. *The Journal of Supercomputing*, 79(11):12219–12237, July 2023. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-023-05115-4.

Sabir:2021:MLD

[SUBG21] Bushra Sabir, Faheem Ullah, M. Ali Babar, and Raj Gaire. Machine learning for detecting data exfiltration: a review. *ACM Computing Surveys*, 54(3):50:1–50:47, June 2021. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/doi/10.1145/3442181.

Sun:2022:CRV

[Sun22] Sheng Sun. A chosen random value attack on WPA3

SAE authentication protocol. *Digital Threats: Research and Practice (DTRAP)*, 3(2): 16:1–16:8, June 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3468526.

Sayeed:2022:ACI

[SVK+22] Aqsa Sayeed, Chaman Verma, Neerendra Kumar, Neha Koul, and Zoltán Illés. Approaches and challenges in Internet of Robotic Things. *Future Internet*, 14(9):265, September 14, 2022. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/14/9/265.

Sahai:2021:HUI

[SW21] Amit Sahai and Brent Waters. How to use indistinguishability obfuscation: Deniable encryption, and more. *SIAM Journal on Computing*, 50(3):857–908, ???? 2021. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Shi:2021:AVC

[SWCS21] Cong Shi, Yan Wang, Yingying Jennifer Chen, and Nitesh Saxena. Authentication of voice commands by leveraging vibrations in wearables. *IEEE Security & Privacy*, 19(6):83–92, November/December 2021. ISSN 1540-7993 (print), 1558-4046 (electronic).

Sun:2020:DAS

[SWK+20] Jianguo Sun, Wenshan Wang, Liang Kou, Yun Lin, Liguo Zhang, Qingan Da, and Lei Chen. A data authentication scheme for UAV ad hoc network communication. *The Journal of Supercomputing*, 76(6):4041–4056, June 2020. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Sun:2021:BEN

[SWLL21] Yuanyuan Sun, Sheng Wang, Huorong Li, and Feifei Li. Building enclave-native storage engines for practical encrypted databases. *Proceedings of the VLDB Endowment*, 14(6):1019–1032, February 2021. CODEN ???? ISSN 2150-8097. URL https://dl.acm.org/doi/10.14778/3447689.3447705.

Shen:2022:IBA

[SWZ22] Shiyu Shen, Hongbing Wang, and Yunlei Zhao. Identity-based authenticated encryption with identity confidentiality. *Theoretical Computer Science*, 901(??):1–18, January 12, 2022. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397521006897.

Sehrawat:2021:EST

[SYD21] Vipin Singh Sehrawat, Foo Yee Yeo, and Yvo Desmedt. Extremal set theory and LWE based access structure hiding verifiable secret sharing with malicious-majority and free verification. *Theoretical Computer Science*, 886 (??):106–138, September 13, 2021. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397521004266.

Sisman:2021:OVC

[SYKL21] Berrak Sisman, Junichi Yamagishi, Simon King, and Haizhou Li. An overview of voice conversion and its challenges: From statistical modeling to deep learning. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 29(??):132–157, January 2021. URL https://dl.acm.org/doi/10.1109/TASLP.2020.3038524.

Shang:2021:IBD

[SZC+21] Tao Shang, Feng Zhang, Xingyue Chen, Jianwei Liu, and Xinxi Lu. Identity-based dynamic data auditing for big data storage. *IEEE Transactions on Big Data*, 7(6):913–921, December 2021. CODEN ???? ISSN 2332-7790.

Sun:2020:CSR

[SZFX20] Yinxia Sun, Futai Zhang, Anmin Fu, and Zhe Xia. CCA-secure and revocable certificateless encryption with ciphertext evolution. *International Journal of Foundations of Computer Science (IJFCS)*, 31(2):175–191, February 2020. ISSN 0129-0541. URL https://www.worldscientific.com/doi/10.1142/S0129054120500021.

Su:2022:BRB

[SZM22] Jian Su, Leyou Zhang, and Yi Mu. BA-RMKABSE: Blockchain-aided ranked multi-keyword attribute-based searchable encryption with hiding policy for smart health system. *Future Generation Computer Systems*, 132(??):299–309, July 2022. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X22000292.

Su:2020:SOA

[SZX20] Qianqian Su, Rui Zhang, and Rui Xue. Secure outsourcing algorithms for composite modular exponentiation based on single untrusted cloud. *The Computer Journal*, 63(8):1271, August 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/63/8/1271/5823571.

Talamo:2020:BBP

[TADS20] Maurizio Talamo, Franco Arcieri, Andrea Dimitri, and

Christian H. Schunck. A blockchain based PKI validation system based on rare events management. *Future Internet*, 12(2):40, February 14, 2020. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/12/2/40.

Tabrizian:2021:HAN

[TB21] Roozbeh Tabrizian and Swarup Bhunia. The hidden authenticators: Nanometer-scale electromechanical tags could thwart counterfeiters. *IEEE Spectrum*, 58(6):32–37, June 2021. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Tseng:2021:LLR

[TCH21] Yuh-Min Tseng, Jian-Lun Chen, and Sen-Shan Huang. A lightweight leakage-resilient identity-based mutual authentication and key exchange protocol for resource-limited devices. *Computer Networks (Amsterdam, Netherlands: 1999)*, 196 (??):??, September 4, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128621002826.

Tarkhanov:2021:CAI

[TFNF21] I. A. Tarkhanov, D. V. Fomin-Nilov, and M. V. Fomin. Crypto access: Is it possible to use cryptocurrencies in scholarly periodicals? *Learned Publishing*, 34 (2):253–261, April 2021. CODEN LEPUFJ. ISSN 0953-1513 (print), 1741-4857 (electronic).

Tang:2021:STM

[TGC+21] Xinyu Tang, Cheng Guo, Kim-Kwang Raymond Choo, Yining Liu, and Long Li. A secure and trustworthy medical record sharing scheme based on searchable encryption and blockchain. *Computer Networks (Amsterdam, Netherlands: 1999)*, 200 (??):??, December 9, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S138912862100462X.

Theofanos:2020:USO

[The20] M. Theofanos. Is usable security an oxymoron? *Computer*, 53(2):71–74, February 2020. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Tiplea:2020:DQR

[TITN20] Ferucio Laurentiu Tiplea, Sorin Iftene, George Teseleanu, and Anca-Maria Nica. On the distribution of quadratic residues and non-residues modulo composite integers and applications to cryptography. *Applied Mathematics and Computation*, 372 (??):Article 124993, May 1,

2020. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300319309853.

Tu:2021:SLM

[TKP21] Yu-Ju Tu, Gaurav Kapoor, and Selwyn Piramuthu. Security of lightweight mutual authentication protocols. *The Journal of Supercomputing*, 77(5):4565–4581, May 2021. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-020-03448-y.

Tian:2020:NCL

[TLD+20] Yangguang Tian, Yingjiu Li, Robert H. Deng, Nan Li, Guomin Yang, and Zheng Yang. A new construction for linkable secret handshake. *The Computer Journal*, 63(4):536–548, April 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/63/4/536/5612724.

Tian:2021:URS

[TLMY21] Yangguang Tian, Yingjiu Li, Yi Mu, and Guomin Yang. Unlinkable and revocable secret handshake. *The Computer Journal*, 64 (8):1303–1314, August 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/64/8/1303/6095852.

Tian:2020:LRB

[TLS+20] Yangguang Tian, Yingjiu Li, Binanda Sengupta, Nan Li, and Chunhua Su. Leakage-resilient biometric-based remote user authentication with fuzzy extractors. *Theoretical Computer Science*, 814(??):223–233, April 24, 2020. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397520300785.

Tsiokanos:2021:DPD

[TMG+21] Ioannis Tsiokanos, Jack Miskelly, Chongyan Gu, Maire O'neill, and Georgios Karakonstantis. DTA-PUF: Dynamic timing-aware physical unclonable function for resource-constrained devices. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 17(3): 32:1–32:24, July 2021. CODEN ???? ISSN 1550-4832. URL https://dl.acm.org/doi/10.1145/3434281.

Tioura:2020:HPS

[TMKS20] Abdelhamid Tioura, Hamouma Moumen, Hamoudi Kalla, and Ahmed Ait Saidi. A hybrid protocol to solve authenticated Byzantine consensus. *Fundamenta Informaticae*, 173(1):73–89, ????

2020. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Tu:2020:LGI

[TMZ+20] Xiaoguang Tu, Zheng Ma, Jian Zhao, Guodong Du, Mei Xie, and Jiashi Feng. Learning generalizable and identity-discriminative representations for face anti-spoofing. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 11(5): 60:1–60:19, September 2020. CODEN ???? ISSN 2157-6904 (print), 2157-6912 (electronic). URL https://dl.acm.org/doi/10.1145/3402446.

Tomida:2020:TSI

[Tom20] Junichi Tomida. Tightly secure inner product functional encryption: Multi-input and function-hiding constructions. *Theoretical Computer Science*, 833(??): 56–86, September 12, 2020. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397520302711.

Thao:2021:OSS

[TRB+21] Tran Phuong Thao, Mohammad Shahriar Rahman, Md Zakirul Alam Bhuiyan, Ayumu Kubota, Shinsaku Kiyomoto, and Kazumasa Omote. Optimizing share size in efficient and robust secret sharing scheme for big data. *IEEE Transactions on Big Data*, 7(4):703–716, 2021. ISSN 2332-7790.

Tanwar:2020:CPP

[TRRB20] Vishesh Kumar Tanwar, Balasubramanian Raman, Amitesh Singh Rajput, and Rama Bhargava. CryptoLesion: a privacy-preserving model for lesion segmentation using whale optimization over cloud. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 16(2):50:1–50:23, June 2020. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3380743.

Turan:2020:HAH

[TRV20] F. Turan, S. S. Roy, and I. Verbauwhede. HEAWS: An accelerator for homomorphic encryption on the Amazon AWS FPGA. *IEEE Transactions on Computers*, 69(8):1185–1196, 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Tomar:2020:MTV

[TS20] Ravi Tomar and Sarishma. Maintaining trust in VANETs using blockchain. *ACM SIGADA Ada Letters*, 40(1): 91–96, October 2020. CODEN AALEE5. ISSN 1094-3641 (print), 1557-9476 (electronic). URL https://

dl.acm.org/doi/10.1145/3431235.3431244.

Tanveer:2022:EIP

[TSAS22] Muhammad Tanveer, Tariq Shah, Asif Ali, and Dawood Shah. An efficient image privacy-preserving scheme based on mixed chaotic map and compression. *International Journal of Image and Graphics (IJIG)*, 22(02):??, April 2022. ISSN 0219-4678. URL https://www.worldscientific.com/doi/10.1142/S0219467822500206.

Tropea:2022:SWS

[TSDG22] Mauro Tropea, Mattia Giovanni Spina, Floriano De Rango, and Antonio Francesco Gentile. Security in wireless sensor networks: a cryptography performance analysis at MAC layer. *Future Internet*, 14(5):145, May 10, 2022. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/14/5/145.

Tsai:2021:LST

[TSFS21] Po-An Tsai, Andres Sanchez, Christopher W. Fletcher, and Daniel Sanchez. Leaking secrets through compressed caches. *IEEE Micro*, 41(3):27–33, 2021. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Thakur:2021:NDB

[TSG21] S. Thakur, A. K. Singh, and S. P. Ghrera. NSCT domain-based secure multiple-watermarking technique through lightweight encryption for medical images. *Concurrency and Computation: Practice and Experience*, 33(2):e5108:1–e5108:??, January 25, 2021. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Tahir:2020:PDQ

[TSR+20] Shahzaib Tahir, Liutauras Steponkus, Sushmita Ruj, Muttukrishnan Rajarajan, and Ali Sajjad. A parallelized disjunctive query based searchable encryption scheme for big data. *Future Generation Computer Systems*, 109(??):583–592, August 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X17321842.

Tan:2021:BEA

[TSY+21] Liang Tan, Na Shi, Keping Yu, Moayad Aloqaily, and Yaser Jararweh. A blockchain-empowered access control framework for smart devices in green Internet of Things. *ACM Transactions on Internet Technology (TOIT)*, 21(3):80:1–80:20, June 2021. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic). URL https://dl.acm.org/doi/10.1145/3433542.

Tian:2021:CIG

[TTL+21] Jiajie Tian, Qihao Tang, Rui Li, Zhu Teng, Baopeng Zhang, and Jianping Fan. A camera identity-guided distribution consistency method for unsupervised multi-target domain person re-identification. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 12(4):38:1–38:18, August 2021. CODEN ???? ISSN 2157-6904 (print), 2157-6912 (electronic). URL https://dl.acm.org/doi/10.1145/3454130.

Trivedi:2020:NIC

[TTP20] Amit Kumar Trivedi, Dalton Meitei Thounaojam, and Shyamosree Pal. Non-invertible cancellable fingerprint template for fingerprint biometric. *Computers & Security*, 90(??): Article 101690, March 2020. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167404819302275.

Tahir:2021:NIP

[TTT+21] Ruhma Tahir, Shahzaib Tahir, Hasan Tahir, Klaus McDonald-Maier, Gareth Howells, and Ali Sajjad. A novel ICMetric public key framework for secure communication. *Journal of Network and Computer Applications*, 195(??):??, December 1, 2021. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804521002332.

Turing:2020:CBP

[Tur20] Dermot Turing. *The Codebreakers of Bletchley Park: the Secret Intelligence Station That Helped Defeat the Nazis*. Arcturus Publishing Limited, London, UK, 2020. ISBN 1-78950-621-2, 1-83857-650-9 (paperback). 256 pp. LCCN ???? With an introduction by Christopher M. Andrew.

Taleb:2021:SVD

[TV21] Abdul Rahman Taleb and Damien Vergnaud. Speeding-up verification of digital signatures. *Journal of Computer and System Sciences*, 116(??):22–39, March 2021. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000020300854.

Takayasu:2021:RIB

[TW21] Atsushi Takayasu and Yohei Watanabe. Revocable identity-based encryption with bounded decryption key exposure resistance: Lattice-based construction and more. *Theoretical Computer Science*, 849 (??):64–98, January 6, 2021.

CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S030439752030579X.

Tu:2021:ROM

[TWH+21] Shanshan Tu, Muhammad Waqas, Fengming Huang, Ghulam Abbas, and Ziaul Haq Abbas. A revocable and outsourced multi-authority attribute-based encryption scheme in fog computing. *Computer Networks (Amsterdam, Netherlands: 1999)*, 195(??):??, August 4, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128621002474.

Tong:2021:IPP

[TZLZ21] Chao Tong, Mengze Zhang, Chao Lang, and Zhigao Zheng. An image privacy protection algorithm based on adversarial perturbation generative networks. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 17 (2):43:1–43:14, June 2021. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL https://dl.acm.org/doi/10.1145/3381088.

Unal:2021:SEI

[UAACH21] Devrim Unal, Abdulla Al-Ali, Ferhat Ozgur Catak, and Mohammad Hammoudeh. A secure and efficient Internet of Things cloud encryption scheme with forensics investigation compatibility based on identity-based encryption. *Future Generation Computer Systems*, 125(??): 433–445, December 2021. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X21002454.

ulHaq:2020:STF

[uHWZ20] Inam ul Haq, Jian Wang, and Youwen Zhu. Secure two-factor lightweight authentication protocol using self-certified public key cryptography for multi-server 5G networks. *Journal of Network and Computer Applications*, 161(??):??, July 1, 2020. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S108480452030134X.

Ueno:2020:HTG

[UMM+20] R. Ueno, S. Morioka, N. Miura, K. Matsuda, M. Nagata, S. Bhasin, Y. Mathieu, T. Graba, J. Danger, and N. Homma. High throughput/gate AES hardware architectures based on datapath compression. *IEEE Transactions on Computers*, 69(4):534–548, April 2020. CODEN ITCOB4. ISSN

0018-9340 (print), 1557-9956 (electronic).

Vachon:2020:IEP

[Vac20] Phil Vachon. The identity in everyone's pocket: Keeping users secure through their smartphones. *ACM Queue: Tomorrow's Computing Today*, 18(4):61–94, August 2020. URL `https://dl.acm.org/doi/10.1145/3424302.3428660`.

Vasan:2020:MCA

[VAV+20] D. Vasan, M. Alazab, S. Venkatraman, J. Akram, and Z. Qin. MTHAEL: Cross-architecture IoT malware detection based on neural network advanced ensemble learning. *IEEE Transactions on Computers*, 69(11):1654–1667, November 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Varshney:2021:RCU

[VCP21] Shubham Varshney, Pankaj Charpe, and S. K. Pal. Relation collection using Pollard special-q sieving to solve integer factorization and discrete logarithm problem. *The Journal of Supercomputing*, 77(3):2734–2769, March 2021. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `https://link.springer.com/article/10.1007/s11227-020-03351-6`.

Vasudev:2021:SPP

[VD21a] Harsha Vasudev and Debasis Das. P^2-SHARP: Privacy preserving secure hash based authentication and revelation protocol in IoVs. *Computer Networks (Amsterdam, Netherlands: 1999)*, 191(??):??, May 22, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128621001146`.

Vishwakarma:2021:SIS

[VD21b] Lokendra Vishwakarma and Debasis Das. SCAB–IoTA: Secure communication and authentication for IoT applications using blockchain. *Journal of Parallel and Distributed Computing*, 154(??):94–105, August 2021. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0743731521000800`.

Beirendonck:2021:SCR

[VDK+21] Michiel Van Beirendonck, Jan-Pieter D'anvers, Angshuman Karmakar, Josep Balasch, and Ingrid Verbauwhede. A side-channel-resistant implementation of SABER. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 17(2):10:1–10:26, April 2021. CODEN ???? ISSN 1550-

4832. URL https://dl.acm.org/doi/10.1145/3429983.

Vandervelden:2022:SKV

[VDSB22] Thibaut Vandervelden, Ruben De Smet, Kris Steenhaut, and An Braeken. SHA 3 and Keccak variants computation speeds on constrained devices. *Future Generation Computer Systems*, 128(??):28–35, March 2022. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X21003885.

Vandana:2022:ARB

[VK22] Vandana and Navdeep Kaur. Analytical review of biometric technology employing vivid modalities. *International Journal of Image and Graphics (IJIG)*, 22(01):??, January 2022. ISSN 0219-4678. URL https://www.worldscientific.com/doi/10.1142/S0219467822500048.

Vgena:2022:DRS

[VKKG22] Katerina Vgena, Angeliki Kitsiou, Christos Kalloniatis, and Stefanos Gritzalis. Determining the role of social identity attributes to the protection of users' privacy in social media. *Future Internet*, 14(9):249, August 24, 2022. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/14/9/249.

Vryzas:2022:PWA

[VKV+22] Nikolaos Vryzas, Anastasia Katsaounidou, Lazaros Vrysis, Rigas Kotsakis, and Charalampos Dimoulas. A prototype Web application to support human-centered audiovisual content authentication and crowdsourcing. *Future Internet*, 14(3):75, February 27, 2022. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/14/3/75.

vanOorschot:2020:CSI

[vO20] Paul C. van Oorschot. *Computer Security and the Internet: Tools and Jewels*. Information Security and Cryptography Series. Springer International Publishing, Cham, Switzerland, 2020. ISBN 3-030-33648-4 (hardcover), 3-030-33649-2 (e-book), 3-030-33650-6. xxi + 365 pp. LCCN QA76.9.A25. URL https://people.scs.carleton.ca/~paulv/toolsjewels.html.

Varri:2020:SRS

[VPK20] Umasankararao Varri, Syamkumar Pasupuleti, and K. V. Kadambari. A scoping review of searchable encryption schemes in cloud computing: taxonomy, methods, and recent developments. *The Journal of Supercomputing*, 76(4):3013–3042, April 2020. CODEN JOSUED. ISSN 0920-

8542 (print), 1573-0484 (electronic).

vanSchaik:2020:CLD

[vSMK+20] Stephan van Schaik, Marina Minkin, Andrew Kwong, Daniel Genkin, and Yuval Yarom. CacheOut: Leaking data on Intel CPUs via cache evictions. Report, University of Michigan and University of Adelaide and Data61, Ann Arbor, MI, USA and Adelaide, Australia, January 27, 2020. 16 pp. URL `https://cacheoutattack.com/CacheOut.pdf`.

Vucinic:2022:LAK

[VSMW22] Mališa Vučinić, Göran Selander, John Preuss Mattsson, and Thomas Watteyne. Lightweight authenticated key exchange with EDHOC. *Computer*, 55(4): 94–100, April 2022. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

vanSchaik:2020:RAA

[vSRW+20] Paul van Schaik, Karen Renaud, Christopher Wilson, Jurjen Jansen, and Joseph Onibokun. Risk as affect: the affect heuristic in cybersecurity. *Computers & Security*, 90(??):Article 101651, March 2020. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167404819301956`.

Vanderhallen:2021:RAA

[VVPM21] Stien Vanderhallen, Jo Van Bulck, Frank Piessens, and Jan Tobias Mühlberg. Robust authentication for automotive control networks through covert channels. *Computer Networks (Amsterdam, Netherlands: 1999)*, 193(??):??, July 5, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128621001699`.

Wang:2021:IFI

[WCD21] Gaoli Wang, Zhenfu Cao, and Xiaolei Dong. Improved file-injection attacks on searchable encryption using finite set theory. *The Computer Journal*, 64(8): 1264–1276, August 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/64/8/1264/6048928`.

Wang:2020:HFR

[WCQ+20] Ge Wang, Haofan Cai, Chen Qian, Jinsong Han, Shouqian Shi, Xin Li, Han Ding, Wei Xi, and Jizhong Zhao. Hu-Fu: Replay-resilient RFID authentication. *IEEE/ACM Transactions on Networking*, 28(2):547–560, April 2020. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic). URL `https:`

//dl.acm.org/doi/abs/10.1109/TNET.2020.2964290.

Wang:2021:ABB

[WCX21] Qin Wang, Shiping Chen, and Yang Xiang. Anonymous blockchain-based system for consortium. *ACM Transactions on Management Information Systems (TMIS)*, 12(3):26:1–26:25, July 2021. CODEN ???? ISSN 2158-656X (print), 2158-6578 (electronic). URL https://dl.acm.org/doi/10.1145/3459087.

Wang:2022:LBP

[WCXW22] Peng Wang, Biwen Chen, Tao Xiang, and Zhongming Wang. Lattice-based public key searchable encryption with fine-grained access control for edge computing. *Future Generation Computer Systems*, 127 (??):373–383, February 2022. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X21003587.

Wu:2020:BLS

[WCYL20] Pin Wu, Xuting Chang, Yang Yang, and Xiaoqiang Li. BASN-learning steganography with a binary attention mechanism. *Future Internet*, 12(3):43, February 27, 2020. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/12/3/43.

Wang:2020:PQH

[WCZQ20] Luping Wang, Jie Chen, Kai Zhang, and Haifeng Qian. A post-quantum hybrid encryption based on QC-LDPC codes in the multi-user setting. *Theoretical Computer Science*, 835(??):82–96, October 2, 2020. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397520303558.

Wang:2021:IFD

[WDFN21] Rong Wang, Xiaoni Du, Cuiling Fan, and Zhihua Niu. Infinite families of 2-designs from a class of linear codes related to Dembowski–Ostrom functions. *International Journal of Foundations of Computer Science (IJFCS)*, 32(03):253–267, April 2021. ISSN 0129-0541. URL https://www.worldscientific.com/doi/10.1142/S0129054121500143.

Wang:2022:ESV

[WDJZ22] Zuan Wang, Xiaofeng Ding, Hai Jin, and Pan Zhou. Efficient secure and verifiable location-based skyline queries over encrypted data. *Proceedings of the VLDB Endowment*, 15(9):1822–1834, May 2022. CODEN ???? ISSN 2150-8097. URL https://dl.acm.org/doi/10.14778/3538598.3538605.

Wazid:2020:LCL

[WDKV20] Mohammad Wazid, Ashok Kumar Das, Vivekananda Bhat K., and Athanasios V. Vasilakos. LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment. *Journal of Network and Computer Applications*, 150(??): ??, January 15, 2020. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S108480451930356X.

Wiefling:2021:VYH

[WDL21] Stephan Wiefling, Markus Dürmuth, and Luigi Lo Iacono. Verify it's you: How users perceive risk-based authentication. *IEEE Security & Privacy*, 19(6):47–57, November/December 2021. ISSN 1540-7993 (print), 1558-4046 (electronic).

West:2022:CIC

[Wes22] Sarah Myers West. Cryptography as information control. *Social Studies of Science*, 52 (3):353–375, June 1, 2022. CODEN SSSCDH. ISSN 0306-3127 (print), 1460-3659 (electronic). URL https://journals.sagepub.com/doi/full/10.1177/03063127221078314.

Wang:2021:MSD

[WFRZ21] Zichi Wang, Guorui Feng, Yanli Ren, and Xinpeng Zhang. Multichannel steganography in digital images for multiple receivers. *IEEE MultiMedia*, 28(1):65–73, 2021. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic).

Wang:2022:CAE

[WGYZ22] Zhihui Wang, Liheng Gong, Jingjing Yang, and Xiao Zhang. Cloud-assisted elliptic curve password authenticated key exchange protocol for wearable healthcare monitoring system. *Concurrency and Computation: Practice and Experience*, 34 (9):e5734:1–e5734:??, April 25, 2022. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Wu:2022:ALC

[WH22] Da-Chun Wu and Yu-Tsung Hsu. Authentication of LINE chat history files by information hiding. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 18 (1):22:1–22:23, January 2022. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL https://dl.acm.org/doi/10.1145/3474225.

Wang:2020:SEC

[WHC20] X. Wang, F. Huang, and H. Chen. Secure and efficient control data isolation with register-based data cloaking.

IEEE Transactions on Computers, 69(2):226–238, February 2020. CODEN ITCOB4. ISSN 2326-3814.

Wang:2020:LMB

[WHF+20] Junchao Wang, Kaining Han, Shengwen Fan, Ying Zhang, Honghao Tan, Gwanggil Jeon, Yu Pang, and Jinzhao Lin. A logistic mapping-based encryption scheme for wireless body area networks. *Future Generation Computer Systems*, 110 (??):57–67, September 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X19335617`.

Wang:2020:DVP

[WHJ20] Huaqun Wang, Debiao He, and Yimu Ji. Designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography. *Future Generation Computer Systems*, 107(??):854–862, June 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X1731350X`.

Wang:2020:GLA

[WHSX20] Danxin Wang, Chuanhe Huang, Xieyang Shen, and Naixue Xiong. A general location-authentication based secure participant recruitment scheme for vehicular crowdsensing. *Computer Networks (Amsterdam, Netherlands: 1999)*, 171(??): Article 107152, April 22, 2020. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128619310618`.

Wang:2022:LCG

[WHW22] Zhihao Wang, Ru Huo, and Shuo Wang. A lightweight certificateless group key agreement method without pairing based on blockchain for smart grid. *Future Internet*, 14(4):119–??, April 14, 2022. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/14/4/119`.

Wang:2020:RIN

[WL20] Hao Wang and Kaiju Li. Resistance of IID noise in differentially private schemes for trajectory publishing. *The Computer Journal*, 63(4): 549–566, April 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/63/4/549/5625061`.

Wang:2021:HPP

[WL21] Baocheng Wang and Zetao Li. Healthchain: a privacy protection system for medical data based on blockchain. *Future Internet*, 13(10):247, September 24, 2021. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/13/10/247.

Wang:2020:HCA

[WLL20] Baocheng Wang, Zetao Li, and Haibin Li. Hybrid consensus algorithm based on modified proof-of-probability and DPoS. *Future Internet*, 12(8):122, July 24, 2020. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/12/8/122.

Wu:2020:SQI

[WLYL20] Zhijun Wu, Rong Li, Panpan Yin, and Changliang Li. Steganalysis of quantization index modulation steganography in G.723.1 codec. *Future Internet*, 12(1):17, January 19, 2020. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/12/1/17.

Wei:2021:IIS

[WLZY21] Tengda Wei, Ping Lin, Quanxin Zhu, and Qi Yao. Instability of impulsive stochastic systems with application to image encryption. *Applied Mathematics and Computation*, 402(??):Article 126098, August 1, 2021. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300321001466.

Wu:2022:PSL

[WMK22] Tsu-Yang Wu, Qian Meng, and Saru Kumari. A provably secure lightweight authentication protocol in mobile edge computing environments. *The Journal of Supercomputing*, 78(12):13893–13914, August 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-022-04411-9.

Wood:2020:HEM

[WNK20] Alexander Wood, Kayvan Najarian, and Delaram Kahrobaei. Homomorphic encryption for machine learning in medicine and bioinformatics. *ACM Computing Surveys*, 53(4):70:1–70:35, September 2020. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/doi/10.1145/3394658.

Park:2021:EIM

[wPHC21] Dong won Park, Seokhie Hong, and Sung Min Cho. Efficient implementation of modular multiplication over 192-bit NIST prime for 8-bit AVR-based sensor node. *The Journal of Supercomputing*, 77(5):4852–4870, May 2021. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-020-03441-5.

Wang:2021:CVP

[WQL+21] Minmei Wang, Chen Qian, Xin Li, Shouqian Shi, and Shigang Chen. Collaborative validation of public-key certificates for IoT by distributed caching. *IEEE/ ACM Transactions on Networking*, 29(1):92–105, February 2021. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic). URL https://dl.acm.org/doi/10.1109/TNET.2020.3029135.

Wang:2020:CSH

[WSS+20] Y. Wang, Y. Shen, C. Su, J. Ma, L. Liu, and X. Dong. CryptSQLite: SQLite with high data security. *IEEE Transactions on Computers*, 69(5):666–678, 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL https://ieeexplore.ieee.org/document/8946540.

Wehner:2021:IWQ

[WSS+21] Nikolas Wehner, Michael Seufert, Joshua Schuler, Sarah Wassermann, Pedro Casas, and Tobias Hossfeld. Improving Web QoE monitoring for encrypted network traffic through time series modeling. *ACM SIGMETRICS Performance Evaluation Review*, 48(4):37–40, May 2021. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic). URL https://dl.acm.org/doi/10.1145/3466826.3466840.

Wang:2020:UAM

[WWC+20] Chen Wang, Yan Wang, Yingying Chen, Hongbo Liu, and Jian Liu. User authentication on mobile devices: Approaches, threats and trends. *Computer Networks (Amsterdam, Netherlands: 1999)*, 170 (??):Article 107118, April 7, 2020. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128618312799.

Wang:2020:UNC

[WWL20] Xueping Wang, Yunhong Wang, and Weixin Li. U-Net conditional GANs for photo-realistic and identity-preserving facial expression synthesis. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 15(3s):1–23, January 2020. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3355397.

Wang:2020:EMF

[WWW20] Ding Wang, Ping Wang, and Chenyu Wang. Efficient multi-factor user authentication protocol with forward secrecy for real-time data access in WSNs. *ACM Transactions on Cyber-Physical Systems (TCPS)*, 4(3):30:1–30:26, March 2020. CODEN ???? ISSN 2378-962X (print), 2378-9638 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3325130.

Wang:2021:BSS

[WWYC21] Pan Wang, Zixuan Wang, Feng Ye, and Xuejiao Chen. ByteSGAN: a semi-supervised generative adversarial network for encrypted traffic classification in SDN edge gateway. *Computer Networks (Amsterdam, Netherlands: 1999)*, 200(??):??, December 9, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S138912862100459X.

Wang:2021:PAA

[WYLG21] Kun Wang, Jiahui Yu, Xiulong Liu, and Song Guo. A pre-authentication approach to proxy re-encryption in big data context. *IEEE Transactions on Big Data*, 7(4):657–667, 2021. ISSN 2332-7790.

Wang:2020:EWR

[WYZ+20] Ziyu Wang, Hui Yu, Zongyang Zhang, Jiaming Piao, and Jianwei Liu. ECDSA weak randomness in Bitcoin. *Future Generation Computer Systems*, 102(??):507–513, January 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X17330030.

Wang:2021:ADU

[WYZZ21] Xuerui Wang, Zheng Yan, Rui Zhang, and Peng Zhang. Attacks and defenses in user authentication systems: a survey. *Journal of Network and Computer Applications*, 188(??):??, August 15, 2021. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804521001028.

Wu:2020:MAR

[WZX20] Zhijun Wu, Yun Zhang, and Enzhong Xu. Multi-authority revocable access control method based on CP-ABE in NDN. *Future Internet*, 12(1):15, January 16, 2020. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/12/1/15.

Wang:2020:ZKV

[WZXX20] Qiang Wang, Fucai Zhou, Jian Xu, and Zifeng Xu. A (zero-knowledge) vector commitment with sum binding and its applications. *The Computer Journal*, 63(4):633–647, April 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/63/4/633/5627774.

Wang:2020:USF

[WZZW20] Ding Wang, Xizhe Zhang, Zijian Zhang, and Ping Wang. Understanding security failures of multi-factor authentication schemes for multi-server environments. *Computers & Security*, 88(??): Article 101619, January 2020. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S016740481930166X.

Xiong:2020:SDD

[XCB+20] Jinbo Xiong, Lei Chen, Md Zakirul Alam Bhuiyan, Chunjie Cao, Minshen Wang, Entao Luo, and Ximeng Liu. A secure data deletion scheme for IoT devices through key derivation encryption and data analysis. *Future Generation Computer Systems*, 111 (??):741–753, October 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X19314499.

Xiong:2022:RIB

[XCV22] Hu Xiong, Kim-Kwang Raymond Choo, and Athanasios V. Vasilakos. Revocable identity-based access control for big data with verifiable outsourced computing. *IEEE Transactions on Big Data*, 8 (1):1–13, February 2022. CODEN ???? ISSN 2332-7790.

Xu:2020:TTT

[XJ20] Runhua Xu and James Joshi. Trustworthy and transparent third-party authority. *ACM Transactions on Internet Technology (TOIT)*, 20(4):31:1–31:23, November 2020. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic). URL https://dl.acm.org/doi/10.1145/3386262.

Xia:2022:FCS

[XJG+22] Zhihua Xia, Qiuju Ji, Qi Gu, Chengsheng Yuan, and Fengjun Xiao. A format-compatible searchable encryption scheme for JPEG images using bag-of-words. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 18(3):85:1–85:18, August 2022. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL https://dl.acm.org/doi/10.1145/3492705.

Xu:2021:BBR

[XLL+21] Zisang Xu, Wei Liang, Kuan-Ching Li, Jianbo Xu, and Hai Jin. A blockchain-based roadside unit-assisted authentication and key agreement protocol for Internet of Vehicles. *Journal of Parallel and Distributed Computing*, 149(??):29–39, March 2021. CODEN JPDCER. ISSN

0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731520304044.

Xu:2022:DLF

[XLL+22] Liangliang Xu, Min Lyu, Zhipeng Li, Cheng Li, and Yinlong Xu. A data layout and fast failure recovery scheme for distributed storage systems with mixed erasure codes. *IEEE Transactions on Computers*, 71(8): 1740–1754, August 2022. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Xu:2020:SQK

[XMZ+20] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, 92(2):025002–??, February 2020. CODEN RMPHAT. ISSN 0034-6861 (print), 1538-4527 (electronic), 1539-0756. URL http://journals.aps.org/rmp/abstract/10.1103/RevModPhys.92.025002.

Xu:2022:MSC

[XPR+22] Zhuang Xu, Owen Pemberton, Sujoy Sinha Roy, David Oswald, Wang Yao, and Zhiming Zheng. Magnifying side-channel leakage of lattice-based cryptosystems with chosen ciphertexts: the case study of Kyber. *IEEE Transactions on Computers*, 71(9):2163–2176, September 2022. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Xiang:2021:MTD

[XRL+21] Yuexin Xiang, Wei Ren, Tiantian Li, Xianghan Zheng, Tianqing Zhu, and Kim-Kwang Raymond Choo. A multi-type and decentralized data transaction scheme based on smart contracts and digital watermarks. *Journal of Network and Computer Applications*, 176(??): ??, February 15, 2021. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804520304057.

Xie:2021:PLA

[XTHL21] Ning Xie, Haijun Tan, Lei Huang, and Alex X. Liu. Physical-layer authentication in wirelessly powered communication networks. *IEEE/ACM Transactions on Networking*, 29 (4):1827–1840, August 2021. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic). URL https://dl.acm.org/doi/10.1109/TNET.2021.3071670.

Xing:2021:AAA

[XWH21] Biao Xing, DanDan Wang, and Cuihua He. Accelerating DES and AES algorithms for a heterogeneous many-core processor. *International Journal of Parallel Programming*, 49(3): 463–486, June 2021. CODEN IJPPE5. ISSN 0885-7458 (print), 1573-7640 (electronic). URL https://link.springer.com/article/10.1007/s10766-021-00692-4.

Xu:2021:GAC

[XWM21] Rui Xu, Xu Wang, and Kirill Morozov. Group authentication for cloud-to-things computing: Review and improvement. *Computer Networks (Amsterdam, Netherlands: 1999)*, 198(??):??, October 24, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S138912862100356X.

Xu:2020:PPD

[XWW+20] Jian Xu, Laiwen Wei, Wei Wu, Andi Wang, Yu Zhang, and Fucai Zhou. Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber-physical system. *Future Generation Computer Systems*, 108(??):1287–1296, July 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X17326067.

Xu:2021:KGI

[XZH+21] Weitao Xu, Junqing Zhang, Shunqi Huang, Chengwen Luo, and Wei Li. Key generation for Internet of Things: a contemporary survey. *ACM Computing Surveys*, 54(1): 14:1–14:37, April 2021. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/doi/10.1145/3429740.

Xie:2020:PLA

[XZL20] Ning Xie, Shengli Zhang, and Alex X. Liu. Physical-layer authentication in non-orthogonal multiple access systems. *IEEE/ACM Transactions on Networking*, 28 (3):1144–1157, June 2020. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic). URL https://dl.acm.org/doi/10.1109/TNET.2020.2979058.

Xiong:2022:BBP

[XZL+22] Ting Xiong, Ran Zhang, Jiang Liu, Tao Huang, Yunjie Liu, and F. Richard Yu. A blockchain-based and privacy-preserved authentication scheme for inter-constellation collaboration in Space-Ground Integrated Networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 206(??):??, April 7, 2022. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http:

//www.sciencedirect.com/science/article/pii/S138912862200024X.

Yang:2021:OCS

[YAZ21] Zheng Yang, Sridhar Adepu, and Jianying Zhou. Opportunities and challenges in securing critical infrastructures through cryptography. *IEEE Security & Privacy*, 19(5):57–65, September/October 2021. ISSN 1540-7993 (print), 1558-4046 (electronic).

Yakubu:2022:BBA

[YC22a] Abukari Mohammed Yakubu and Yi Ping Phoebe Chen. A blockchain-based application for genomic access and variant discovery using smart contracts and homomorphic encryption. *Future Generation Computer Systems*, 137(??):234–247, December 2022. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X22002400.

Yan:2022:CDC

[YC22b] Hui Yan and Chaoyuan Cui. CacheHawkeye: Detecting cache side channel attacks based on memory events. *Future Internet*, 14(1):24, January 08, 2022. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/14/1/24.

Yang:2020:SLC

[YCL+20] Zhichao Yang, Rongmao Chen, Chao Li, Longjiang Qu, and Guomin Yang. On the security of LWE cryptosystem against subversion attacks. *The Computer Journal*, 63(4):495–507, April 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/63/4/495/5560305.

Yang:2020:SEF

[YCM+20] Fan Yang, Youmin Chen, Haiyu Mao, Youyou Lu, and Jiwu Shu. ShieldNVM: an efficient and fast recoverable system for secure non-volatile memory. *ACM Transactions on Storage*, 16(2):12:1–12:31, June 2020. CODEN ???? ISSN 1553-3077 (print), 1553-3093 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3381835.

Yan:2021:NMZ

[YD21] Zhenbin Yan and Yi Deng. Non-malleable zero-knowledge arguments with lower round complexity. *The Computer Journal*, 64(4):534–549, April 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/64/4/534/5869147.

Ye:2022:OAD

[YD22] Qianchuan Ye and Benjamin Delaware. Oblivious algebraic data types. *Proceedings of the ACM on Programming Languages (PACMPL)*, 6(POPL):51:1–51:29, January 2022. CODEN ???? ISSN 2475-1421 (electronic). URL `https://dl.acm.org/doi/10.1145/3498713`.

Yang:2020:HIB

[YDS+20] Zhichao Yang, Dung H Duong, Willy Susilo, Guomin Yang, Chao Li, and Rongmao Chen. Hierarchical identity-based signature in polynomial rings. *The Computer Journal*, 63(10):1490–1499, October 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/63/10/1490/5826091`.

Yang:2022:NVM

[YF22] Jing Yang and Fang-Wei Fu. New (k, l, m)-verifiable multi-secret sharing schemes based on XTR public key system. *Theoretical Computer Science*, 910(??):54–67, April 2, 2022. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397522000500`.

Yang:2020:ESM

[YFW20] Jing Yang, Mingyu Fan, and Guangwei Wang. Encryption scheme with mixed homomorphic signature based on message authentication for digital image. *The Journal of Supercomputing*, 76(2):1201–1211, February 2020. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Yadav:2020:EIA

[YG20] Navneet Yadav and Navdeep Goel. An effective image-adaptive hybrid watermarking scheme with transform coefficients. *International Journal of Image and Graphics (IJIG)*, 20(01):??, January 2020. ISSN 0219-4678. URL `https://www.worldscientific.com/doi/10.1142/S0219467820500023`.

Yao:2020:ETC

[YGW+20] Zhongjiang Yao, Jingguo Ge, Yulei Wu, Xiaosheng Lin, Runkang He, and Yuxiang Ma. Encrypted traffic classification based on Gaussian mixture models and Hidden Markov Models. *Journal of Network and Computer Applications*, 166(??):??, September 15, 2020. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804520301855`.

Yang:2022:UPL

[YH22] Shaojun Yang and Xinyi Huang. Universal product learning with errors: a new variant of LWE for lattice-based cryptography. *Theoretical Computer Science*, 915 (??):90–100, May 14, 2022. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397522001268.

Yang:2020:AMD

[YHC20] Ta-Wei Yang, Yu-Han Ho, and Cheng-Fu Chou. Achieving M2M-device authentication through heterogeneous information bound with USIM card. *Future Generation Computer Systems*, 110(??):629–637, September 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X19307228.

Yiu:2021:DSC

[Yiu21] Neo C. K. Yiu. Decentralizing supply chain anti-counterfeiting and traceability systems using blockchain technology. *Future Internet*, 13(4):84, March 25, 2021. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/13/4/84.

Yan:2021:RSI

[YLLL21] Xuehu Yan, Lintao Liu, Longlong Li, and Yuliang Lu. Robust secret image sharing resistant to noise in shares. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 17(1):24:1–24:22, April 2021. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL https://dl.acm.org/doi/10.1145/3419750.

Yao:2022:IET

[YLZ+22] Haipeng Yao, Chong Liu, Peiying Zhang, Sheng Wu, Chunxiao Jiang, and Shui Yu. Identification of encrypted traffic through attention mechanism based long short term memory. *IEEE Transactions on Big Data*, 8 (1):241–252, February 2022. CODEN ???? ISSN 2332-7790.

Yan:2021:LSH

[YM21] Xiaobei Yan and Maode Ma. A lightweight and secure handover authentication scheme for 5G network using neighbour base stations. *Journal of Network and Computer Applications*, 193 (??):??, November 1, 2021. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804521002095.

Ying:2022:CNC

[YYH22] Qianjin Ying, Yulei Yu, and Changzhen Hu. CJSpector: A novel cryptojacking detection method using hardware trace and deep learning. *Journal of Grid Computing*, 20(4):??, December 2022. CODEN ???? ISSN 1570-7873 (print), 1572-9184 (electronic). URL https://link.springer.com/article/10.1007/s10723-022-09621-2.

Yuan:2020:EEB

[YYZ+20] X. Yuan, X. Yuan, Y. Zhang, B. Li, and C. Wang. Enabling encrypted Boolean queries in geographically distributed databases. *IEEE Transactions on Parallel and Distributed Systems*, 31(3):634–646, March 2020. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Yuan:2022:IBP

[YZL22] Yilin Yuan, Jianbiao Zhang, and Zheng Li. Identity-based public data integrity verification scheme in cloud storage system via blockchain. *The Journal of Supercomputing*, 78(6):8509–8530, April 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://link.springer.com/article/10.1007/s11227-021-04193-6.

Zakaria:2021:TDM

[Zak21a] La Zakaria. A two-dimensional mKdV linear map and its application in digital image cryptography. *Algorithms (Basel)*, 14(4), April 2021. CODEN ALGOCH. ISSN 1999-4893 (electronic). URL https://www.mdpi.com/1999-4893/14/4/124.

Zhao:2021:EBS

[ZAK+21b] Benjamin Zi Hao Zhao, Hassan Jameel Asghar, Mohamed Ali Kaafar, Francesca Trevisan, and Haiyue Yuan. Exploiting behavioral side channels in observation resilient cognitive authentication schemes. *ACM Transactions on Privacy and Security (TOPS)*, 24(1):1:1–1:33, January 2021. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/doi/10.1145/3414844.

Zaki:2022:GGM

[ZAR+22] Faiz Zaki, Firdaus Afifi, Shukor Abd Razak, Abdullah Gani, and Nor Badrul Anuar. GRAIN: Granular multi-label encrypted traffic classification using classifier chain. *Computer Networks (Amsterdam, Netherlands: 1999)*, 213(??):??, August 4, 2022. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128622002213.

Zijlstra:2022:LBC

[ZBT22] Timo Zijlstra, Karim Bigou, and Arnaud Tisserand. Lattice-based cryptosystems on

FPGA: Parallelization and comparison using HLS. *IEEE Transactions on Computers*, 71(8):1916–1927, August 2022. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Zaidi:2021:TBC

[ZCJ+21] Ahmad Zairi Zaidi, Chun Yong Chong, Zhe Jin, Rajendran Parthiban, and Ali Safaa Sadiq. Touch-based continuous mobile device authentication: State-of-the-art, challenges and opportunities. *Journal of Network and Computer Applications*, 191(??):??, October 1, 2021. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804521001740`.

Zhu:2021:FEE

[ZCLG21] Jinwei Zhu, Kun Cheng, Jiayang Liu, and Liang Guo. Full encryption: an end to end encryption mechanism in GaussDB. *Proceedings of the VLDB Endowment*, 14(12):2811–2814, July 2021. CODEN ???? ISSN 2150-8097. URL `https://dl.acm.org/doi/10.14778/3476311.3476351`.

Zhao:2021:ICA

[ZCWW21] Zishen Zhao, Shiyao Chen, Meiqin Wang, and Wei Wang. Improved cube-attack-like cryptanalysis of reduced-round Ketje-Jr and Keccak-MAC. *Information Processing Letters*, 171(??): Article 106124, October 2021. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019021000387`.

Zhou:2021:FPT

[ZCZ+21] H. Zhou, K. Chen, W. Zhang, C. Qin, and N. Yu. Feature-preserving tensor voting model for mesh steganalysis. *IEEE Transactions on Visualization and Computer Graphics*, 27(1):57–67, 2021. CODEN ITVGEA. ISSN 1077-2626.

Zhang:2020:ABE

[ZDX+20] Yinghui Zhang, Robert H. Deng, Shengmin Xu, Jianfei Sun, Qi Li, and Dong Zheng. Attribute-based encryption for cloud computing access control: a survey. *ACM Computing Surveys*, 53(4): 83:1–83:41, September 2020. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL `https://dl.acm.org/doi/10.1145/3398036`.

Zhao:2020:AAI

[ZGL+20] Zhen Zhao, Fuchun Guo, Jianchang Lai, Willy Susilo, Baocang Wang, and Yupu Hu. Accountable authority identity-based broadcast encryption with constant-size private keys and ciphertexts. *Theoretical Computer Science*, 809(??):73–87, February 24, 2020. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397519307613`.

Zhandry:2021:HCQ

[Zha21] Mark Zhandry. How to construct quantum random functions. *Journal of the ACM*, 68(5):33:1–33:43, October 2021. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `https://dl.acm.org/doi/10.1145/3450745`.

Zhang:2020:EPC

[ZHC+20] F. Zhang, W. He, R. Cheng, J. Kos, N. Hynes, N. Johnson, A. Juels, A. Miller, and D. Song. The Ekiden platform for confidentiality-preserving, trustworthy, and performant smart contracts. *IEEE Security & Privacy*, 18(3):17–27, May/June 2020. ISSN 1558-4046.

Zhou:2021:SHC

[ZHL+21] Zhen Zhou, Debiao He, Zhe Liu, Min Luo, and Kim-Kwang Raymond Choo. A software/hardware co-design of crystals-dilithium signature scheme. *ACM Transactions on Reconfigurable Technology and Systems*, 14(2):11:1–11:21, July 2021. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic). URL `https://dl.acm.org/doi/10.1145/3447812`.

Zhou:2020:HBA

[ZHM20] L. Zhou, Y. Hu, and Y. Makris. A hardware-based architecture-neutral framework for real-time IoT workload forensics. *IEEE Transactions on Computers*, 69(11):1668–1680, November 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Zolotavkin:2022:IUA

[ZJK+22] Yevhen Zolotavkin, Jongkil Jay Jeong, Veronika Kuchta, Maksym Slavnenko, and Robin Doss. Improving unlinkability of attribute-based authentication through game theory. *ACM Transactions on Privacy and Security (TOPS)*, 25(2):12:1–12:36, May 2022. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/10.1145/3501260`.

Zhou:2020:BBT

[ZJZL20] Jia Zhou, Prachi Joshi, Haibo Zeng, and Renfa Li. BTMonitor: Bit-time-based intrusion detection and attacker identification in controller area network. *ACM Transactions on Embedded Computing Systems*, 18(6):1–23, January 2020. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3362034.

Zheng:2021:CRV

[ZKY21] Mengce Zheng, Noboru Kunihiro, and Yuanzhi Yao. Cryptanalysis of the RSA variant based on cubic Pell equation. *Theoretical Computer Science*, 889(??):135–144, October 8, 2021. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S030439752100445X.

Zhong:2020:EDM

[ZLC+20] Hong Zhong, Zhanfei Li, Jie Cui, Yue Sun, and Lu Liu. Efficient dynamic multi-keyword fuzzy search over encrypted cloud data. *Journal of Network and Computer Applications*, 149(??):??, January 1, 2020. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804519303297.

Zhou:2020:PKR

[ZLD+20] Haibo Zhou, Zheng Li, Xiaoyang Dong, Keting Jia, and Willi Meier. Practical key-recovery attacks on round-reduced Ketje Jr, Xoodoo-AE and Xoodyak. *The Computer Journal*, 63(8):1231–1246, August 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/63/8/1231/5709729.

Zhang:2020:FEA

[ZM20] Lyuye Zhang and Maode Ma. FKR: an efficient authentication scheme for IEEE 802.11ah networks. *Computers & Security*, 88(??): Article 101633, January 2020. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167404818313373.

Zhang:2021:QAY

[ZMR21] Lei Zhang, Andriy Miranskyy, and Walid Rjaibi. Quantum advantage and the Y2K bug: a comparison. *IEEE Software*, 38(2):80–87, March/April 2021. CODEN IESOEG. ISSN 0740-7459 (print), 1937-4194 (electronic).

Zilio:2021:FSG

[ZOZ21] Daniel Zilio, Nicola Orio, and Luca Zamparo. FakeMuse: a serious game on authentication for cultural heritage. *Journal on Computing and Cultural Heritage (JOCCH)*, 14(2):17:1–17:22, June 2021. CODEN ????. ISSN 1556-4673 (print), 1556-4711 (electronic). URL https://dl.acm.org/doi/10.1145/3441627.

Zhang:2020:NAE

[ZQY+20] N. Zhang, Q. Qin, H. Yuan, C. Zhou, S. Yin, S. Wei, and L. Liu. NTTU: An area-efficient low-power NTT-uncoupled architecture for NTT-based multiplication. *IEEE Transactions on Computers*, 69(4):520–533, April 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Zhang:2022:CLA

[ZQY+22] Wenzheng Zhang, Zirui Qiao, Bo Yang, Yanwei Zhou, and Mingwu Zhang. Continuous leakage-amplified public-key encryption with CCA security. *The Computer Journal*, 65(7):1760–1775, July 2022. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/65/7/1760/6236091`.

Zhao:2020:FFC

[ZSS20] R. K. Zhao, R. Steinfeld, and A. Sakzad. FACCT: FAst, Compact, and Constant-Time discrete Gaussian sampler over integers. *IEEE Transactions on Computers*, 69(1):126–137, January 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Zhang:2022:VSB

[ZSS+22] Jiliang Zhang, Chaoqun Shen, Haihan Su, Md Tanvir Arafin, and Gang Qu. Voltage over-scaling-based lightweight authentication for IoT security. *IEEE Transactions on Computers*, 71(2):323–336, February 2022. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Zhao:2020:BBA

[ZWG+20] Zhen Zhao, Ge Wu, Fuchun Guo, Willy Susilo, Yi Mu, Baocang Wang, and Yupu Hu. Black-box accountable authority identity-based revocation system. *The Computer Journal*, 63(4):525–535, April 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/63/4/525/5618849`.

Zhong:2020:SDM

[ZWR+20] Sheng-Hua Zhong, Yuantian Wang, Tongwei Ren, Mingjie Zheng, Yan Liu, and Gangshan Wu. Steganographer detection via multi-scale embedding probability estimation. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 15(4):1–23, January 2020. ISSN 1551-6857 (print), 1551-6865 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3352691`.

Zheng:2022:CSE

[ZWT22] Lijuan Zheng, Zihan Wang, and Senping Tian. Comparative study on electrocardiogram encryption using elliptic curves cryptography and data encryption standard for applications in Internet of Medical Things. *Concurrency and Computation: Practice and Experience*, 34 (9):e5776:1–e5776:??, April 25, 2022. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Zhang:2021:DHD

[ZWW+21] Guangxue Zhang, Tian Wang, Guojun Wang, Anfeng Liu, and Weijia Jia. Detection of hidden data attacks combined fog computing and trust evaluation method in sensor-cloud system. *Concurrency and Computation: Practice and Experience*, 33 (7):1, April 10, 2021. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Zhou:2022:OBS

[ZWYL22] Chao Zhou, Chunhua Wang, Wei Yao, and Hairong Lin. Observer-based synchronization of memristive neural networks under DoS attacks and actuator saturation and its application to image encryption. *Applied Mathematics and Computation*, 425(??):??, July 15, 2022. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300322001643.

Zou:2022:NIE

[ZWZ+22] Chengye Zou, Xingyuan Wang, Changjun Zhou, Shujuan Xu, and Chun Huang. A novel image encryption algorithm based on DNA strand exchange and diffusion. *Applied Mathematics and Computation*, 430(??):??, October 1, 2022. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300322003654.

Zhou:2021:CLR

[ZXQ+21] Yanwei Zhou, Yuan Xu, Zirui Qiao, Bo Yang, and Mingwu Zhang. Continuous leakage-resilient certificate-based signcryption scheme and application in cloud computing. *Theoretical Computer Science*, 860(??):1–22, March 8, 2021. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397521000451.

Zhang:2020:STH

[ZXY20] Xiao Zhang, Lijia Xie, and Wang Yao. Spatio-temporal heterogeneous bandwidth allocation mechanism against DDoS attack. *Journal of Network and Computer Applications*, 162(??):??, July 15, 2020. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-

8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804520301326.

Zhang:2020:IIF

[ZY20] Diming Zhang and Shaodi You. iFlask: Isolate flask security system from dangerous execution environment by using ARM TrustZone. *Future Generation Computer Systems*, 109 (??):531–537, August 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X17322239.

Zhang:2021:TES

[ZY21] Hailong Zhang and Wei Yang. Theoretical estimation on the success rate of the asymptotic higher order optimal distinguisher. *The Computer Journal*, 64(8):1277–1292, August 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/64/8/1277/6062487.

Zhu:2022:FSE

[ZYA+22] Fei Zhu, Xun Yi, Alsharif Abuadbba, Ibrahim Khalil, Surya Nepal, and Xinyi Huang. Forward-secure edge authentication for graphs. *The Computer Journal*, 65 (7):1653–1665, July 2022. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/65/7/1653/6178962.

Zhang:2020:SCA

[ZYD+20] F. Zhang, B. Yang, X. Dong, S. Guilley, Z. Liu, W. He, F. Zhang, and K. Ren. Side-channel analysis and countermeasure design on arm-based quantum-resistant SIKE. *IEEE Transactions on Computers*, 69(11):1681–1693, November 2020. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Zhang:2020:DMB

[ZYH+20] Xiang Zhang, Lina Yao, Chaoran Huang, Tao Gu, Zheng Yang, and Yunhao Liu. DeepKey: a multimodal biometric authentication system via deep decoding gaits and brainwaves. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 11(4):49:1–49:24, July 2020. CODEN ???? ISSN 2157-6904 (print), 2157-6912 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3393619.

Zhou:2020:CLR

[ZYW+20] Yanwei Zhou, Bo Yang, Tao Wang, Zhe Xia, and Hongxia Hou. Continuous leakage-resilient certificate-based encryption scheme without bilinear pairings. *The Computer Journal*, 63(4):508–

524, April 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/63/4/508/5614856.

Zhou:2020:IBE

[ZYX+20] Yanwei Zhou, Bo Yang, Zhe Xia, Mingwu Zhang, and Yi Mu. Identity-based encryption with leakage-amplified chosen-ciphertext attacks security. *Theoretical Computer Science*, 809 (??):277–295, February 24, 2020. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397519307935.

Zhang:2021:FEC

[ZZ21a] Zheng Zhang and Fangguo Zhang. Functional encryption for cubic polynomials and implementation. *Theoretical Computer Science*, 885(??):41–54, September 11, 2021. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397521003649.

Zhang:2021:DSS

[ZZ21b] Zhishuo Zhang and Shijie Zhou. A decentralized strongly secure attribute-based encryption and authentication scheme for distributed Internet of mobile things. *Computer Networks (Amsterdam, Netherlands: 1999)*, 201(??):??, December 24, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128621004722.

Zhang:2021:CAL

[ZZC+21] Fangfang Zhang, Xue Zhang, Maoyong Cao, Fengying Ma, and Zhengfeng Li. Characteristic analysis of 2D lag-complex logistic map and its application in image encryption. *IEEE MultiMedia*, 28(4):96–106, October/December 2021. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic).

Zhou:2021:IAR

[ZZD+21] Haibo Zhou, Rui Zong, Xiaoyang Dong, Keting Jia, and Willi Meier. Interpolation attacks on round-reduced Elephant, Kravatte and Xoofff. *The Computer Journal*, 64(4):628–638, April 2021. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/64/4/628/5880072.

Zhang:2022:SHI

[ZZhC22] Xiaomei Zhang, Pengming Zhang, and Chi hung Chi. sAuth: a hierarchical implicit authentication mechanism for service robots.

The Journal of Supercomputing, 78(14):16029–16055, September 2022. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `https://link.springer.com/article/10.1007/s11227-022-04472-w`.

Zhang:2021:PHP

[ZZQ21] Zhishuo Zhang, Wei Zhang, and Zhiguang Qin. A partially hidden policy CP–ABE scheme against attribute values guessing attacks with online privacy-protective decryption testing in IoT assisted cloud computing. *Future Generation Computer Systems*, 123 (??):181–195, October 2021. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X21001436`.

Zhao:2021:DAR

[ZZX^{+}21] Juan Zhao, Tianrui Zong, Yong Xiang, Longxiang Gao, Wanlei Zhou, and Gleb Beliakov. Desynchronization attacks resilient watermarking method based on frequency singular value coefficient modification. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 29(??):2282–2295, 2021. CODEN ???? ISSN 2329-9290.