A Complete Bibliography of Publications in *International Journal of Information Security*

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
FAX: +1 801 581 4148

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

19 May 2020
Version 1.14

Title word cross-reference

(t, n) [QDW09]. 2^w [Bae10]. k [BDD01, MU18, RMSCR19]. n [CC12]. $O(n)$ [DYDW10]. t [BDD01].

-anonymization [MU18, RMSCR19]. **-ary** [Bae10]. **-database** [BDD01]. **-Diffie** [CC12]. **-private** [BDD01].

.NET [KKKV07].

/SSL [BJ16].

1 [KJS17]. **11770** [CH16].

2.0 [AMLH18]. **2002** [ACM05]. **2003** [BM05, Sne05]. **2004** [DSY06]. **2012** [SKK+17]. **2013** [BJ15].

3 [ABM+12]. **3GPP** [EWR+09].

88 [vOLW05].

AAnA [SK14]. **absence** [AvO13]. **absolute** [AvO13]. **abstract** [BLM11, DM07, MS14]. **abstract-based** [BLM11]. **abstraction** [MLCS16]. **abused** [CYA+18]. **Acceptable** [BB04b]. **Access** [Lop18, SAL17, ACF17, ACBC+15, BLM11, CF03, CK08, CZ06, HSMY12, JSMG18a, KAC16, KAC17, Kud02, LD17, LRB+10, MS15, Pen12, PMPGMLLM12, RD16]. **accessibility** [SHA20]. **account** [BRS06]. **accounts** [ASN+16]. **accreditation**

Xen-based [PPL15]. **XML** [BFPP07, CF03, KMR09]. **XOR** [BP08, BGP07b]. **XQuery** [DTK+18]. **XTEA** [Lu09].

Yao [BPW05b, BP08]. **Yao-style** [BPW05b, BP08]. **yoking** [HLS18].

zero [DGF+17, PSDSNAHJ19]. **zero-confirmation** [PSDSNAHJ19]. **zero-day** [DGF+17]. **Zheng** [BZ03]. **ZombieCoin** [AMLH18].

References

Abbadi:2013:FET

[Abb13] Imad M. Abbadi. A framework for establishing trust in cloud provenance. *International Journal of Information Security*, 12(2):111–128, April 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0179-0.

Aliasgari:2017:SCH

[ABB17] Mehrdad Aliasgari, Marina Blanton, and Fattaneh Bayatbabolghani. Secure computation of hidden Markov models and secure floating-point arithmetic in the malicious model. *International Journal of Information Security*, 16(6):577–601, November 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0350-0.

Alfaro:2008:CAC

[ABCC08] J. G. Alfaro, N. Boulahia-Cuppens, and F. Cuppens. Complete analysis of configuration rules to guarantee reliable network security policies. *International Journal of Information Security*, 7(2):103–122, April 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0045-7.

Ates:2012:WHI

[ABFL12] Mikaël Ates, Francesco Buccafurri, Jacques Fayolle, and Gianluca Lax. A warning on how to implement anonymous credential protocols into the information card framework. *International Journal of Information Security*, 11(1):33–40, February 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0150-5.

Aimeur:2008:LPP

[ABFO08] Esma Aïmeur, Gilles Brassard, José M. Fernandez, and Flavien Serge Mani Onana. Alambic: a privacy-preserving recom-

mender system for electronic commerce. *International Journal of Information Security*, 7(5): 307–334, October 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-007-0049-3`.

Andreeva:2012:SAS

[ABM+12] Elena Andreeva, Andrey Bogdanov, Bart Mennink, Bart Preneel, and Christian Rechberger. On security arguments of the second round SHA-3 candidates. *International Journal of Information Security*, 11(2):103–120, April 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-012-0156-7`.

Albeshri:2014:EGI

[ABN14] Aiiad Albeshri, Colin Boyd, and Juan González Nieto. Enhanced GeoProof: improved geographic assurance for data in the cloud. *International Journal of Information Security*, 13 (2):191–198, April 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-013-0217-6`.

Abbes:2016:DFC

[ABR16] Tarek Abbes, Adel Bouhoula, and Michaël Rusinowitch. Detection of firewall configuration errors with updatable tree. *International Journal of Information Security*, 15(3):301–317, June 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-015-0290-0`.

Armando:2008:SBM

[AC08] Alessandro Armando and Luca Compagna. SAT-based model-checking for security protocols analysis. *International Journal of Information Security*, 7(1):3–32, January 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-007-0041-y`.

Alabrah:2014:ESC

[ACB14] Amerah Alabrah, Jeffrey Cashion, and Mostafa Bassiouni. Enhancing security of cookie-based sessions in mobile networks using sparse caching. *International Journal of Information Security*, 13(4): 355–366, August 2014. CODEN ???? ISSN

1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0223-8.

Azkia:2015:DPA

[ACBC+15] Hanieh Azkia, Nora Cuppens-Boulahia, Frédéric Cuppens, Gouenou Coatrieux, and Said Oulmakhzoune. Deployment of a posteriori access control using IHE ATNA. *International Journal of Information Security*, 14(5): 471–483, October 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0265-6.

Albertini:2017:EAC

[ACF17] Davide Alberto Albertini, Barbara Carminati, and Elena Ferrari. An extended access control mechanism exploiting data dependencies. *International Journal of Information Security*, 16(1):75–89, February 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0322-4.

Abe:2013:DTA

[ACHO13] Masayuki Abe, Sherman S. M. Chow, Kristiyan Haralambiev, and Miyako Ohkubo. Double-trapdoor anonymous tags for traceable signatures. *International Journal of Information Security*, 12 (1):19–31, February 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0184-3.

Autexier:2005:PSI

[ACM05] Serge Autexier, Iliano Cervesato, and Heiko Mantel. Preface to the special issue of selected papers from FCS/VERIFY 2002. *International Journal of Information Security*, 4(1–2):1, February 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0053-9; http://link.springer.com/content/pdf/10.1007/s10207-004-0053-9.pdf.

Armando:2015:FMA

[ACMV15] Alessandro Armando, Gabriele Costa, Alessio Merlo, and Luca Verderame. Formal modeling and automatic enforcement of Bring Your Own Device policies. *International Journal of Information Security*, 14(2):123–140, April 2015. CODEN ???? ISSN 1615-5262 (print), 1615-

5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0252-y.

Aldini:2008:EMI

[AD08] Alessandro Aldini and Alessandra Di Pierro. Estimating the maximum information leakage. *International Journal of Information Security*, 7(3): 219–242, June 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0050-x.

Anagnostakis:2007:CDR

[AGIK07] Kostas G. Anagnostakis, Michael B. Greenwald, Sotiris Ioannidis, and Angelos D. Keromytis. COVERAGE: detecting and reacting to worm epidemics using cooperation and validation. *International Journal of Information Security*, 6(6):361–378, October 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0032-z.

Ayed:2018:ADS

[AICC18] Samiha Ayed, Muhammad Sabir Idrees, Nora Cuppens, and Frederic Cuppens. Achieving dynamicity in security policies enforcement using aspects. *International Journal of Information Security*, 17(1): 83–103, February 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0357-6.

An:2009:UIC

[AJC+09] Xiangdong An, Dawn Jutla, Nick Cercone, Charnyote Pluempitiwiriyawej, and Hai Wang. Uncertain inference control in privacy protection. *International Journal of Information Security*, 8(6): 423–431, December 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0088-z.

Anagnostopoulos:2016:NFM

[AKG16] Marios Anagnostopoulos, Georgios Kambourakis, and Stefanos Gritzalis. New facets of mobile botnet: architecture and evaluation. *International Journal of Information Security*, 15(5): 455–473, October 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.

com/article/10.1007/s10207-015-0310-0.

Anada:2020:KUP

[AKMW20] Hiroaki Anada, Akira Kanaoka, Natsume Matsuzaki, and Yohei Watanabe. Key-updatable public-key encryption with keyword search (or: How to realize PEKS with efficient key updates for IoT environments). *International Journal of Information Security*, 19 (1):15–38, February 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00441-2.

Adepu:2020:ASG

[AKZM20] Sridhar Adepu, Nandha Kumar Kandasamy, Jianying Zhou, and Aditya Mathur. Attacks on smart grid: power supply interruption and malicious power generation. *International Journal of Information Security*, 19(2):189–211, April 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00452-z.

Atallah:2005:SOS

[AL05] Mikhail J. Atallah and Jiangtao Li. Secure outsourcing of sequence comparisons. *International Journal of Information Security*, 4(4): 277–287, October 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-005-0070-3.

Alawatugoda:2017:GCM

[Ala17] Janaka Alawatugoda. Generic construction of an eCK-secure key exchange protocol in the standard model. *International Journal of Information Security*, 16 (5):541–557, October 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0346-9.

Arbit:2015:IPK

[ALOW15] Alex Arbit, Yoel Livne, Yossef Oren, and Avishai Wool. Implementing public-key cryptography on passive RFID tags is practical. *International Journal of Information Security*, 14(1):85–99, February 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0236-y.

Asghar:2013:CCH

[ALPW13] Hassan Jameel Asghar,

Shujun Li, Josef Pieprzyk, and Huaxiong Wang. Cryptanalysis of the convex hull click human identification protocol. *International Journal of Information Security*, 12(2):83–96, April 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0161-x.

Ali:2018:ZMN

[AMLH18] Syed Taha Ali, Patrick McCorry, Peter Hyun-Jeen Lee, and Feng Hao. ZombieCoin 2.0: managing next-generation botnets using Bitcoin. *International Journal of Information Security*, 17(4):411–422, August 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0379-8.

Andreeva:2012:PFG

[AMP12] Elena Andreeva, Bart Mennink, and Bart Preneel. The parazoa family: generalizing the sponge hash functions. *International Journal of Information Security*, 11(3):149–165, June 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0157-6.

Arapinis:2017:APM

[AMRR17] Myrto Arapinis, Loretta Ilaria Mancini, Eike Ritter, and Mark Dermot Ryan. Analysis of privacy in mobile telephony systems. *International Journal of Information Security*, 16(5):491–523, October 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0338-9; http://link.springer.com/content/pdf/10.1007/s10207-016-0338-9.pdf.

Anonymous:2011:P

[Ano11a] Anonymous. Preface. *International Journal of Information Security*, 10(2):61, June 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0134-5; http://link.springer.com/content/pdf/10.1007/s10207-011-0134-5.pdf.

Anonymous:2011:SIS

[Ano11b] Anonymous. Special issue on "SCADA and control system security". *International Journal of Information Security*, 10

(2):135–136, June 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0128-3.

Anonymous:2014:SCC

[Ano14] Anonymous. Security in cloud computing. *International Journal of Information Security*, 13(2): 95–96, April 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0232-2.

Ahmed:2012:MGE

[ANS+12] Irfan Ahmed, Martin Naedele, Bradley Schatz, Ryoichi Sasaki, and Andrew West. Message from the guest editors. *International Journal of Information Security*, 11(4): 213, August 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0168-3; http://link.springer.com/content/pdf/10.1007/s10207-012-0168-3.pdf.

Al-Riyami:2006:EFE

[ARMLS06] S. S. Al-Riyami, J. Malone-Lee, and N. P. Smart. Escrow-free encryption supporting cryptographic workflow. *International Journal of Information Security*, 5(4):217–229, October 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-006-0002-x.

Al-Saleh:2015:IDC

[ASAAS15] Mohammed I. Al-Saleh, Fatima M. AbuHjeela, and Ziad A. Al-Sharif. Investigating the detection capabilities of antiviruses under concurrent attacks. *International Journal of Information Security*, 14 (4):387–396, August 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0261-x.

Abie:2004:DDR

[ASF04] Habtamu Abie, Pål Spilling, and Bent Foyn. A distributed digital rights management model for secure information-distribution systems. *International Journal of Information Security*, 3(2):113–128, November 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/

10.1007/s10207-004-0058-4.

Almaatouq:2016:IIL

[ASN+16] Abdullah Almaatouq, Erez Shmueli, Mariam Nouh, Ahmad Alabdulkareem, Vivek K. Singh, Mansour Alsaleh, Abdulrahman Alarifi, Anas Alfaris, and Alex 'Sandy' Pentland. If it looks like a spammer and behaves like a spammer, it must be a spammer: analysis and detection of microblogging spam accounts. *International Journal of Information Security*, 15(5): 475–491, October 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0321-5.

Aufner:2020:ISG

[Auf20] Peter Aufner. The IoT security gap: a look down into the valley between threat models and their implementation. *International Journal of Information Security*, 19 (1):3–14, February 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00445-y; http://link.springer.com/content/pdf/10.1007/s10207-019-00445-y.pdf.

Antunes:2017:DVT

[AV17] Nuno Antunes and Marco Vieira. Designing vulnerability testing tools for web services: approach, components, and tools. *International Journal of Information Security*, 16 (4):435–457, August 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0334-0.

Alsaleh:2013:EAA

[AvO13] Mansour Alsaleh and P. C. van Oorschot. Evaluation in the absence of absolute ground truth: toward reliable evaluation methodology for scan detectors. *International Journal of Information Security*, 12 (2):97–110, April 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0178-1.

Akiyama:2018:HDC

[AYHK18] Mitsuaki Akiyama, Takeshi Yagi, Takeo Hariu, and Youki Kadobayashi. HoneyCirculator: distributing credential honeytoken for introspection of web-based attack cycle.

International Journal of Information Security, 17 (2):135–151, April 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0361-5; http://link.springer.com/content/pdf/10.1007/s10207-017-0361-5.pdf.

Aamir:2019:DAD

[AZ19] Muhammad Aamir and Syed Mustafa Ali Zaidi. DDoS attack detection with feature engineering and machine learning: the framework and performance evaluation. *International Journal of Information Security*, 18(6): 761–785, December 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00434-1.

Blanton:2016:POS

[BA16] Marina Blanton and Everaldo Aguiar. Private and oblivious set and multiset operations. *International Journal of Information Security*, 15(5): 493–518, October 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0301-1.

Baek:2010:RAR

[Bae10] Yoo-Jin Baek. Regular 2^w-ary right-to-left exponentiation algorithm with very efficient DPA and FA countermeasures. *International Journal of Information Security*, 9(5): 363–370, October 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-010-0118-x.

Biskup:2004:CQE

[BB04a] Joachim Biskup and Piero Bonatti. Controlled query evaluation for enforcing confidentiality in complete information systems. *International Journal of Information Security*, 3 (1):14–27, October 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0032-1.

Blakley:2004:ASN

[BB04b] B. Blakley and G. R. Blakley. All sail, no anchor II: Acceptable high-end PKI. *International Journal of Information Security*, 2(2):66–77, January 2004. CODEN ???? ISSN 1615-5262 (print), 1615-

5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-003-0029-1.

BenAttia:2020:UHT

[BBB20] Hasiba Ben Attia, Laid Kahloul Saber Benharzallah, and Samir Bourekkache. Using hierarchical timed coloured Petri nets in the formal study of TRBAC security policies. *International Journal of Information Security*, 19 (2):163–187, April 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00448-9. See author name correction [BKBB20].

Bindel:2018:CAA

[BBR18] Nina Bindel, Johannes Buchmann, and Susanne Rieß. Comparing apples with apples: performance analysis of lattice-based authenticated key exchange protocols. *International Journal of Information Security*, 17(6): 701–718, November 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0397-6.

Bayly:2010:FBS

[BCA+10] Duncan Bayly, Maurice Castro, Arathi Arakala, Jason Jeffers, and Kathy Horadam. Fractional biometrics: safeguarding privacy in biometric applications. *International Journal of Information Security*, 9(1):69–82, February 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0096-z.

Bresson:2013:LLS

[BCD+13] Emmanuel Bresson, Dario Catalano, Mario Di Raimondo, Dario Fiore, and Rosario Gennaro. Offline/on-line signatures revisited: a general unifying paradigm, efficient threshold variants and experimental results. *International Journal of Information Security*, 12(6): 439–465, November 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0200-2.

Burgess:2004:GTM

[BCEM04] Mark Burgess, Geoffrey Canright, and Kenth Engø-Monsen. A graph-theoretical model of computer security. *International Journal of Information Security*, 3(2):70–85, November 2004. CODEN ???? ISSN

1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0044-x.

Boyd:2017:AAK

[BCF+17] Colin Boyd, Cas Cremers, Michèle Feltz, Kenneth G. Paterson, Bertram Poettering, and Douglas Stebila. ASICS: authenticated key exchange security incorporating certification systems. *International Journal of Information Security*, 16 (2):151–171, April 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0312-y.

Backes:2011:CSS

[BCJ+11] Michael Backes, Iliano Cervesato, Aaron D. Jaggard, Andre Scedrov, and Joe-Kai Tsay. Cryptographically sound security proofs for basic and public-key Kerberos. *International Journal of Information Security*, 10 (2):107–134, June 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0125-6.

Brickell:2009:SSN

[BCL09] Ernie Brickell, Liqun Chen, and Jiangtao Li. Simplified security notions of direct anonymous attestation and a concrete scheme from pairings. *International Journal of Information Security*, 8(5): 315–330, October 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0076-3.

Beauquier:2013:SPE

[BCL13] Danièle Beauquier, Joëlle Cohen, and Ruggero Lanotte. Security policies enforcement using finite and pushdown edit automata. *International Journal of Information Security*, 12 (4):319–336, August 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0195-8.

Blundo:2001:PDI

[BDD01] Carlo Blundo, Paolo D'Arco, and Alfredo De Santis. A t-private k-database information retrieval scheme. *International Journal of Information Security*, 1 (1):64–68, August 2001. CODEN ???? ISSN 1615-5262 (print), 1615-

5270 (electronic). URL http://link.springer.com/article/10.1007/s102070100005.

Bartoletti:2004:SIS

[BDF04] Massimo Bartoletti, Pierpaolo Degano, and Gian Luigi Ferrari. Stack inspection and secure program transformations. *International Journal of Information Security*, 2(3–4):187–217, August 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0038-8.

Buhan:2010:ERC

[BDH+10] Ileana Buhan, Jeroen Doumen, Pieter Hartel, Qian Tang, and Raymond Veldhuis. Embedding renewable cryptographic keys into noisy data. *International Journal of Information Security*, 9(3):193–208, June 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-010-0103-4.

Backes:2008:CRS

[BDHK08] Michael Backes, Markus Dürmuth, Dennis Hofheinz, and Ralf Küsters. Conditional reactive simulatability. *International Journal of Information Security*, 7(2):155–169, April 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0046-6.

Bertino:2015:SPE

[BDHZ15] Elisa Bertino, Robert H. Deng, Xinyi Huang, and Jianying Zhou. Security and privacy of electronic health information systems. *International Journal of Information Security*, 14(6):485–486, November 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0303-z; http://link.springer.com/content/pdf/10.1007/s10207-015-0303-z.pdf.

Bernardi:2019:DMD

[BDMM19] Mario Luca Bernardi, Marta Cimitile Damiano Distante, Fabio Martinelli, and Francesco Mercaldo. Dynamic malware detection and phylogeny analysis using process mining. *International Journal of Information Security*, 18(3):257–284, June 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.

com/article/10.1007/s10207-018-0415-3.

Bertoni:2014:SCS

[BDPV14] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Sufficient conditions for sound tree and sequential hashing modes. *International Journal of Information Security*, 13(4):335–353, August 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0220-y.

Bella:2010:PGA

[Bel10] Giampaolo Bella. The principle of guarantee availability for security protocol analysis. *International Journal of Information Security*, 9(2):83–97, April 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0097-y.

Bat-Erdene:2017:EAC

[BEPL+17] Munkhbayar Bat-Erdene, Hyundo Park, Hongzhe Li, Heejo Lee, and Mahn-Soo Choi. Entropy analysis to classify unknown packing algorithms for malware detection. *International Journal of Information Security*, 16(3):227–248, June 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0330-4.

Boteanu:2013:CSQ

[BF13] Daniel Boteanu and José M. Fernandez. A comprehensive study of queue management as a DoS counter-measure. *International Journal of Information Security*, 12(5):347–382, October 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0197-6.

Bernhard:2013:AAU

[BFG+13] D. Bernhard, G. Fuchsbauer, E. Ghadafi, N. P. Smart, and B. Warinschi. Anonymous attestation with user-controlled linkability. *International Journal of Information Security*, 12(3):219–249, June 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0191-z.

Bertino:2003:CBF

[BFP03] Elisa Bertino, Elena Ferrari, and Andrea Perego. Content-based filtering of Web documents: the MaX

system and the EUFORBIA project. *International Journal of Information Security*, 2(1): 45–58, November 2003. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-003-0024-6.

Bertino:2007:SSP

[BFPP07] Elisa Bertino, Elena Ferrari, Federica Paci, and Loredana Parasiliti Provenza. A system for securing push-based distribution of XML documents. *International Journal of Information Security*, 6(4):255–284, July 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0020-3.

Brzuska:2013:LMR

[BFS+13] C. Brzuska, M. Fischlin, N. P. Smart, B. Warinschi, and S. C. Williams. Less is more: relaxed yet composable security notions for key exchange. *International Journal of Information Security*, 12 (4):267–297, August 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0192-y.

Bracciali:2008:SFM

[BFT08] Andrea Bracciali, Gianluigi Ferrari, and Emilio Tuosto. A symbolic framework for multi-faceted security protocol analysis. *International Journal of Information Security*, 7 (1):55–84, January 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0043-9.

Balopoulos:2008:SIP

[BGK08] Theodoros Balopoulos, Stefanos Gritzalis, and Sokratis K. Katsikas. Specifying and implementing privacy-preserving cryptographic protocols. *International Journal of Information Security*, 7(6): 395–420, November 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-008-0057-y.

Bagheri:2012:SFP

[BGKZ12] Nasour Bagheri, Praveen Gauravaram, Lars R. Knudsen, and Erik Zenner. The suffix-free-prefix-free hash function construction and its indifferentiability security analysis. *International Journal of Information Security*,

11(6):419–434, November 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0175-4.

Backes:2007:P

[BGP07a] Michael Backes, Stefanos Gritzalis, and Bart Preneel. Preface. *International Journal of Information Security*, 6(6):359–360, October 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0034-x.

Blundo:2007:LRC

[BGP07b] Carlo Blundo, Clemente Galdi, and Giuseppe Persiano. Low-randomness constant-round private XOR computations. *International Journal of Information Security*, 6(1):15–26, January 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-006-0007-5.

Ben-Ghorbel-Talbi:2010:DME

[BGTCCBB10] Meriam Ben-Ghorbel-Talbi, Frédéric Cuppens, Nora Cuppens-Boulahia, and Adel Bouhoula. A delegation model for extended RBAC. *International Journal of Information Security*, 9(3):209–236, June 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-010-0104-3.

Bella:2015:SIS

[BJ15] Giampaolo Bella and Helge Janicke. Special issue on the Security Track at the ACM Symposium on Applied Computing 2013. *International Journal of Information Security*, 14(2):101–102, April 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0280-2; http://link.springer.com/content/pdf/10.1007/s10207-015-0280-2.pdf.

Brown:2016:API

[BJ16] Christopher W. Brown and Michael Jenkins. Analyzing proposals for improving authentication on the TLS-/SSL-protected Web. *International Journal of Information Security*, 15(6):621–635, November 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0316-2.

BenAttia:2020:CUH

[BKBB20] Hasiba Ben Attia, Laid Kahloul, Saber Benharzallah, and Samir Bourekkache. Correction to: Using Hierarchical Timed Coloured Petri Nets in the formal study of TRBAC security policies. *International Journal of Information Security*, 19(2):241, April 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00454-x; http://link.springer.com/content/pdf/10.1007/s10207-019-00454-x.pdf. See [BBB20].

Bryans:2008:OGT

[BKMR08] Jeremy W. Bryans, Maciej Koutny, Laurent Mazaré, and Peter Y. A. Ryan. Opacity generalised to transition systems. *International Journal of Information Security*, 7(6): 421–435, November 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-008-0058-x.

Bouzida:2011:CAB

[BLM11] Yacine Bouzida, Luigi Logrippo, and Serge Mankovski. Concrete- and abstract-based access control. *International Journal of Information Security*, 10(4): 223–238, August 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0138-1.

Boyd:2005:PSI

[BM05] Colin Boyd and Wenbo Mao. Preface to the special issue on ISC 2003. *International Journal of Information Security*, 4 (4):227, October 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0066-4.

Bielova:2011:DYR

[BM11] Nataliia Bielova and Fabio Massacci. Do you really mean what you actually enforced? *International Journal of Information Security*, 10(4): 239–254, August 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0137-2.

Bella:2005:OVS

[BMP05] Giampaolo Bella, Fabio Massacci, and Lawrence C. Paulson. An overview of the verification of SET. *International Journal of In-*

formation Security, 4(1–2):17–28, February 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0047-7.

Bates:2014:DCR

[BMP+14] Adam Bates, Benjamin Mood, Joe Pletcher, Hannah Pruse, Masoud Valafar, and Kevin Butler. On detecting co-resident cloud instances using network flow watermarking techniques. *International Journal of Information Security*, 13(2):171–189, April 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0210-0.

Basin:2005:OSM

[BMV05] David Basin, Sebastian Mödersheim, and Luca Viganò. OFMC: A symbolic model checker for security protocols. *International Journal of Information Security*, 4(3):181–208, June 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0055-7.

Buchholtz:2004:CCF

[BNN04] Mikael Buchholtz, Hanne Riis Nielson, and Flemming Nielson. A calculus for control flow analysis of security protocols. *International Journal of Information Security*, 2(3–4):145–167, August 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0036-x.

Bogdanov:2012:HPS

[BNTW12] Dan Bogdanov, Margus Niitsoo, Tomas Toft, and Jan Willemson. High-performance secure multiparty computation for data mining applications. *International Journal of Information Security*, 11(6):403–418, November 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0177-2.

Backes:2004:CPN

[BP04] Michael Backes and Birgit Pfitzmann. Computational probabilistic noninterference. *International Journal of Information Security*, 3(1):42–60, October 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0039-7.

Backes:2008:LBU

[BP08] Michael Backes and Birgit Pfitzmann. Limits of the BRSIM/UC soundness of Dolev–Yao-style XOR. *International Journal of Information Security*, 7(1):33–54, January 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-007-0040-z`.

Backes:2005:RSS

[BPW05a] Michael Backes, Birgit Pfitzmann, and Michael Waidner. Reactively secure signature schemes. *International Journal of Information Security*, 4(4):242–252, October 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-004-0062-8`.

Backes:2005:SAS

[BPW05b] Michael Backes, Birgit Pfitzmann, and Michael Waidner. Symmetric authentication in a simulatable Dolev–Yao-style cryptographic library. *International Journal of Information Security*, 4(3):135–154, June 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-004-0056-6`.

Bernardini:2017:MRP

[BR17] Riccardo Bernardini and Roberto Rinaldo. Making random permutations from physically unclonable constants. *International Journal of Information Security*, 16(3):249–261, June 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-016-0324-2`.

Bernardini:2018:GES

[BR18] Riccardo Bernardini and Roberto Rinaldo. Generalized Elias schemes for efficient harvesting of truly random bits. *International Journal of Information Security*, 17(1):67–81, February 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-016-0358-5`.

Brandt:2006:HOF

[Bra06] Felix Brandt. How to obtain full privacy in auctions. *International Journal of Information Security*, 5(4):201–216, October 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL

http://link.springer.com/article/10.1007/s10207-006-0001-y.

Bohli:2006:KSA

[BRS06] Jens-Matthias Bohli, Stefan Röhrich, and Rainer Steinwandt. Key substitution attacks revisited: Taking into account malicious signers. *International Journal of Information Security*, 5(1):30–36, January 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-005-0071-2.

Baldwin:2005:ESA

[BS05] Adrian Baldwin and Simon Shiu. Enabling shared audit data. *International Journal of Information Security*, 4(4):263–276, October 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0061-9.

Baumgarten:2011:CSH

[BSCZ11] Alex Baumgarten, Michael Steffen, Matthew Clausman, and Joseph Zambreno. A case study in hardware Trojan design and implementation. *International Journal of Information Security*, 10(1):1–14, February 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-010-0115-0.

Bao:2020:LSP

[BSK+20] Zijian Bao, Wenbo Shi, Saru Kumari, Zhi yin Kong, and Chien-Ming Chen. Lockmix: a secure and privacy-preserving mix service for Bitcoin anonymity. *International Journal of Information Security*, 19(3):311–321, June 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00459-6.

Bononi:2007:IDS

[BT07] Luciano Bononi and Carlo Tacconi. Intrusion detection for secure clustering and routing in Mobile Multi-hop Wireless Networks. *International Journal of Information Security*, 6(6):379–392, October 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0035-9.

Bohli:2007:SGK

[BVS07] Jens-Matthias Bohli, María Isabel González Vasco, and Rainer Steinwandt. Secure

group key establishment revisited. *International Journal of Information Security*, 6(4):243–254, July 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0018-x.

Biskup:2008:KSI

[BW08] Joachim Biskup and Torben Weibert. Keeping secrets in incomplete databases. *International Journal of Information Security*, 7(3):199–217, June 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0037-7.

Baek:2003:ZSP

[BZ03] Joonsang Baek and Yuliang Zheng. Zheng and Seberry's public key encryption scheme revisited. *International Journal of Information Security*, 2(1):37–44, November 2003. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-003-0023-7.

Yehuda:2020:PAR

[BZ20] Raz Ben Yehuda and Nezer Jacob Zaidenberg. Protection against reverse engineering in ARM. *International Journal of Information Security*, 19(1):39–51, February 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00450-1.

Bai:2005:SAP

[BZV05] Yun Bai, Yan Zhang, and Vijay Varadharajan. On the sequence of authorization policy transformations. *International Journal of Information Security*, 4(1–2):120–131, February 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0069-1.

Chikha:2016:BBA

[CACB16] Randa Jabeur Ben Chikha, Tarek Abbes, Wassim Ben Chikha, and Adel Bouhoula. Behavior-based approach to detect spam over IP telephony attacks. *International Journal of Information Security*, 15(2):131–143, April 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0281-1.

Corbett:2008:PCW

[CBC08] Cherita L. Corbett, Raheem A. Beyah, and John A. Copeland. Passive classification of wireless NICs during active scanning. *International Journal of Information Security*, 7(5):335–348, October 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-007-0053-7`.

Cheng:2020:SAA

[CBRY20] Peng Cheng, Ibrahim Ethem Bagci, Utz Roedig, and Jeff Yan. SonarSnoop: active acoustic side-channel attacks. *International Journal of Information Security*, 19(2):213–228, April 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-019-00449-8; http://link.springer.com/content/pdf/10.1007/s10207-019-00449-8.pdf`.

Chen:2010:HSS

[CC10] Haiyong Chen and Hailiang Chen. A hybrid scheme for securing fingerprint templates. *International Journal of Information Security*, 9(5):353–361, October 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-010-0114-1`.

Chen:2012:DHP

[CC12] Liqun Chen and Yu Chen. The n-Diffie–Hellman problem and multiple-key encryption. *International Journal of Information Security*, 11(5):305–320, October 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-012-0171-8`.

Cuppens:2008:MCS

[CCB08] Frédéric Cuppens and Nora Cuppens-Boulahia. Modeling contextual security policies. *International Journal of Information Security*, 7(4):285–305, August 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-007-0051-9`.

Cederquist:2007:ABC

[CCD+07] J. G. Cederquist, R. Corin, M. A. C. Dekker, S. Etalle, J. I. den Hartog, and G. Lenzini. Audit-based compliance control. *International Journal of Information Security*, 6(2–3):133–151, March 2007.

CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0017-y.

Chen:2007:IBK

[CCS07] L. Chen, Z. Cheng, and N. P. Smart. Identity-based key agreement protocols from pairings. *International Journal of Information Security*, 6(4): 213–241, July 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-006-0011-9.

Catalano:2013:FNI

[CDF+13] Dario Catalano, Mario Di Raimondo, Dario Fiore, Rosario Gennaro, and Orazio Puglisi. Fully non-interactive onion routing with forward secrecy. *International Journal of Information Security*, 12 (1):33–47, February 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0185-2.

Carminati:2003:MAC

[CF03] Barbara Carminati and Elena Ferrari. Management of access control policies for XML document sources. *International Journal of Information Security*, 1(4):236–260, July 2003. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-003-0020-x.

Clarke:2007:AMP

[CF07] N. L. Clarke and S. M. Furnell. Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security*, 6 (1):1–14, January 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-006-0006-6.

Chiasson:2009:UID

[CFBvO09] Sonia Chiasson, Alain Forget, Robert Biddle, and P. C. van Oorschot. User interface design affects security: patterns in click-based graphical passwords. *International Journal of Information Security*, 8(6): 387–398, December 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0080-7.

Catalano:2017:CAO

[CFG17] Dario Catalano, Dario Fiore, and Rosario Gennaro. A certificateless approach to onion routing. *International Journal of Information Security*, 16(3):327–343, June 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-016-0337-x`.

Catuogno:2014:ATF

[CG14] Luigi Catuogno and Clemente Galdi. Analysis of a two-factor graphical password scheme. *International Journal of Information Security*, 13(5):421–437, October 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-014-0228-y`.

Coker:2011:PRA

[CGL+11] George Coker, Joshua Guttman, Peter Loscocco, Amy Herzog, Jonathan Millen, Brian O'Hanlon, John Ramsdell, Ariel Segall, Justin Sheehy, and Brian Sniffen. Principles of remote attestation. *International Journal of Information Security*, 10(2):63–81, June 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-011-0124-7`.

Cremers:2016:III

[CH16] Cas Cremers and Marko Horvat. Improving the ISO/IEC 11770 standard for key management techniques. *International Journal of Information Security*, 15(6):659–673, November 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-015-0306-9; http://link.springer.com/content/pdf/10.1007/s10207-015-0306-9.pdf`.

Camacho:2012:SAC

[CHKO12] Philippe Camacho, Alejandro Hevia, Marcos Kiwi, and Roberto Opazo. Strong accumulators from collision-resistant hashing. *International Journal of Information Security*, 11 (5):349–363, October 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-012-0169-2`.

Chen:2018:MGE

[CHM18] Liqun Chen, Jinguang Han, and Chris Mitchell.

Message from the Guest Editors. *International Journal of Information Security*, 17(5):491–492, October 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0416-2.

Chen:2016:SOK

[CHZ16] Yu Chen, Qiong Huang, and Zongyang Zhang. Sakai–Ohgishi–Kasahara identity-based non-interactive key exchange revisited and more. *International Journal of Information Security*, 15(1):15–33, February 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0274-0.

Chang:2019:CTM

[CJMS19] Donghoon Chang, Arpan Jati, Sweta Mishra, and Somitra Kumar Sanadhya. Cryptanalytic time-memory trade-off for password hashing schemes. *International Journal of Information Security*, 18 (2):163–180, April 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0405-5.

Crampton:2008:DRB

[CK08] Jason Crampton and Hemanth Khambhammettu. Delegation in role-based access control. *International Journal of Information Security*, 7(2):123–136, April 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0044-8.

Cai:2019:STP

[CKW19] Yixian Cai, George Karakostas, and Alan Wassyng. Secure and trusted partial grey-box verification. *International Journal of Information Security*, 18(6): 677–700, December 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00431-4.

Chen:2008:IID

[CL08] Pei-Te Chen and Chi-Sung Laih. IDSIC: an intrusion detection system with identification capability. *International Journal of Information Security*, 7(3):185–197, June 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.

com/article/10.1007/s10207-007-0024-z.

Cheng:2009:CKA

[CL09] Jiin-Chiou Cheng and Chi-Sung Laih. Conference key agreement protocol with non-interactive fault-tolerance over broadcast network. *International Journal of Information Security*, 8(1):37–48, February 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-008-0062-1.

Chen:2013:AMA

[CL13] Yu-Shian Chen and Chin-Laung Lei. Aggregate message authentication codes (AMACs) with on-the-fly verification. *International Journal of Information Security*, 12(6):495–504, November 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0202-0.

Crampton:2011:UFC

[CLPP11] Jason Crampton, Hoon Wei Lim, Kenneth G. Paterson, and Geraint Price. User-friendly and certificate-free grid security infrastructure. *International Journal of Information Security*, 10(3):137–153, June 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0123-8.

Chang:2011:EHS

[CLW+11] Ee-Chien Chang, Liming Lu, Yongzheng Wu, Roland H. C. Yap, and Jie Yu. Enhancing host security using external environment sensors. *International Journal of Information Security*, 10(5):285–299, October 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0130-9.

Chen:2016:MGE

[CM16] Liqun Chen and Chris Mitchell. Message from the guest editors. *International Journal of Information Security*, 15(6):573–574, November 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0353-x.

Casassa-Mont:2015:TSI

[CMMPS15] Marco Casassa-Mont, Ilaria Matteucci, Marinella Petrocchi, and Marco Luca Sbodio. Towards safer information sharing in the

cloud. *International Journal of Information Security*, 14(4):319–334, August 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0258-5.

[CMS10]

Cimitile:2018:TNM

[CMN+18] Aniello Cimitile, Francesco Mercaldo, Vittoria Nardone, Antonella Santone, and Corrado Aaron Visaggio. Talos: no more ransomware victims with formal methods. *International Journal of Information Security*, 17(6):719–738, November 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0398-5.

Chakrabarti:2006:KPD

[CMR06] Dibyendu Chakrabarti, Subhamoy Maitra, and Bimal Roy. A key predistribution scheme for wireless sensor networks: merging blocks in combinatorial design. *International Journal of Information Security*, 5(2):105–114, April 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-006-0085-4.

[CON09]

Chakraborty:2010:CDB

Anindya Chakraborty, Arun K. Majumdar, and Shamik Sural. A column dependency-based approach for static and dynamic recovery of databases from malicious transactions. *International Journal of Information Security*, 9(1):51–67, February 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0095-0.

Chadwick:2009:ASX

David W. Chadwick, Sassa Otenko, and Tuan Anh Nguyen. Adding support to XACML for multi-domain user to user dynamic delegation of authority. *International Journal of Information Security*, 8(2):137–152, April 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-008-0073-y.

[CPPK15]

Chakravarty:2015:DAE

Sambuddho Chakravarty, Georgios Portokalidis, Michalis Polychronakis, and Angelos D. Keromytis. Detection and analysis of eavesdropping in anonymous communication net-

works. *International Journal of Information Security*, 14(3):205–220, June 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-014-0256-7`.

Celdran:2016:RPP

[CTM+16] Alberto Huertas Celdrán, Ginés Dólera Tormo, Félix Gómez Mármol, Manuel Gil Pérez, and Gregorio Martínez Pérez. Resolving privacy-preserving relationships over outsourced encrypted data storages. *International Journal of Information Security*, 15 (2):195–209, April 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-015-0283-z`.

Chiba:2018:DTA

[CYA+18] Daiki Chiba, Takeshi Yagi, Mitsuaki Akiyama, Toshiki Shibahara, Tatsuya Mori, and Shigeki Goto. DomainProfiler: toward accurate and early discovery of domain names abused in future. *International Journal of Information Security*, 17(6):661–680, November 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-017-0396-7; http://link.springer.com/content/pdf/10.1007/s10207-017-0396-7.pdf`.

Cook:2009:EBC

[CYK09] Debra L. Cook, Moti Yung, and Angelos D. Keromytis. Elastic block ciphers: method, security and instantiations. *International Journal of Information Security*, 8 (3):211–231, June 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-008-0075-9`.

Crescini:2006:PSD

[CZ06] Vino Fernando Crescini and Yan Zhang. PolicyUpdater: a system for dynamic access control. *International Journal of Information Security*, 5 (3):145–165, July 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-005-0078-8`.

deAlbuquerque:2010:FVA

[dAKdG10] João Porto de Albuquerque, Heiko Krumm, and Paulo Lício de Geus. Formal validation of automated policy refinement in the management of

network security systems. *International Journal of Information Security*, 9 (2):99–125, April 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-010-0101-6.

Danezis:2007:BFM

[Dan07] George Danezis. Breaking four mix-related schemes based on Universal Re-encryption. *International Journal of Information Security*, 6(6): 393–402, October 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0033-y.

Das:2012:RKE

[Das12] Ashok Kumar Das. A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks. *International Journal of Information Security*, 11 (3):189–211, June 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0162-9.

Dawson:2004:PSI

[Daw04] E. Dawson. Preface to the special issue on PKI. *International Journal of Information Security*, 2(2):65, January 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-003-0031-7; http://link.springer.com/content/pdf/10.1007/s10207-003-0031-7.pdf.

Dupasquier:2010:AIL

[DBMS10] Benoît Dupasquier, Stefan Burschka, Kieran McLaughlin, and Sakir Sezer. Analysis of information leakage from encrypted Skype conversations. *International Journal of Information Security*, 9(5):313–325, October 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-010-0111-4.

DArco:2013:TTR

[DdP13] Paolo D'Arco and Angel Perez del Pozo. Toward tracing and revoking schemes secure against collusion and any form of secret information leakage. *International Journal of Information Security*, 12(1):1–17, February 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL

http://link.springer.com/article/10.1007/s10207-012-0186-1.

Damiani:2002:SSS

[DDPS02] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati. Securing SOAP e-services. *International Journal of Information Security*, 1(2): 100–115, February 2002. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s102070100009.

Dyer:2019:PHE

[DDX19] James Dyer, Martin Dyer, and Jie Xu. Practical homomorphic encryption over the integers for secure computation in the cloud. *International Journal of Information Security*, 18(5): 549–579, October 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00427-0.

Dent:2008:SCE

[Den08] Alexander W. Dent. A survey of certificateless encryption schemes and security models. *International Journal of Information Security*, 7(5): 349–377, October 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-008-0055-0.

Desoky:2009:LLB

[Des09] Abdelrahman Desoky. Listega: list-based steganography methodology. *International Journal of Information Security*, 8(4): 247–261, August 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0079-0.

Domingo-Ferrer:2018:DGS

[DFBJR18] Josep Domingo-Ferrer, Alberto Blanco-Justicia, and Carla Ràfols. Dynamic group size accreditation and group discounts preserving anonymity. *International Journal of Information Security*, 17 (3):243–260, June 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0368-y.

Degabriele:2016:UPC

[DFF+16] Jean Paul Degabriele, Victoria Fehr, Marc Fischlin, Tommaso Gagliardoni, Felix Günther, Giorgia Azzurra Marson, Arno Mittelbach, and Kenneth G. Pa-

terson. Unpicking PLAID: a cryptographic analysis of an ISO-standards-track authentication protocol. *International Journal of Information Security*, 15(6): 637–657, November 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-015-0309-6`.

Duessel:2017:DZD

[DGF+17] Patrick Duessel, Christian Gehl, Ulrich Flegel, Sven Dietrich, and Michael Meier. Detecting zero-day attacks using context-aware anomaly detection at the application-layer. *International Journal of Information Security*, 16(5): 475–490, October 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-016-0344-y`.

Draper-Gil:2013:OFE

[DGZFGH13] G. Draper-Gil, J. Zhou, J. L. Ferrer-Gomila, and M. F. Hinarejos. An optimistic fair exchange protocol with active intermediaries. *International Journal of Information Security*, 12(4):299–318, August 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-013-0194-9`.

Daza:2004:PUI

[DHS04] Vanesa Daza, Javier Herranz, and Germán Sáez. Protocols useful on the Internet from distributed signature schemes. *International Journal of Information Security*, 3(2): 61–69, November 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-004-0043-y`.

DiPierro:2011:PTC

[DHW11] Alessandra Di Pierro, Chris Hankin, and Herbert Wiklicky. Probabilistic timing covert channels: to close or not to close? *International Journal of Information Security*, 10(2):83–106, June 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-010-0107-0`.

Damgaard:2010:GPP

[DJN10] Ivan Damgård, Mads Jurik, and Jesper Buus Nielsen. A generalization of Paillier's public-key system with applications to electronic voting. *International Journal of In-*

formation Security, 9(6): 371–385, December 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-010-0119-9.

Dolzhenko:2015:MRE

[DLR15] Egor Dolzhenko, Jay Ligatti, and Srikar Reddy. Modeling runtime enforcement with mandatory results automata. *International Journal of Information Security*, 14 (1):47–60, February 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0239-8.

DeFrancesco:2007:ILS

[DM07] Nicoletta De Francesco and Luca Martini. Instruction-level security typing by abstract interpretation. *International Journal of Information Security*, 6(2–3):85–106, March 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0015-0.

DeKeulenaer:2016:LTS

[DMDD16] Ronald De Keulenaer, Jonas Maebe, Koen De Bosschere, and Bjorn De Sutter. Link-time smart card code hardening. *International Journal of Information Security*, 15 (2):111–130, April 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0282-0.

DeCristofaro:2013:PDC

[DMP13] Emiliano De Cristofaro, Mark Manulis, and Bertram Poettering. Private discovery of common social contacts. *International Journal of Information Security*, 12(1):49–65, February 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0183-4.

Dimitrakos:2007:GEP

[DMRS07] Theo Dimitrakos, Fabio Martinelli, Peter Y. A. Ryan, and Steve Schneider. Guest Editors' preface. *International Journal of Information Security*, 6(2–3):65–66, March 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0012-3.

Dasgupta:2019:DIN

[DNF+19] Dipankar Dasgupta, Ab-

hijit Kumar Nag, Denise Ferebee, Sanjib Kumar Saha, Kul Prasad Subedi, Arunava Roy, Alvaro Madero, Abel Sanchez, and John R. Williams. Design and implementation of Negative Authentication System. *International Journal of Information Security*, 18 (1):23–48, February 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-017-0395-8`.

Dewri:2012:OSH

[DRPW12] Rinku Dewri, Indrajit Ray, Nayot Poolsappasit, and Darrell Whitley. Optimal security hardening on attack tree models of networks: a cost-benefit analysis. *International Journal of Information Security*, 11(3):167–188, June 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-012-0160-y`.

Delicata:2007:AAV

[DS07] Rob Delicata and Steve Schneider. An algebraic approach to the verification of a class of Diffie–Hellman protocols. *International Journal of Information Security*, 6(2–3):183–196, March 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-007-0013-2`.

Das:2019:DSI

[DSB19] Debasish Das, Utpal Sharma, and D. K. Bhattacharyya. Defeating SQL injection attack in authentication security: an experimental study. *International Journal of Information Security*, 18(1):1–22, February 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-017-0393-x`.

Faria:2019:DAA

[dSFK19] Gerson de Souza Faria and Hae Yong Kim. Differential audio analysis: a new side-channel attack on PIN pads. *International Journal of Information Security*, 18(1):73–84, February 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-018-0403-7`.

Diaz-Santiago:2016:CST

[DSRHC16] Sandra Díaz-Santiago, Lil María Rodríguez-Henríquez, and Debrup Chakraborty. A cryptographic study of to-

kenization systems. *International Journal of Information Security*, 15(4): 413–432, August 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0313-x.

Ding:2006:CNT

[DSY06] Jintai Ding, Dieter Schmidt, and Zhijun Yin. Cryptanalysis of the new TTS scheme in CHES 2004. *International Journal of Information Security*, 5(4): 231–240, October 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-006-0003-9.

Deepa:2018:BBD

[DTK+18] G. Deepa, P. Santhi Thilagam, Furqan Ahmed Khan, Amit Praseed, Alwyn R. Pais, and Nushafreen Palsetia. Black-box detection of XQuery injection and parameter tampering vulnerabilities in web applications. *International Journal of Information Security*, 17(1): 105–120, February 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0359-4.

Degano:2008:P

[DV08] Pierpaolo Degano and Luca Viganò. Preface. *International Journal of Information Security*, 7(1): 1, January 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0038-6.

Dawson:2002:CCP

[DVB02] Ed Dawson, Kapali Viswanathan, and Colin Boyd. Compliant cryptologic protocols. *International Journal of Information Security*, 1(3): 189–202, November 2002. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-002-0016-y.

Ding:2010:NHA

[DYDW10] Xuhua Ding, Yanjiang Yang, Robert H. Deng, and Shuhong Wang. A new hardware-assisted PIR with $O(n)$ shuffle cost. *International Journal of Information Security*, 9 (4):237–252, August 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.

com/article/10.1007/s10207-010-0105-2.

Deng:2018:SPT

[DZW+18] Hua Deng, Yunya Zhou, Qianhong Wu, Bo Qin, and Jianwei Liu. Secure pay-TV for chained hotels. *International Journal of Information Security*, 17(1):33–42, February 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0354-9.

Esponda:2007:PDP

[EAH+07] Fernando Esponda, Elena S. Ackley, Paul Helman, Haixia Jia, and Stephanie Forrest. Protecting data privacy through hard-to-reverse negative databases. *International Journal of Information Security*, 6(6): 403–415, October 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0030-1.

ElHassani:2015:ION

[EEB+15] Abdeljebar Ameziane El Hassani, Anas Abou El Kalam, Adel Bouhoula, Ryma Abassi, and Abdellah Ait Ouahman. Integrity-OrBAC: a new model to preserve Critical Infrastructures integrity. *International Journal of Information Security*, 14(4): 367–385, August 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0254-9.

Esponda:2009:NRI

[EFH09] Fernando Esponda, Stephanie Forrest, and Paul Helman. Negative representations of information. *International Journal of Information Security*, 8(5): 331–345, October 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0078-1.

ElSalamouny:2018:ONF

[EG18] Ehab ElSalamouny and Sébastien Gambs. Optimal noise functions for location privacy on continuous regions. *International Journal of Information Security*, 17(6): 613–630, November 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0384-y.

Egners:2015:MOW

[EHM15] André Egners, Patrick Herrmann, and Ulrike Meyer.

Multi-operator wireless mesh networks secured by an all-encompassing security architecture. *International Journal of Information Security*, 14 (2):169–186, April 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0244-y.

Emura:2014:GSI

[EHSS14] Keita Emura, Goichiro Hanaoka, Yusuke Sakai, and Jacob C. N. Schuldt. Group signature implies public-key encryption with non-interactive opening. *International Journal of Information Security*, 13 (1):51–62, February 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0204-y.

Esfahani:2017:EHM

[EMRN17] Alireza Esfahani, Georgios Mantas, Jonathan Rodriguez, and José Carlos Neves. An efficient homomorphic MAC-based scheme against data and tag pollution attacks in network coding-enabled wireless networks. *International Journal of Information Security*, 16(6): 627–639, November 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0351-z.

Estevez-Tapiador:2008:BRE

[ETAHCR08] Juan M. Estevez-Tapiador, Almudena Alcaide, Julio C. Hernandez-Castro, and Arturo Ribagorda. Bayesian rational exchange. *International Journal of Information Security*, 7(1): 85–100, January 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0039-5.

Elmufti:2009:MWS

[EWR+09] Kalid Elmufti, Dasun Weerasinghe, M. Rajarajan, Veselin Rakocevic, Sanowar Khan, and John A. MacDonald. Mobile Web services authentication using SAML and 3GPP generic bootstrapping architecture. *International Journal of Information Security*, 8(2): 77–87, April 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-008-0065-y.

Ferraris:2020:TTR

[FFG20] Davide Ferraris and Carmen Fernandez-Gago. TrUStAPIS: a trust requirements elicitation method for IoT. *International Journal of Information Security*, 19(1): 111–127, February 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00438-x.

Fiore:2012:RBS

[FGS12] D. Fiore, R. Gennaro, and N. P. Smart. Relations between the security models for certificateless encryption and ID-based key agreement. *International Journal of Information Security*, 11 (1):1–22, February 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0149-y.

Faust:2018:OPM

[FHV18] Sebastian Faust, Carmit Hazay, and Daniele Venturi. Outsourced pattern matching. *International Journal of Information Security*, 17(3):327–346, June 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0374-0.

Faghani:2019:MBM

[FN19] Mohammad R. Faghani and Uyen T. Nguyen. Mobile botnets meet social networks: design and analysis of a new type of botnet. *International Journal of Information Security*, 18(4):423–449, August 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0412-6.

Fong:2008:DCC

[Fon08] Philip W. L. Fong. Discretionary capability confinement. *International Journal of Information Security*, 7(2):137–154, April 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0047-5.

Frattolillo:2018:WPE

[Fra18] Franco Frattolillo. Watermarking protocols: an excursus to motivate a new approach. *International Journal of Information Security*, 17(5): 587–601, October 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.

com/article/10.1007/s10207-017-0386-9.

Farras:2019:PSP

[FRG19] Oriol Farràs and Jordi Ribes-González. Provably secure public-key encryption with conjunctive and subset keyword search. *International Journal of Information Security*, 18(5): 533–548, October 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-00426-7.

Fernandes:2014:SIC

[FSG+14] Diogo A. B. Fernandes, Liliana F. B. Soares, João V. Gomes, Mário M. Freire, and Pedro R. M. Inácio. Security issues in cloud environments: a survey. *International Journal of Information Security*, 13 (2):113–170, April 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0208-7.

Fan:2020:SHB

[FTS+20] Chun-I Fan, Yi-Fan Tseng, Hui-Po Su, Ruei-Hau Hsu, and Hiroaki Kikuchi. Secure hierarchical Bitcoin wallet scheme against privilege escalation attacks. *International Journal of Information Security*, 19 (3):245–255, June 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00476-5.

Granadillo:2014:RBC

[GBDJ14] Gustavo Gonzalez Granadillo, Malek Belhaouane, Hervé Debar, and Grégoire Jacob. RORI-based countermeasure selection using the OrBAC formalism. *International Journal of Information Security*, 13(1):63–79, February 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0207-8.

Gruber:2018:UTB

[GBG18] A. Gruber and I. Ben-Gal. Using targeted Bayesian network learning for suspect identification in communication networks. *International Journal of Information Security*, 17 (2):169–181, April 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0362-4.

Gao:2019:LBD

[GCH+19] Wen Gao, Liqun Chen,

Yupu Hu, Christopher J. P. Newton, Baocang Wang, and Jiangshan Chen. Lattice-based deniable ring signatures. *International Journal of Information Security*, 18 (3):355–370, June 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0417-1; http://link.springer.com/content/pdf/10.1007/s10207-018-0417-1.pdf.

Guerra-Casanova:2012:AMD

[GCSÁBdSS12] J. Guerra-Casanova, C. Sánchez-Ávila, G. Bailador, and A. de Santos Sierra. Authentication in mobile devices through hand gesture recognition. *International Journal of Information Security*, 11(2):65–83, April 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0154-9.

Garcia:2014:WLS

[GdKGV14] Flavio D. Garcia, Gerhard de Koning Gans, and Roel Verdult. Wirelessly lockpicking a smart card reader. *International Journal of Information Security*, 13(5): 403–420, October 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0234-0.

Guttman:2005:RAN

[GH05] Joshua D. Guttman and Amy L. Herzog. Rigorous automated network security management. *International Journal of Information Security*, 4(1–2):29–48, February 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0052-x.

Gulyas:2019:HIA

[GI19] Gábor György Gulyás and Sándor Imre. Hiding information against structural re-identification. *International Journal of Information Security*, 18 (2):125–139, April 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0400-x.

Gritzalis:2012:FAR

[GKBS12] Dimitris Gritzalis, Panagiotis Katsaros, Stylianos Basagiannis, and Yannis Soupionis. Formal analysis for robust anti-SPIT protection using model checking. *International Jour-*

nal of Information Security, 11(2):121–135, April 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0159-4.

Gauravaram:2010:HFU

[GKKT10] Praveen Gauravaram, John Kelsey, Lars R. Knudsen, and Søren S. Thomsen. On hash functions using checksums. *International Journal of Information Security*, 9(2):137–151, April 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0100-7.

Grining:2019:PPP

[GKS19] Krzysztof Grining, Marek Klonowski, and Piotr Syga. On practical privacy-preserving fault-tolerant data aggregation. *International Journal of Information Security*, 18 (3):285–304, June 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0413-5.

Gorrieri:2004:AAT

[GLMS+04] Roberto Gorrieri, Ruggero Lanotte, Andrea Maggiolo-Schettini, Fabio Martinelli, Simone Tini, and Enrico Tronci. Automated analysis of timed security: a case study on web privacy. *International Journal of Information Security*, 2(3–4):168–186, August 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0037-9.

Garra:2019:RAB

[GLMS19] Ricard Garra, Dominik Leibenger, Josep M. Miret, and Francesc Sebé. Repairing an aggregation-based smart metering system. *International Journal of Information Security*, 18(5): 637–646, October 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00435-0.

Gurgens:2003:ACP

[GLP03] Sigrid Gürgens, Javier Lopez, and René Peralta. Analysis of e-commerce protocols: Adapting a traditional technique. *International Journal of Information Security*, 2(1): 21–36, November 2003. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.

com/article/10.1007/s10207-003-0021-9.

Gouglidis:2014:SPV

[GMH14] Antonios Gouglidis, Ioannis Mavridis, and Vincent C. Hu. Security policy verification for multi-domains in cloud systems. *International Journal of Information Security*, 13 (2):97–111, April 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0205-x.

Galindo:2005:FOH

[GMMV05] David Galindo, Sebastià Martín, Paz Morillo, and Jorge L. Villar. Fujisaki–Okamoto hybrid encryption revisited. *International Journal of Information Security*, 4(4): 228–241, October 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0042-z.

Giorgini:2006:RET

[GMMZ06] Paolo Giorgini, Fabio Massacci, John Mylopoulos, and Nicola Zannone. Requirements engineering for trust management: model, methodology, and reasoning. *International Journal of Information Security*, 5(4):257–274, October 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-006-0005-7.

Gollman:2001:E

[GMO01] Dieter Gollman, Catherine A. Meadows, and Eiji Okamoto. Editorial. *International Journal of Information Security*, 1(1):1–2, August 2001. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s102070100004.

Geiselmann:2003:AIP

[GMS03] Willi Geiselmann, Willi Meier, and Rainer Steinwandt. An attack on the isomorphisms of polynomials problem with one secret. *International Journal of Information Security*, 2(1):59–64, November 2003. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-003-0025-5.

Gao:2014:TTR

[GNS14] Weizheng Gao, Kashi Neupane, and Rainer Steinwandt. Tuning a two-round group key agreement. *International Journal of Information Security*, 13(5):

467–476, October 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0225-6.

Garcia:2011:SID

[GOBdlC11] Sergio Sánchez García, Ana Gómez Oliva, Emilia Pérez Belleboni, and Iván Pau de la Cruz. Solving identity delegation problem in the e-government environment. *International Journal of Information Security*, 10(6): 351–372, November 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0140-7.

Gollmann:2008:E

[Gol08] Dieter Gollmann. Editorial. *International Journal of Information Security*, 7(2):101, April 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0052-8.

Golic:2012:NAM

[Gol12] Jovan Dj. Golić. A new authentication model for ad hoc networks. *International Journal of Information Security*, 11(5): 333–347, October 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0167-4.

Gunther:2017:LMT

[GP17] Felix Günther and Bertram Poettering. Linkable message tagging: solving the key distribution problem of signature schemes. *International Journal of Information Security*, 16 (3):281–297, June 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0327-z.

Garg:2017:NBD

[GPS17] Shree Garg, Sateesh K. Peddoju, and Anil K. Sarje. Network-based detection of Android malicious apps. *International Journal of Information Security*, 16(4): 385–400, August 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0343-z.

Gritzalis:2006:PKI

[Gri06] Stefanos Gritzalis. Public Key Infrastructure: Research and applications.

International Journal of Information Security, 5 (1):1–2, January 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-005-0075-y.

Gurgens:2005:SFN

[GRV05] Sigrid Gürgens, Carsten Rudolph, and Holger Vogt. On the security of fair non-repudiation protocols. *International Journal of Information Security*, 4(4): 253–262, October 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0063-7.

Giffhorn:2015:NAL

[GS15] Dennis Giffhorn and Gregor Snelting. A new algorithm for low-deterministic security. *International Journal of Information Security*, 14(3):263–287, June 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0257-6.

Gonzalez-Serrano:2018:SML

[GSAMCA18] Francisco-Javier González-Serrano, Adrián Amor-Martín, and Jorge Casamayón-Antón. Supervised machine learning using encrypted training data. *International Journal of Information Security*, 17(4): 365–377, August 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0381-1.

Glisson:2011:ERW

[GSM+11] William Bradley Glisson, Tim Storer, Gavin Mayall, Iain Moug, and George Grispos. Electronic retention: what does your mobile phone reveal about you? *International Journal of Information Security*, 10(6):337–349, November 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0144-3.

Gritti:2016:BED

[GSP+16] Clémentine Gritti, Willy Susilo, Thomas Plantard, Kaitai Liang, and Duncan S. Wong. Broadcast encryption with dealership. *International Journal of Information Security*, 15(3):271–283, June 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0285-x.

Goldschlag:2010:THB

[GSS10] David M. Goldschlag, Stuart G. Stubblebine, and Paul F. Syverson. Temporarily hidden bit commitment and lottery applications. *International Journal of Information Security*, 9(1):33–50, February 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-009-0094-1`.

Gyorffy:2011:TBG

[GTM11] John Charles Gyorffy, Andrew F. Tappenden, and James Miller. Token-based graphical password authentication. *International Journal of Information Security*, 10(6):321–336, November 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-011-0147-0`.

Geron:2009:CCR

[GW09] Erel Geron and Avishai Wool. CRUST: cryptographic remote untrusted storage without public keys. *International Journal of Information Security*, 8(5):357–377, October 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-009-0081-6`.

Gritzalis:2007:PMO

[GYL+07] S. Gritzalis, A. N. Yannacopoulos, C. Lambrinoudakis, P. Hatzopoulos, and S. K. Katsikas. A probabilistic model for optimal insurance contracts against security risks and privacy violation in IT outsourcing environments. *International Journal of Information Security*, 6(4):197–211, July 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-006-0010-x`.

Hadziosmanovic:2012:LMA

[HBH12] Dina Hadziosmanović, Damiano Bolzoni, and Pieter H. Hartel. A log mining approach for process monitoring in SCADA. *International Journal of Information Security*, 11(4):231–251, August 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-012-0163-8; http://link.springer.com/content/pdf/10.1007/s10207-012-0163-8.pdf`.

Han:2010:CBI

[HC10] Shui-Hua Han and Chao-Hsien Chu. Content-based image authentication: current status, issues, and challenges. *International Journal of Information Security*, 9(1): 19–32, February 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0093-2.

Hoang:2015:GAM

[HCN15] Thang Hoang, Deokjai Choi, and Thuc Nguyen. Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. *International Journal of Information Security*, 14(6): 549–560, November 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0273-1.

Hu:2016:EWS

[HH16] Changhui Hu and Lidong Han. Efficient wildcard search over encrypted data. *International Journal of Information Security*, 15 (5):539–547, October 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0302-0.

Hinarejos:2019:DPE

[HIDFGHR19] M. Francisca Hinarejos, Andreu-Pere Isern-Deyà, Josep-Lluís Ferrer-Gomila, and Llorenç Huguet-Rotger. Deployment and performance evaluation of mobile multicoupon solutions. *International Journal of Information Security*, 18(1): 101–124, February 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0404-6; http://link.springer.com/content/pdf/10.1007/s10207-018-0404-6.pdf.

Hasegawa:2009:PFC

[HIST09] Shingo Hasegawa, Shuji Isobe, Hiroki Shizuya, and Katsuhiro Tashiro. On the pseudo-freeness and the CDH assumption. *International Journal of Information Security*, 8(5): 347–355, October 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0087-0.

Hadavi:2015:SSS

[HJDC15] Mohammad Ali Hadavi, Rasool Jalili, Ernesto

Damiani, and Stelvio Cimato. Security and searchability in secret sharing-based data outsourcing. *International Journal of Information Security*, 14(6):513–529, November 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-015-0277-x`.

Hiemenz:2019:DSS

[HK19] Benedikt Hiemenz and Michel Krämer. Dynamic searchable symmetric encryption for storing geospatial data in the cloud. *International Journal of Information Security*, 18 (3):333–354, June 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-018-0414-4`.

Hopcroft:2004:ASA

[HL04] Philippa Hopcroft and Gavin Lowe. Analysing a stream authentication protocol using model checking. *International Journal of Information Security*, 3(1):2–13, October 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-004-0040-1`.

Han:2015:MAU

[HLKI15] Kyoung Soo Han, Jae Hyun Lim, Boojoong Kang, and Eul Gyu Im. Malware analysis using visualized images and entropy graphs. *International Journal of Information Security*, 14 (1):1–14, February 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-014-0242-0`.

Ham:2018:IYP

[HLS18] HyoungMin Ham, JongHyup Lee, and JooSeok Song. Improved yoking proof protocols for preserving anonymity. *International Journal of Information Security*, 17(4): 379–393, August 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-017-0383-z`.

Hitchcock:2004:ESM

[HMCD04] Yvonne Hitchcock, Paul Montague, Gary Carter, and Ed Dawson. The efficiency of solving multiple discrete logarithm problems and the implications for the security of fixed elliptic curves. *In-*

ternational Journal of Information Security, 3(2): 86–98, November 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0045-9.

Herranz:2014:SEA

[HN14] Javier Herranz and Jordi Nin. Secure and efficient anonymization of distributed confidential databases. *International Journal of Information Security*, 13(6):497–512, November 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0237-x.

Harn:2009:EIB

[HRL09] Lein Harn, Jian Ren, and Changlu Lin. Efficient identity-based GQ multisignatures. *International Journal of Information Security*, 8(3):205–210, June 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-008-0072-z.

Hammer:2009:FSC

[HS09] Christian Hammer and Gregor Snelting. Flow-sensitive, context-sensitive, and object-sensitive information flow control based on program dependence graphs. *International Journal of Information Security*, 8(6): 399–422, December 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0086-1.

Halevi:2015:KAS

[HS15] Tzipora Halevi and Nitesh Saxena. Keyboard acoustic side channel attacks: exploring realistic and security-sensitive scenarios. *International Journal of Information Security*, 14 (5):443–456, October 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0264-7.

Huang:2008:SUD

[HSMW08] Xinyi Huang, Willy Susilo, Yi Mu, and Wei Wu. Secure universal designated verifier signature without random oracles. *International Journal of Information Security*, 7 (3):171–183, June 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.

com/article/10.1007/s10207-007-0021-2.

Han:2012:NCO

[HSMY12] Jinguang Han, Willy Susilo, Yi Mu, and Jun Yan. New constructions of OSBE schemes and their applications in oblivious access control. *International Journal of Information Security*, 11(6): 389–401, November 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0176-3.

Hanley:2011:UTD

[HTM11] Neil Hanley, Michael Tunstall, and William P. Marnane. Using templates to distinguish multiplications from squaring operations. *International Journal of Information Security*, 10(4):255–266, August 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0135-4.

Huber:2012:PSS

[Hub12] Michael Huber. Perfect secrecy systems immune to spoofing attacks. *International Journal of Information Security*, 11(4): 281–289, August 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0166-5.

Huang:2011:ESD

[HYWS11] Qiong Huang, Guomin Yang, Duncan S. Wong, and Willy Susilo. Efficient strong designated verifier signature schemes without random oracle or with non-delegatability. *International Journal of Information Security*, 10(6): 373–385, November 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0146-1.

Huang:2012:NEO

[HYWS12] Qiong Huang, Guomin Yang, Duncan S. Wong, and Willy Susilo. A new efficient optimistic fair exchange protocol without random oracles. *International Journal of Information Security*, 11 (1):53–63, February 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0152-3.

Huang:2017:MAP

[HZL+17] Cheng-Ta Huang, Yu-Hong Zhang, Li-Chiun Lin, Wei-

Jen Wang, and Shiuh-Jeng Wang. Mutual authentications to parties with QR-code applications in mobile systems. *International Journal of Information Security*, 16(5): 525–540, October 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-016-0349-6`.

Isern-Deya:2015:PUG

[IDHRPCMP15] Andreu Pere Isern-Deyà, Llorenç Huguet-Rotger, M. Magdalena Payeras-Capellà, and Macià Mut-Puigserver. On the practicability of using group signatures on mobile devices: implementation and performance analysis on the Android platform. *International Journal of Information Security*, 14(4): 335–345, August 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-014-0259-4`.

Itakura:2002:PPI

[IHNT02] Yukio Itakura, Masaki Hashiyada, Toshio Nagashima, and Shigeo Tsujii. Proposal on personal identifiers generated from the STR information of DNA. *International Journal of Information Security*, 1(3): 149–160, November 2002. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-002-0013-1`.

Imamura:2018:IAA

[IMI18] Kazuya Imamura, Kazuhiko Minematsu, and Tetsu Iwata. Integrity analysis of authenticated encryption based on stream ciphers. *International Journal of Information Security*, 17 (5):493–511, October 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-017-0378-9`.

Itakura:2005:PMB

[IT05] Yukio Itakura and Shigeo Tsujii. Proposal on a multifactor biometric authentication method based on cryptosystem keys containing biometric signatures. *International Journal of Information Security*, 4(4):288–296, October 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-004-0065-5`.

Imamoto:2008:AEC

[IZS08] Kenji Imamoto, Jianying

Zhou, and Kouichi Sakurai. Achieving evenhandedness in certified email system for contract signing. *International Journal of Information Security*, 7(6): 383–394, November 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-008-0056-z.

Jia:2018:ERH

[JCL+18] Hongyong Jia, Yue Chen, Julong Lan, Kaixiang Huang, and Jun Wang. Efficient revocable hierarchical identity-based encryption using cryptographic accumulators. *International Journal of Information Security*, 17(4): 477–490, August 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0387-8.

James:2015:AIP

[JG15] Joshua I. James and Pavel Gladyshev. Automated inference of past action instances in digital investigations. *International Journal of Information Security*, 14(3):249–261, June 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0249-6.

Jovanovikj:2014:CMS

[JGK14] Vladimir Jovanovikj, Dusan Gabrijelcic, and Tomaz Klobucar. A conceptual model of security context. *International Journal of Information Security*, 13(6):571–581, November 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0229-x.

Joh:2017:PSV

[JM17] HyunChul Joh and Yashwant K. Malaiya. Periodicity in software vulnerability discovery, patching and exploitation. *International Journal of Information Security*, 16(6): 673–690, November 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0345-x.

Johnson:2001:ECD

[JMV01] Don Johnson, Alfred Menezes, and Scott Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, 1 (1):36–63, August 2001. CODEN ???? ISSN 1615-5262 (print), 1615-

5270 (electronic). URL http://link.springer.com/article/10.1007/s102070100002.

Jiang:2018:CPA

[JSMG18a] Yinhao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo. Ciphertext-policy attribute-based encryption supporting access policy update and its extension with preserved attributes. *International Journal of Information Security*, 17 (5):533–548, October 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0388-7.

Jiang:2018:FCP

[JSMG18b] Yinhao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo. Flexible ciphertext-policy attribute-based encryption supporting AND-gate and threshold with short ciphertexts. *International Journal of Information Security*, 17(4): 463–475, August 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0376-y.

Joudaki:2019:ETS

[JTV19] Zeinab Joudaki, Julie Thorpe, and Miguel Vargas Martin. Enhanced Tacit Secrets: System-assigned passwords you can't write down, but don't need to. *International Journal of Information Security*, 18 (2):239–255, April 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0408-2.

Jajodia:2011:MGE

[JZ11] Sushil Jajodia and Jianying Zhou. Message from the Guest Editors. *International Journal of Information Security*, 10(5): 267–268, October 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0131-8; http://link.springer.com/content/pdf/10.1007/s10207-011-0131-8.pdf.

Kirubavathi:2018:SAD

[KA18] G. Kirubavathi and R. Anitha. Structural analysis and detection of Android botnets using machine learning techniques. *International Journal of Information Security*, 17 (2):153–167, April 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.

com/article/10.1007/s10207-017-0363-3.

Karimi:2016:UAA

[KAC16] Vahid R. Karimi, Paulo S. C. Alencar, and Donald D. Cowan. A uniform approach for access control and business models with explicit rule realization. *International Journal of Information Security*, 15(2):145–171, April 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0275-z.

Karimi:2017:FMA

[KAC17] Vahid R. Karimi, Paulo S. C. Alencar, and Donald D. Cowan. A formal modeling and analysis approach for access control rules, policies, and their combinations. *International Journal of Information Security*, 16 (1):43–74, February 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0314-4.

Kundu:2013:PPA

[KB13] Ashish Kundu and Elisa Bertino. Privacy-preserving authentication of trees and graphs. *International Journal of Information Security*, 12(6): 467–494, November 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0198-5.

Knight:2007:IJI

[KBH07] Scott Knight, Scott Buffett, and Patrick C. K. Hung. The *International Journal of Information Security* special issue on privacy, security and trust technologies and e-business services. *International Journal of Information Security*, 6(5): 285–286, September 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0036-8.

Kotzanikolaou:2017:BAR

[KCB17] Panayiotis Kotzanikolaou, George Chatzisofroniou, and Mike Burmester. Broadcast anonymous routing (BAR): scalable real-time anonymous communication. *International Journal of Information Security*, 16(3):313–326, June 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0318-0.

Ko:2020:FDD

[KCB20] Ili Ko, Desmond Chambers, and Enda Barrett. Feature dynamic deep learning approach for DDoS mitigation within the ISP domain. *International Journal of Information Security*, 19 (1):53–70, February 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-019-00453-y`.

Kozakevicius:2015:UQS

[KCM+15] Alice Kozakevicius, Cristian Cappo, Bruno A. Mozzaquatro, Raul Ceretta Nunes, and Christian E. Schaerer. URL query string anomaly sensor designed with the bidimensional Haar wavelet transform. *International Journal of Information Security*, 14 (6):561–581, November 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-015-0276-y`.

Kulah:2019:SAD

[KDYS19] Yusuf Kulah, Berkay Dincer, Cemal Yilmaz, and Erkay Savas. SpyDetector: An approach for detecting side-channel attacks at runtime. *International Journal of Information Security*, 18(4): 393–422, August 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-018-0411-7`.

Kate:2011:GCB

[KG11] Aniket Kate and Ian Goldberg. Generalizing cryptosystems based on the subset sum problem. *International Journal of Information Security*, 10 (3):189–199, June 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-011-0129-2`.

Kozina:2009:MIW

[KGG09] Mario Kozina, Marin Golub, and Stjepan Gros. A method for identifying Web applications. *International Journal of Information Security*, 8(6): 455–467, December 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-009-0092-3`.

Kim:2014:EVE

[KJ14] Kee Sung Kim and Ik Rae Jeong. Efficient verifiably encrypted signatures

from lattices. *International Journal of Information Security*, 13(4): 305–314, August 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0226-0.

Kong:2011:SSA

[KJG+11] Deguang Kong, Yoon-Chan Jhi, Tao Gong, Sencun Zhu, Peng Liu, and Hongsheng Xi. SAS: semantics aware signature generation for polymorphic worm detection. *International Journal of Information Security*, 10(5): 269–283, October 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0132-7.

Kim:2017:MES

[KJS17] Minchul Kim, Younghoon Jung, and Junghwan Song. A modified exhaustive search on a password system using SHA-1. *International Journal of Information Security*, 16 (3):263–269, June 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0332-2.

Kananizadeh:2017:DDP

[KK17] Shahrzad Kananizadeh and Kirill Kononenko. Development of dynamic protection against timing channels. *International Journal of Information Security*, 16(6):641–651, November 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0356-7.

Kolias:2017:TDS

[KKK17] Constantinos Kolias, Vasilis Kolias, and Georgios Kambourakis. TermID: a distributed swarm intelligence-based approach for wireless intrusion detection. *International Journal of Information Security*, 16 (4):401–416, August 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0335-z.

Klinkoff:2007:ENS

[KKKV07] Patrick Klinkoff, Engin Kirda, Christopher Kruegel, and Giovanni Vigna. Extending .NET security to unmanaged code. *International Journal of Information Security*, 6(6): 417–428, October 2007. CODEN ???? ISSN 1615-5262 (print), 1615-

5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0031-0.

Koshutanski:2009:EGS

[KLMM09] Hristo Koshutanski, Aliaksandr Lazouski, Fabio Martinelli, and Paolo Mori. Enhancing grid security by fine-grained behavioral control and negotiation-based authorization. *International Journal of Information Security*, 8(4): 291–314, August 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0083-4.

Kremer:2003:FMP

[KM03] Steve Kremer and Olivier Markowitch. Fair multi-party non-repudiation protocols. *International Journal of Information Security*, 1(4):223–235, July 2003. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-003-0019-3.

Kopf:2007:TTU

[KM07] Boris Köpf and Heiko Mantel. Transformational typing and unification for automatically correcting insecure programs. *International Journal of Information Security*, 6(2–3):107–131, March 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0016-z.

Knudsen:2010:CEA

[KM10] Lars R. Knudsen and Charlotte V. Miolane. Counting equations in algebraic attacks on block ciphers. *International Journal of Information Security*, 9 (2):127–135, April 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0099-9.

Kasamatsu:2016:TSE

[KME+16] Kohei Kasamatsu, Takahiro Matsuda, Keita Emura, Nuttapong Attrapadung, Goichiro Hanaoka, and Hideki Imai. Time-specific encryption from forward-secure encryption: generic and direct constructions. *International Journal of Information Security*, 15 (5):549–571, October 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0304-y.

Korzhik:2003:HAB

[KML03] Valery Korzhik and Guillermo Morales-Luna. Hybrid authentication based on noisy channels. *International Journal of Information Security*, 1(4):203–210, July 2003. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-002-0017-x.

Kuper:2009:GXS

[KMR09] Gabriel Kuper, Fabio Massacci, and Nataliya Rassadko. Generalized XML security views. *International Journal of Information Security*, 8(3):173–203, June 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-008-0074-x.

Krukow:2007:TS

[KN07] Karl Krukow and Mogens Nielsen. Trust structures. *International Journal of Information Security*, 6(2–3):153–181, March 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0014-1.

[KNL16] **Kurek:2016:TBC**

Tytus Kurek, Marcin Niemiec, and Artur Lason. Taking back control of privacy: a novel framework for preserving cloud-based firewall policy confidentiality. *International Journal of Information Security*, 15(3):235–250, June 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0292-y; http://link.springer.com/content/pdf/10.1007/s10207-015-0292-y.pdf.

[KO02] **Kim:2002:NEC**

S. Kim and H. Oh. A new electronic check system with reusable refunds. *International Journal of Information Security*, 1(3):175–188, November 2002. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-002-0015-z.

[KOSU16] **Khayati:2016:PPP**

Leyli Javid Khayati, Cengiz Orencik, Erkay Savas, and Berkant Ustaoğlu. A practical privacy-preserving targeted advertising scheme for IPTV users. *International Journal of Information Security*, 15(4):

335–360, August 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0296-7.

Kontaxis:2012:MID

[KPM12] Georgios Kontaxis, Michalis Polychronakis, and Evangelos P. Markatos. Minimizing information disclosure to third parties in social login platforms. *International Journal of Information Security*, 11(5): 321–332, October 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0173-6.

Kundu:2010:DID

[KSM10] Amlan Kundu, Shamik Sural, and A. K. Majumdar. Database intrusion detection using sequence alignment. *International Journal of Information Security*, 9(3):179–191, June 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-010-0102-5.

Konstantinou:2007:EGS

[KSZ07] Elisavet Konstantinou, Yannis C. Stamatiou, and Christos Zaroliagis. Efficient generation of secure elliptic curves. *International Journal of Information Security*, 6(1):47–63, January 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-006-0009-3.

Kiraz:2016:EVA

[KU16] Mehmet Sabir Kiraz and Osmanbey Uzunkol. Efficient and verifiable algorithms for secure outsourcing of cryptographic computations. *International Journal of Information Security*, 15(5): 519–537, October 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0308-7.

Kudo:2002:PPB

[Kud02] Michiharu Kudo. PBAC: Provision-based access control model. *International Journal of Information Security*, 1(2): 116–130, February 2002. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s102070100010.

Kusters:2005:DCP

[Küs05] Ralf Küsters. On the de-

cidability of cryptographic protocols with open-ended data structures. *International Journal of Information Security*, 4(1–2):49–70, February 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0050-z.

Kamm:2015:SFP

[KW15] Liina Kamm and Jan Willemson. Secure floating point arithmetic and private satellite collision analysis. *International Journal of Information Security*, 14(6):531–548, November 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0271-8; http://link.springer.com/content/pdf/10.1007/s10207-014-0271-8.pdf.

Kluczniak:2019:MDA

[KWCK19] Kamil Kluczniak, Jianfeng Wang, Xiaofeng Chen, and Miroslaw Kutylowski. Multi-device anonymous authentication. *International Journal of Information Security*, 18 (2):181–197, April 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0406-4; http://link.springer.com/content/pdf/10.1007/s10207-018-0406-4.pdf.

Kuo:2018:DRA

[KYH18] Tsung-Min Kuo, Sung-Ming Yen, and Meng-Che Han. Dynamic reversed accumulator. *International Journal of Information Security*, 17 (2):183–191, April 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0360-6.

Landwehr:2001:CS

[Lan01] Carl E. Landwehr. Computer security. *International Journal of Information Security*, 1(1):3–13, August 2001. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s102070100003.

Ligatti:2005:EAE

[LBW05] Jay Ligatti, Lujo Bauer, and David Walker. Edit automata: enforcement mechanisms for run-time security policies. *International Journal of Information Security*, 4(1–2):2–16, February 2005. CODEN ???? ISSN

1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0046-8.

Liu:2010:EOO

[LBZ+10] Joseph K. Liu, Joonsang Baek, Jianying Zhou, Yanjiang Yang, and Jun Wen Wong. Efficient online/offline identity-based signature for wireless sensor network. *International Journal of Information Security*, 9(4):287–296, August 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-010-0109-y.

Laih:2004:GVR

[LC04] C. S. Laih and K. Y. Chen. Generating visible RSA public keys for PKI. *International Journal of Information Security*, 2(2):103–109, January 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-003-0030-8.

Lian:2014:PSC

[LCL14] Bin Lian, Gongliang Chen, and Jianhua Li. Provably secure e-cash system with practical and efficient complete tracing. *International Journal of Information Security*, 13(3):271–289, June 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0240-2.

Liu:2016:STP

[LCL16] Liang Liu, Xiaofeng Chen, and Wenjing Lou. Secure three-party computational protocols for triangle area. *International Journal of Information Security*, 15(1):1–13, February 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0284-y.

Li:2014:AAM

[LCPD14] Fudong Li, Nathan Clarke, Maria Papadaki, and Paul Dowland. Active authentication for mobile devices utilising behaviour profiling. *International Journal of Information Security*, 13(3):229–244, June 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0209-6.

Luo:2018:ASI

[LcSCL+18] Ying Luo, Sen ching S. Cheung, Riccardo Lazzeretti, Tommaso Pignata, and

Mauro Barni. Anonymous subject identification and privacy information management in video surveillance. *International Journal of Information Security*, 17(3):261–278, June 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0380-2.

Lauer:2007:BOT

[LD07] Thomas W. Lauer and Xiaodong Deng. Building online trust through privacy practices. *International Journal of Information Security*, 6(5):323–331, September 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0028-8.

Li:2017:WOO

[LD17] Lichun Li and Anwitaman Datta. Write-only oblivious RAM-based privacy-preserved access of outsourced data. *International Journal of Information Security*, 16(1):23–42, February 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0329-x; http://link.springer.com/content/pdf/10.1007/s10207-016-0329-x.pdf.

Levin:2007:WSL

[Lev07] Avner Levin. Is workplace surveillance legal in Canada? *International Journal of Information Security*, 6(5):313–321, September 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0026-x.

Li:2015:TMM

[LH15] Tao Li and Aiqun Hu. Trusted mobile model based on DTE technology. *International Journal of Information Security*, 14(5):457–469, October 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0266-5.

Liu:2007:ICR

[LI07] Jinshan Liu and Valérie Issarny. An incentive compatible reputation mechanism for ubiquitous computing environments. *International Journal of Information Security*, 6(5):297–311, September 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL

http://link.springer.com/article/10.1007/s10207-007-0029-7.

Lin:2015:RNR

[Lin15] Han-Yu Lin. RPCAE: a novel revocable proxy convertible authenticated encryption scheme. *International Journal of Information Security*, 14(5): 431–441, October 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0269-2.

Lee:2009:RTB

[LKH09] Sangho Lee, Jong Kim, and Sung Je Hong. Redistributing time-based rights between consumer devices for content sharing in DRM system. *International Journal of Information Security*, 8(4): 263–273, August 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0082-5.

Liao:2014:POC

[LL14] Qi Liao and Zhen Li. Portfolio optimization of computer and mobile botnets. *International Journal of Information Security*, 13 (1):1–14, February 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0206-9.

Lanet:2018:WTM

[LLBL18] Jean-Louis Lanet, Hélène Le Bouder, Mohammed Benattou, and Axel Legay. When time meets test. *International Journal of Information Security*, 17 (4):395–409, August 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0371-3.

Liu:2016:PCC

[LLW+16] Weiran Liu, Jianwei Liu, Qianhong Wu, Bo Qin, and Yan Li. Practical chosen-ciphertext secure Hierarchical Identity-Based Broadcast Encryption. *International Journal of Information Security*, 15(1):35–50, February 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0287-8.

Li:2009:DSA

[LLWY09] Jiangtao Li, Ninghui Li, XiaoFeng Wang, and Ting Yu. Denial of service attacks and defenses in decentralized trust manage-

ment. *International Journal of Information Security*, 8(2):89–101, April 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-008-0068-8.

Li:2006:USS

[LM06] Ninghui Li and John C. Mitchell. Understanding SPKI/SDSI using first-order logic. *International Journal of Information Security*, 5(1):48–64, January 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-005-0073-0.

Li:2017:RRS

[LMD17] Lichun Li, Michael Militzer, and Anwitaman Datta. rPIR: ramp secret sharing-based communication-efficient private information retrieval. *International Journal of Information Security*, 16(6):603–625, November 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0347-8.

Lai:2017:EIB

[LMG17] Jianchang Lai, Yi Mu, and Fuchun Guo. Efficient identity-based online/offline encryption and signcryption with short ciphertext. *International Journal of Information Security*, 16(3):299–311, June 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0320-6.

Lopez:2004:PDB

[LMMO04] Javier Lopez, Antonio Maña, Jose A. Montenegro, and Juan J. Ortega. PKI design based on the use of on-line certification authorities. *International Journal of Information Security*, 2(2):91–102, January 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-003-0027-3.

Lioy:2006:PPP

[LMMP06] Antonio Lioy, Marius Marian, Natalia Moltchanova, and Massimiliano Pala. PKI past, present and future. *International Journal of Information Security*, 5(1):18–29, January 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-005-0077-9.

Lazouski:2017:SDU

[LMMS17] Aliaksandr Lazouski, Fabio Martinelli, Paolo Mori, and Andrea Saracino. Stateful data usage control for Android mobile devices. *International Journal of Information Security*, 16 (4):345–369, August 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-016-0336-y`.

Lopriore:2018:ARM

[Lop18] Lanfranco Lopriore. Access right management by extended password capabilities. *International Journal of Information Security*, 17 (5):603–612, October 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-017-0390-0`.

Lim:2011:IBC

[LP11] Hoon Wei Lim and Kenneth G. Paterson. Identity-based cryptography for grid security. *International Journal of Information Security*, 10(1): 15–32, February 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-010-0116-z`.

Lin:2010:ECE

[LRB+10] Dan Lin, Prathima Rao, Elisa Bertino, Ninghui Li, and Jorge Lobo. EXAM: a comprehensive environment for the analysis of access control policies. *International Journal of Information Security*, 9(4): 253–273, August 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-010-0106-1`.

Lee:2014:AGU

[LSWW14] Ming-Feng Lee, Nigel P. Smart, Bogdan Warinschi, and Gaven J. Watson. Anonymity guarantees of the UMTS/LTE authentication and connection protocol. *International Journal of Information Security*, 13(6): 513–527, November 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-014-0231-3`.

Lu:2009:RKR

[Lu09] Jiqiang Lu. Related-key rectangle attack on 36 rounds of the XTEA block cipher. *International Journal of Information Secu-*

rity, 8(1):1–11, February 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-008-0059-9.

Lin:2010:MTE

[LV10] Ching Lin and Vijay Varadharajan. MobileTrust: a trust enhanced security architecture for mobile agent systems. *International Journal of Information Security*, 9(3):153–178, June 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0098-x.

Laszka:2018:GTA

[LVK18] Aron Laszka, Yevgeniy Vorobeychik, and Xenofon Koutsoukos. A game-theoretic approach for integrity assurance in resource-bounded systems. *International Journal of Information Security*, 17(2):221–242, April 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0364-2.

Li:2018:IVC

[LZQ+18] Yuxi Li, Fucai Zhou, Yuhai Qin, Muqing Lin, and Zifeng Xu. Integrity-verifiable conjunctive keyword searchable encryption in cloud storage. *International Journal of Information Security*, 17(5):549–568, October 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0394-9.

Malhi:2016:PPA

[MB16] Avleen Malhi and Shalini Batra. Privacy-preserving authentication framework using Bloom filter for secure vehicular communications. *International Journal of Information Security*, 15(4):433–453, August 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0299-4.

Mehrnezhad:2017:PCI

[MBHT17] Maryam Mehrnezhad, Abbas Ghaemi Bafghi, Ahad Harati, and Ehsan Toreini. PiSHi: click the images and I tell if you are a human. *International Journal of Information Security*, 16(2):133–149, April 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-

015-0311-z; http://link.springer.com/content/pdf/10.1007/s10207-015-0311-z.pdf.

Martinez-Balleste:2018:DIS

[MBRPS18] Antoni Martínez-Ballesté, Hatem Rashwan, Domenec Puig, and Agusti Solanas. Design and implementation of a secure and trustworthy platform for privacy-aware video surveillance. *International Journal of Information Security*, 17 (3):279–290, June 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0370-4.

Marconi:2011:CPE

[MCD11] Luciana Marconi, Mauro Conti, and Roberto Di Pietro. CASSANDRA: a probabilistic, efficient, and privacy-preserving solution to compute set intersection. *International Journal of Information Security*, 10 (5):301–319, October 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0133-6.

McHugh:2001:IID

[McH01] John McHugh. Intrusion and intrusion detection. *International Journal of Information Security*, 1(1):14–35, August 2001. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s102070100001.

Martina:2015:ATM

[MdSC+15] Jean Everson Martina, Eduardo dos Santos, Marcelo Carlomagno Carlos, Geraint Price, and Ricardo Felipe Custódio. An adaptive threat model for security ceremonies. *International Journal of Information Security*, 14 (2):103–121, April 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0253-x.

Munoz:2004:CRS

[MFES04] Jose L. Muñoz, Jordi Forne, Oscar Esparza, and Miguel Soriano. Certificate revocation system implementation based on the Merkle hash tree. *International Journal of Information Security*, 2(2): 110–124, January 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-003-0026-4.

Makhlouf:2019:SAS

[MG19] Amel Meddeb Makhlouf and Mohsen Guizani. SE-AOMDV: secure and efficient AOMDV routing protocol for vehicular communications. *International Journal of Information Security*, 18(5): 665–676, October 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-019-00436-z`.

Marco-Gisbert:2019:SES

[MGRR19] Héctor Marco-Gisbert and Ismael Ripoll-Ripoll. SSPFA: effective stack smashing protection for Android OS. *International Journal of Information Security*, 18 (4):519–532, August 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-018-00425-8; http://link.springer.com/content/pdf/10.1007/s10207-018-00425-8.pdf`.

Malatras:2017:EUI

[MGV17] Apostolos Malatras, Dimitris Geneiatakis, and Ioannis Vakalis. On the efficiency of user identification: a system-based approach. *International Journal of Information Security*, 16(6):653–671, November 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-016-0340-2; http://link.springer.com/content/pdf/10.1007/s10207-016-0340-2.pdf`.

Mousazadeh:2014:RGA

[ML14] Mousa Mousazadeh and Behrouz Tork Ladani. Randomized gossip algorithms under attack. *International Journal of Information Security*, 13(4): 391–402, August 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-013-0221-x`.

Mann:2017:TFA

[ML17] Christopher Mann and Daniel Loebenberger. Two-factor authentication for the Bitcoin protocol. *International Journal of Information Security*, 16 (2):213–226, April 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-016-0325-1`.

Miao:2016:MDU

[MLCS16] Qiguang Miao, Jiachen

Liu, Ying Cao, and Jianfeng Song. Malware detection using bilayer behavior abstraction and improved one-class support vector machines. *International Journal of Information Security*, 15(4): 361–379, August 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-015-0297-6`.

Mesbah:2019:REJ

[MLM19] Abdelhak Mesbah, Jean-Louis Lanet, and Mohamed Mezghiche. Reverse engineering Java Card and vulnerability exploitation: a shortcut to ROM. *International Journal of Information Security*, 18(1): 85–100, February 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-018-0401-9`.

Mana:2004:FSE

[MLO+04] Antonio Maña, Javier Lopez, Juan J. Ortega, Ernesto Pimentel, and Jose M. Troya. A framework for secure execution of software. *International Journal of Information Security*, 3(2): 99–112, November 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-004-0048-6`.

Meng:2020:ECB

[MLYL20] Weizhi Meng, Wenjuan Li, Laurence T. Yang, and Peng Li. Enhancing challenge-based collaborative intrusion detection networks against insider attacks using blockchain. *International Journal of Information Security*, 19 (3):279–290, June 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-019-00462-x`.

Mateu:2016:HAV

[MMS16] Víctor Mateu, Josep M. Miret, and Francesc Sebé. A hybrid approach to vector-based homomorphic tallying remote voting. *International Journal of Information Security*, 15 (2):211–221, April 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-015-0279-8`.

Martina:2015:VMB

[MP15] Jean Everson Martina and Lawrence Charles Paulson. Verifying multicast-

based security protocols using the inductive method. *International Journal of Information Security*, 14 (2):187–204, April 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0251-z.

Mennink:2016:EPH

[MP16] Bart Mennink and Bart Preneel. Efficient parallelizable hashing using small non-compressing primitives. *International Journal of Information Security*, 15(3):285–300, June 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0288-7.

Mavrogiannopoulos:2014:TSK

[MPP14] Nikos Mavrogiannopoulos, Andreas Pashalidis, and Bart Preneel. Toward a secure Kerberos key exchange with smart cards. *International Journal of Information Security*, 13 (3):217–228, June 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0213-x.

MacKenzie:2010:PAK

[MPS10] Philip MacKenzie, Sarvar Patel, and Ram Swaminathan. Password-authenticated key exchange based on RSA. *International Journal of Information Security*, 9(6): 387–410, December 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-010-0120-3.

Manulis:2014:PAI

[MPS14] Mark Manulis, Bertram Poettering, and Douglas Stebila. Plaintext awareness in identity-based key encapsulation. *International Journal of Information Security*, 13(1): 25–49, February 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0218-5.

MacKenzie:2003:NCD

[MR03] Philip MacKenzie and Michael K. Reiter. Networked cryptographic devices resilient to capture. *International Journal of Information Security*, 2 (1):1–20, November 2003. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL

http://link.springer.com/article/10.1007/s10207-003-0022-8.

MacKenzie:2004:TPG

[MR04] Philip MacKenzie and Michael K. Reiter. Two-party generation of DSA signatures. *International Journal of Information Security*, 2(3–4): 218–239, August 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0041-0.

Monrose:2002:PHB

[MRW02] Fabian Monrose, Michael K. Reiter, and Susanne Wetzel. Password hardening based on keystroke dynamics. *International Journal of Information Security*, 1(2):69–83, February 2002. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s102070100006.

Mashatan:2009:ITC

[MS09] Atefeh Mashatan and Douglas R. Stinson. Interactive two-channel message authentication based on Interactive–Collision Resistant hash functions. *International Journal of Information Security*, 8(1): 49–60, February 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-008-0063-0.

Miret:2011:CAH

[MS11] Josep M. Miret and Francesc Sebé. Cryptanalysis of an ad-hoc cryptosystem for mix-based e-voting robust against relation attacks. *International Journal of Information Security*, 10 (6):387–389, November 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0145-2.

Mizuki:2014:FCB

[MS14] Takaaki Mizuki and Hiroki Shizuya. A formalization of card-based cryptographic protocols via abstract machine. *International Journal of Information Security*, 13(1):15–23, February 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0219-4.

Mustafa:2015:UIA

[MS15] Tanveer Mustafa and Karsten Sohr. Understanding the implemented access control policy of Android system services with slicing and extended static check-

ing. *International Journal of Information Security*, 14(4):347–366, August 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0260-y.

Morales-Sandoval:2018:PBC

[MSGCDPSS18] Miguel Morales-Sandoval, Jose Luis Gonzalez-Compean, Arturo Diaz-Perez, and Victor J. Sosa-Sosa. A pairing-based cryptographic approach for data security in the cloud. *International Journal of Information Security*, 17(4):441–461, August 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0375-z.

Manulis:2016:SMP

[MSKD16] Mark Manulis, Douglas Stebila, Franziskus Kiefer, and Nick Denham. Secure modular password authentication for the web using channel bindings. *International Journal of Information Security*, 15(6):597–620, November 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0348-7; http://link.springer.com/content/pdf/10.1007/s10207-016-0348-7.pdf.

Mizuki:2002:CCF

[MSN02] Takaaki Mizuki, Hiroki Shizuya, and Takao Nishizeki. A complete characterization of a family of key exchange protocols. *International Journal of Information Security*, 1(2):131–142, February 2002. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s102070100011.

Marmol:2013:PEA

[MSP+13] Félix Gómez Mármol, Christoph Sorge, Ronald Petrlic, Osman Ugus, Dirk Westhoff, and Gregorio Martínez Pérez. Privacy-enhanced architecture for smart metering. *International Journal of Information Security*, 12(2):67–82, April 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0181-6.

Mehrnezhad:2018:SPM

[MTSH18] Maryam Mehrnezhad, Ehsan Toreini, Siamak F. Shahandashti, and Feng Hao. Stealing PINs via mobile sensors: actual risk versus user perception. *In-*

ternational Journal of Information Security, 17 (3):291–313, June 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0369-x; http://link.springer.com/content/pdf/10.1007/s10207-017-0369-x.pdf.

McEvoy:2014:ANT

[MTW+14] Robert P. McEvoy, Michael Tunstall, Claire Whelan, Colin C. Murphy, and William P. Marnane. All-or-Nothing Transforms as a countermeasure to differential side-channel analysis. *International Journal of Information Security*, 13(3):291–304, June 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0212-y.

Murakami:2018:OAA

[MU18] Keisuke Murakami and Takeaki Uno. Optimization algorithm for k-anonymization of datasets with low information loss. *International Journal of Information Security*, 17 (6):631–644, November 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0392-y.

Mayer:2006:OFA

[MWZ06] Alain Mayer, Avishai Wool, and Elisha Ziskind. Offline firewall analysis. *International Journal of Information Security*, 5 (3):125–144, July 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-005-0074-z.

Mu:2014:RBD

[MYLZ14] Chengpo Mu, Meng Yu, Yingjiu Li, and Wanyu Zang. Risk balance defense approach against intrusions for network server. *International Journal of Information Security*, 13 (3):255–269, June 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0214-9.

Nunez:2014:BPP

[NA14] David Nuñez and Isaac Agudo. BlindIdM: A privacy-preserving approach for identity management as a service. *International Journal of Information Security*, 13 (2):199–215, April 2014. CODEN ???? ISSN

1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0230-4.

Nali:2006:HTB

[NAM06] Deholo Nali, Carlisle Adams, and Ali Miri. Hierarchical time-based information release. *International Journal of Information Security*, 5(2):92–104, April 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-006-0084-5.

Niebuhr:2012:SPS

[NMBB12] Robert Niebuhr, Mohammed Meziani, Stanislav Bulygin, and Johannes Buchmann. Selecting parameters for secure McEliece-based cryptosystems. *International Journal of Information Security*, 11(3):137–147, June 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0153-2.

Naor:2010:ETR

[NP10] Moni Naor and Benny Pinkas. Efficient trace and revoke schemes. *International Journal of Information Security*, 9(6):411–424, December 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-010-0121-2.

Nappa:2015:MDI

[NRC15] Antonio Nappa, M. Zubair Rafique, and Juan Caballero. The MALICIA dataset: identification and analysis of drive-by download operations. *International Journal of Information Security*, 14 (1):15–33, February 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0248-7.

Nguyen:2006:VSF

[NSNK06] Lan Nguyen, Rei Safavi-Naini, and Kaoru Kurosawa. Verifiable shuffles: a formal model and a paillier-based three-round construction with provable security. *International Journal of Information Security*, 5(4):241–255, October 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-006-0004-8.

Narasimha:2009:PPR

[NST09] M. Narasimha, J. Solis, and G. Tsudik. Privacy-

preserving revocation checking. *International Journal of Information Security*, 8(1):61–75, February 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-008-0064-z.

Nayak:2020:SSE

[NT20] Sanjeet Kumar Nayak and Somanath Tripathy. SEDS: secure and efficient server-aided data deduplication scheme for cloud storage. *International Journal of Information Security*, 19 (2):229–240, April 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00455-w.

Nuida:2012:SCS

[Nui12] Koji Nuida. Short collusion-secure fingerprint codes against three pirates. *International Journal of Information Security*, 11 (2):85–102, April 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0155-8.

Nieto:2002:KRC

[NVB+02] J. M. Gonzáles Nieto, K. Viswanathan, C. Boyd, A. Clark, and E. Dawson. Key recovery for the commercial environment. *International Journal of Information Security*, 1(3): 161–174, November 2002. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-002-0014-0.

Ozawa:2020:SIM

[OBH+20] Seiichi Ozawa, Tao Ban, Naoki Hashimoto, Junji Nakazato, and Jumpei Shimamura. A study of IoT malware activities using association rule learning for darknet sensor data. *International Journal of Information Security*, 19 (1):83–92, February 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00439-w.

Orencik:2016:MKS

[OSSK16] Cengiz Orencik, Ayse Selcuk, Erkay Savas, and Murat Kantarcioğlu. Multi-keyword search over encrypted data with scoring and search pattern obfuscation. *International Journal of Information Security*, 15(3):251–269, June 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL

http://link.springer.com/article/10.1007/s10207-015-0294-9.

Okeya:2006:SAC

[OT06] Katsuyuki Okeya and Tsuyoshi Takagi. Security analysis of CRT-based cryptosystems. *International Journal of Information Security*, 5(3):177–185, July 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-005-0080-1.

Patsakis:2019:HID

[PC19] Constantinos Patsakis and Fran Casino. Hydras and IPFS: a decentralised playground for malware. *International Journal of Information Security*, 18(6):787–799, December 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00443-0.

Peng:2011:MOS

[PDB11] Kun Peng, Ed Dawson, and Feng Bao. Modification and optimisation of a shuffling scheme: stronger security, formal analysis and higher efficiency. *International Journal of Information Security*, 10 (1):33–47, February 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-010-0117-y.

Patil:2020:DVA

[PDM20] Rajendra Patil, Harsha Dudeja, and Chirag Modi. Designing in-VM-assisted lightweight agent-based malware detection framework for securing virtual machines in cloud computing. *International Journal of Information Security*, 19(2):147–162, April 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00447-w.

Peng:2011:GEC

[Pen11] Kun Peng. A general and efficient countermeasure to relation attacks in mix-based e-voting. *International Journal of Information Security*, 10 (1):49–60, February 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-010-0122-1.

Peng:2012:TDA

[Pen12] Kun Peng. Threshold distributed access control with public verification:

a practical application of PVSS. *International Journal of Information Security*, 11(1):23–31, February 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0151-4.

Peng:2013:SAH

[Pen13] Kun Peng. A shuffle to achieve high efficiency through pre-computation and batch verification. *International Journal of Information Security*, 12(4):337–345, August 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0193-x.

Pereniguez-Garcia:2013:KPA

[PGMLK+13] F. Pereñíguez-García, R. Marín-López, G. Kambourakis, A. Ruiz-Martínez, S. Gritzalis, and A. F. Skarmeta-Gómez. KAMU: providing advanced user privacy in Kerberos multi-domain scenarios. *International Journal of Information Security*, 12(6):505–525, November 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0201-1.

Pais:2010:NPR

[PJ10] Alwyn R. Pais and Shankar Joshi. A new probabilistic rekeying method for secure multicast groups. *International Journal of Information Security*, 9(4):275–286, August 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-010-0108-z.

Plaga:2009:BKS

[Pla09] Rainer Plaga. Biometric keys: suitable use cases and achievable information content. *International Journal of Information Security*, 8(6):447–454, December 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0090-5.

Perez-Mendez:2012:CLS

[PMPGMLLM12] Alejandro Pérez-Méndez, Fernando Pereñíguez-García, Rafael Marín-López, and Gabriel López-Millán. A cross-layer SSO solution for federating access to kerberized services in the eduroam/DAMe network. *International Journal of Information Security*, 11(6):365–388, November 2012. CODEN ???? ISSN

1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0174-5.

Pitropakis:2015:BRP

[PPL15] Nikolaos Pitropakis, Aggelos Pikrakis, and Costas Lambrinoudakis. Behaviour reflects personality: detecting co-residence attacks on Xen-based cloud environments. *International Journal of Information Security*, 14(4): 299–305, August 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0255-8.

Phan:2013:ACB

[PPSS13] Duong-Hieu Phan, David Pointcheval, Siamak F. Shahandashti, and Mario Strefler. Adaptive CCA broadcast encryption with constant-size secret keys and ciphertexts. *International Journal of Information Security*, 12(4): 251–265, August 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0190-0.

Priami:2004:PSI

[Pri04] Corrado Priami. Preface to the special issue on Security in Global Computing. *International Journal of Information Security*, 2(3–4):125, August 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0034-z; http://link.springer.com/content/pdf/10.1007/s10207-004-0034-z.pdf.

Poettering:2017:DAP

[PS17] Bertram Poettering and Douglas Stebila. Double-authentication-preventing signatures. *International Journal of Information Security*, 16(1):1–22, February 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0307-8.

Perez-Sola:2019:DSP

[PSDSNAHJ19] Cristina Pérez-Solà, Sergi Delgado-Segura, Guillermo Navarro-Arribas, and Jordi Herrera-Joancomartí. Double-spending prevention for Bitcoin zero-confirmation transactions. *International Journal of Information Security*, 18(4): 451–463, August 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL

http://link.springer.com/article/10.1007/s10207-018-0422-4.

Qin:2009:SSS

[QDW09] Huawang Qin, Yuewei Dai, and Zhiquan Wang. A secret sharing scheme based on (t, n) threshold and adversary structure. *International Journal of Information Security*, 8(5): 379–385, October 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0085-2.

Qin:2015:FAB

[QDW+15] Bo Qin, Hua Deng, Qianhong Wu, Josep Domingo-Ferrer, David Naccache, and Yunya Zhou. Flexible attribute-based encryption applicable to secure e-healthcare records. *International Journal of Information Security*, 14(6): 499–511, November 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0272-7.

Quinn:2009:AAE

[QLOW09] Karl Quinn, David Lewis, Declan O'Sullivan, and Vincent P. Wade. An analysis of accuracy experiments carried out over of a multi-faceted model of trust. *International Journal of Information Security*, 8(2):103–119, April 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-008-0069-7.

Qian:2015:PPP

[QLZH15] Huiling Qian, Jiguo Li, Yichen Zhang, and Jinguang Han. Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation. *International Journal of Information Security*, 14(6): 487–497, November 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0270-9.

Raad:2016:PSR

[RAC16] Elie Raad, Bechara Al Bouna, and Richard Chbeir. Preventing sensitive relationships disclosure for better social media preservation. *International Journal of Information Security*, 15(2):173–194, April 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0278-9.

Rodeh:2002:UAT

[RBD02] Ohad Rodeh, Kenneth P. Birman, and Danny Dolev. Using AVL trees for fault-tolerant group key management. *International Journal of Information Security*, 1(2):84–99, February 2002. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s102070100008`.

Riecker:2015:LEC

[RBEH15] Michael Riecker, Sebastian Biedermann, Rachid El Bansarkhani, and Matthias Hollick. Lightweight energy consumption-based intrusion detection system for wireless sensor networks. *International Journal of Information Security*, 14 (2):155–167, April 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-014-0241-1`.

Rao:2016:EAB

[RD16] Y. Sreenivasa Rao and Ratna Dutta. Efficient attribute-based signature and signcryption realizing expressive access structures. *International Journal of Information Security*, 15(1): 81–109, February 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-015-0289-6`.

Rial:2018:PPS

[RDK18] Alfredo Rial, George Danezis, and Markulf Kohlweiss. Privacy-preserving smart metering revisited. *International Journal of Information Security*, 17 (1):1–31, February 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-016-0355-8`.

Rizomiliotis:2013:SAP

[RG13] Panagiotis Rizomiliotis and Stefanos Gritzalis. On the security of AUTH, a provably secure authentication protocol based on the subspace LPN problem. *International Journal of Information Security*, 12(2):151–154, April 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-012-0188-z`.

Rowe:2016:MPS

[RGL16] Paul D. Rowe, Joshua D. Guttman, and Moses D. Liskov. Measuring protocol strength with security goals. *Interna-*

tional Journal of Information Security, 15(6): 575–596, November 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0319-z.

Ruiz-Heras:2017:AAB

[RHGTSC17] A. Ruiz-Heras, P. García-Teodoro, and L. Sánchez-Casado. ADroid: anomaly-based detection of malicious events in Android platforms. *International Journal of Information Security*, 16(4): 371–384, August 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0333-1.

Ragab-Hassen:2017:KMS

[RHL17] Hani Ragab-Hassen and Esma Lounes. A key management scheme evaluation using Markov processes. *International Journal of Information Security*, 16(3):271–280, June 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0323-3; http://link.springer.com/content/pdf/10.1007/s10207-016-0323-3.pdf.

Ribeiro:2018:SRH

[RLEM18] Carlos Ribeiro, Herbert Leitold, Simon Esposito, and David Mitzam. STORK: a real, heterogeneous, large-scale eID management system. *International Journal of Information Security*, 17(5): 569–585, October 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0385-x.

Reaves:2012:OVT

[RM12] Bradley Reaves and Thomas Morris. An open virtual testbed for industrial control system security research. *International Journal of Information Security*, 11(4):215–229, August 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0164-7.

Rebollo-Monedero:2013:MPA

[RMPADF13] David Rebollo-Monedero, Javier Parra-Arnau, Claudia Diaz, and Jordi Forné. On the measurement of privacy as an attacker's estimation error. *International Journal of Information Security*, 12 (2):129–149, April 2013. CODEN ???? ISSN

1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0182-5.

Ros-Martin:2019:SND

[RMSCR19] Miguel Ros-Martín, Julián Salas, and Jordi Casas-Roma. Scalable non-deterministic clustering-based k-anonymization for rich networks. *International Journal of Information Security*, 18 (2):219–238, April 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0409-1.

Roelse:2011:DST

[Roe11a] Peter Roelse. Dynamic subtree tracing and its application in pay-TV systems. *International Journal of Information Security*, 10(3):173–187, June 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0126-5. See erratum [Roe11b].

Roelse:2011:EDS

[Roe11b] Peter Roelse. Erratum to: Dynamic subtree tracing and its application in pay-TV systems. *International Journal of Information Security*, 10 (6):391, November 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0141-6; http://link.springer.com/content/pdf/10.1007/s10207-011-0141-6.pdf. See [Roe11a].

Rezvani:2019:AXP

[RRI+19] Mohsen Rezvani, David Rajaratnam, Aleksandar Ignjatovic, Maurice Pagnucco, and Sanjay Jha. Analyzing XACML policies using answer set programming. *International Journal of Information Security*, 18(4):465–479, August 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0421-5.

Roy:2018:DSC

[RS18] Sangita Roy and Ashok Singh Sairam. Distributed star coloring of network for IP traceback. *International Journal of Information Security*, 17(3):315–326, June 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0366-0.

Rastegari:2019:CDV

[RSD19] Parvin Rastegari, Willy Susilo, and Mohammad Dakhilalian. Certificateless designated verifier signature revisited: achieving a concrete scheme in the standard model. *International Journal of Information Security*, 18(5): 619–635, October 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-019-00430-5`.

Resende:2019:BMI

[RSMA19] João S. Resende, Patrícia R. Sousa, Rolando Martins, and Luís Antunes. Breaking MPC implementations through compression. *International Journal of Information Security*, 18(4): 505–518, August 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-018-0424-2`.

Rashwan:2016:UTP

[RSPMB16] Hatem A. Rashwan, Agusti Solanas, Domènec Puig, and Antoni Martínez-Ballesté. Understanding trust in privacy-aware video surveillance systems. *International Journal of Information Security*, 15 (3):225–234, June 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-015-0286-9`.

Russell:2004:TBR

[Rus04] Selwyn Russell. Theory and benefits of recursive certificate structures. *International Journal of Information Security*, 2(2):78–90, January 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-003-0028-2`.

Ruan:2003:FGB

[RV03] Chun Ruan and Vijay Varadharajan. A formal graph based framework for supporting authorization delegations and conflict resolutions. *International Journal of Information Security*, 1(4):211–222, July 2003. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-003-0018-4`.

Riesco:2019:LCT

[RV19] R. Riesco and V. A. Villagrá. Leveraging cyber threat intelligence for a dynamic risk framework. *International Journal of In-*

formation Security, 18(6): 715–739, December 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00433-2.

Shaikh:2017:DCM

[SAL17] Riaz Ahmed Shaikh, Kamel Adi, and Luigi Logrippo. A data classification method for inconsistency and incompleteness detection in access control policy sets. *International Journal of Information Security*, 16 (1):91–113, February 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0317-1.

Sourour:2009:ESD

[SAT09] Meharouech Sourour, Bouhoula Adel, and Abbes Tarek. Ensuring security in depth based on heterogeneous network security technologies. *International Journal of Information Security*, 8(4):233–246, August 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0077-2.

Sattath:2020:IQB

[Sat20] Or Sattath. On the insecurity of quantum Bitcoin mining. *International Journal of Information Security*, 19(3):291–302, June 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-020-00493-9.

Shay:2009:CST

[SB09] Richard Shay and Elisa Bertino. A comprehensive simulation tool for the analysis of password policies. *International Journal of Information Security*, 8(4):275–289, August 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0084-3.

Saikia:2014:PHF

[SB14] Navajit Saikia and Prabin K. Bora. Perceptual hash function for scalable video. *International Journal of Information Security*, 13(1):81–93, February 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0211-z.

Samadani:2019:SPM

[SBB19] Mohammad Hasan Samadani, Mehdi Berenjkoob, and Marina Blanton. Secure

pattern matching based on bit parallelism. *International Journal of Information Security*, 18 (3):371–391, June 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0410-8.

Scaife:2018:OSR

[SCL+18] Nolen Scaife, Henry Carter, Lyrissa Lidsky, Rachael L. Jones, and Patrick Traynor. OnionDNS: a seizure-resistant top-level domain. *International Journal of Information Security*, 17 (6):645–660, November 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0391-z.

Skoric:2016:FBR

[SdHZ16] Boris Skorić, Sebastiaan J. A. de Hoogh, and Nicola Zannone. Flow-based reputation with uncertainty: evidence-based subjective logic. *International Journal of Information Security*, 15(4):381–402, August 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0298-5; http://link.springer.com/content/pdf/10.1007/s10207-015-0298-5.pdf.

Sowjanya:2020:ECC

[SDR20] K. Sowjanya, Mou Dasgupta, and Sangram Ray. An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems. *International Journal of Information Security*, 19(1): 129–146, February 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00464-9.

Sen:2014:UIW

[Sen14] Sevil Sen. Using instance-weighted naive Bayes for adapting concept drift in masquerade detection. *International Journal of Information Security*, 13(6): 583–590, November 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0238-9.

Seo:2018:AOF

[SEXY18] Jae Hong Seo, Keita Emura, Keita Xagawa, and Kazuki Yoneyama. Accumulable optimistic fair exchange from verifiably encrypted homomorphic signatures. *Inter-*

national Journal of Information Security, 17 (2):193–220, April 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0367-z.

Singh:2017:RUA

[SF17] Ankit Singh and Hervais C. Simo Fhom. Restricted usage of anonymous credentials in vehicular ad hoc networks for misbehavior detection. *International Journal of Information Security*, 16 (2):195–211, April 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0328-y.

Steinwandt:2002:APB

[SGE02] Rainer Steinwandt, Willi Geiselmann, and Regine Endsuleit. Attacking a polynomial-based cryptosystem: Polly cracker. *International Journal of Information Security*, 1(3): 143–148, November 2002. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-002-0012-2.

Shah:2019:MEF

[SGJ19] Ankit Shah, Rajesh Ganesan, and Sushil Jajodia. A methodology for ensuring fair allocation of CSOC effort for alert investigation. *International Journal of Information Security*, 18(2):199–218, April 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0407-3.

Shah:2018:MMM

[SGJC18] Ankit Shah, Rajesh Ganesan, Sushil Jajodia, and Hasan Cam. A methodology to measure and monitor level of operational effectiveness of a CSOC. *International Journal of Information Security*, 17 (2):121–134, April 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0365-1.

Saini:2019:YCS

[SGLC19] Anil Saini, Manoj Singh Gaur, Vijay Laxmi, and Mauro Conti. You click, I steal: analyzing and detecting click hijacking attacks in web pages. *International Journal of Information Security*, 18(4): 481–504, August 2019.

CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0423-3.

Shayesteh:2020:TMS

[SHA20] Behshid Shayesteh, Vesal Hakami, and Ahmad Akbari. A trust management scheme for IoT-enabled environmental health/accessibility monitoring services. *International Journal of Information Security*, 19(1): 93–110, February 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00446-x.

Sajedi:2009:SSB

[SJ09] Hedieh Sajedi and Mansour Jamzad. Secure steganography based on embedding capacity. *International Journal of Information Security*, 8(6): 433–445, December 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0089-y.

Sajedi:2010:UCT

[SJ10] Hedieh Sajedi and Mansour Jamzad. Using contourlet transform and cover selection for secure steganography. *International Journal of Information Security*, 9(5): 337–352, October 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-010-0112-3.

Sidiroglou:2006:ETD

[SK06] Stelios Sidiroglou and Angelos D. Keromytis. Execution transactions for defending against software failures: use and evaluation. *International Journal of Information Security*, 5(2):77–91, April 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-006-0083-6.

Shin:2014:AAA

[SK14] Sooyeon Shin and Taekyoung Kwon. AAnA: Anonymous authentication and authorization based on short traceable signatures. *International Journal of Information Security*, 13 (5):477–495, October 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0227-z.

Salini:2016:EPA

[SK16] P. Salini and S. Kanmani. Effectiveness and performance analysis of model-oriented security requirements engineering to elicit security requirements: a systematic solution for developing secure software systems. *International Journal of Information Security*, 15(3):319–334, June 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-015-0305-x`.

Sisaat:2017:STM

[SKK+17] Khamphao Sisaat, Surin Kittitornkun, Hiroaki Kikuchi, Chaxiong Yukonhiatou, Masato Terada, and Hiroshi Ishii. A spatio-temporal malware and country clustering algorithm: 2012 IIJ MITF case study. *International Journal of Information Security*, 16(5):459–473, October 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-016-0342-0`.

Lhee:2005:DFB

[sLC05] Kyung suk Lhee and Steve J. Chapin. Detection of file-based race conditions. *International Journal of Information Security*, 4(1–2):105–119, February 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-004-0068-2`.

Skoric:2010:FDS

[SM10] Boris Skorić and Marc X. Makkes. Flowchart description of security primitives for controlled physical unclonable functions. *International Journal of Information Security*, 9(5):327–335, October 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-010-0113-2`.

Smith:2004:OAP

[Smi04] Sean W. Smith. Outbound authentication for programmable secure coprocessors. *International Journal of Information Security*, 3(1):28–41, October 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-004-0033-0`.

Sole:2012:EMT

[SMMN12] Marc Solé, Victor Muntés-Mulero, and Jordi Nin.

Efficient microaggregation techniques for large numerical data volumes. *International Journal of Information Security*, 11(4): 253–267, August 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0158-5.

Snekkenes:2005:PSI

[Sne05] Einar Snekkenes. Preface to the special issue on ESORICS 2003. *International Journal of Information Security*, 4(3):133–134, June 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0054-8.

Stasinopoulos:2019:CAE

[SNX19] Anastasios Stasinopoulos, Christoforos Ntantogian, and Christos Xenakis. Commix: automating evaluation and exploitation of command injection vulnerabilities in Web applications. *International Journal of Information Security*, 18(1):49–72, February 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0399-z.

Stevanovic:2017:MIC

[SPDR17] Matija Stevanovic, Jens Myrup Pedersen, Alessandro D'Alconzo, and Stefan Ruehrup. A method for identifying compromised clients based on DNS traffic analysis. *International Journal of Information Security*, 16 (2):115–132, April 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0331-3.

Schreuders:2013:FBA

[SPM13] Z. Cliffe Schreuders, Christian Payne, and Tanya McGill. The functionality-based application confinement model. *International Journal of Information Security*, 12(5): 393–422, October 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0199-4.

Serjantov:2005:PAA

[SS05a] Andrei Serjantov and Peter Sewell. Passive-attack analysis for connection-based anonymity systems. *International Journal of Information Security*, 4 (3):172–180, June 2005. CODEN ???? ISSN 1615-5262 (print), 1615-

5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0059-3.

Skalka:2005:SUB

[SS05b] Christian Skalka and Scott Smith. Static use-based object confinement. *International Journal of Information Security*, 4(1–2):87–104, February 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0049-5.

Sampangi:2017:HSR

[SS17] Raghav V. Sampangi and Srinivas Sampalli. HiveSec: security in resource-constrained wireless networks inspired by beehives and bee swarms. *International Journal of Information Security*, 16(4):417–433, August 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0341-1.

Shameli-Sendi:2014:ACA

[SSD14] Alireza Shameli-Sendi and Michel Dagenais. ARITO: Cyber-attack response system using accurate risk impact tolerance. *International Journal of Information Security*, 13(4):367–390, August 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0222-9.

Spreitzenbarth:2015:MSC

[SSE+15] Michael Spreitzenbarth, Thomas Schreck, Florian Echtler, Daniel Arp, and Johannes Hoffmann. Mobile-Sandbox: combining static and dynamic analysis with machine-learning techniques. *International Journal of Information Security*, 14(2):141–153, April 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0250-0.

Seifi:2015:ATA

[SSFB15] Younes Seifi, Suriadi Suriadi, Ernest Foo, and Colin Boyd. Analysis of two authorization protocols using Colored Petri Nets. *International Journal of Information Security*, 14(3):221–247, June 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0243-z.

Silva:2015:RMP

[SSN15] Helber Silva, Aldri Santos, and Michele Nogueira. Routing management for performance and security tradeoff in wireless mesh networks. *International Journal of Information Security*, 14 (1):35–46, February 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-014-0246-9`.

Sepahi:2014:LBC

[SSP14] Reza Sepahi, Ron Steinfeld, and Josef Pieprzyk. Lattice-based certificateless public-key encryption in the standard model. *International Journal of Information Security*, 13 (4):315–333, August 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-013-0215-8`.

Susil:2016:SSA

[SSVC16] Petr Susil, Pouyan Sepehrdad, Serge Vaudenay, and Nicolas Courtois. On selection of samples in algebraic attacks and a new technique to find hidden low degree equations. *International Journal of Information Security*, 15 (1):51–65, February 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-015-0295-8`.

Saxena:2011:DRE

[SV11] Nitesh Saxena and Jonathan Voris. Data remanence effects on memory-based entropy collection for RFID systems. *International Journal of Information Security*, 10(4):213–222, August 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-011-0139-0`.

Takahashi:2020:MGE

[TCS+20] Takeshi Takahashi, Rodrigo Roman Castro, Bilhanan Silverajan, Ryan K. L. Ko, and Said Tabet. Message from the guest editors. *International Journal of Information Security*, 19(1):1–2, February 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-019-00472-9; http://link.springer.com/content/pdf/10.1007/s10207-019-00472-9.pdf`.

Trostle:2005:TIS

[TG05] Jonathan Trostle and Bill Gossman. Techniques for improving the security and manageability of IPsec policy. *International Journal of Information Security*, 4(3):209–226, June 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-004-0064-6`.

Tiloca:2017:IRD

[TGS17] Marco Tiloca, Christian Gehrmann, and Ludwig Seitz. On improving resistance to Denial of Service and key provisioning scalability of the DTLS handshake. *International Journal of Information Security*, 16(2):173–193, April 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-016-0326-0`.

Takase:2020:PIE

[TKKO20] Hayate Takase, Ryotaro Kobayashi, Masahiko Kato, and Ren Ohmura. A prototype implementation and evaluation of the malware detection mechanism for IoT devices using the processor information. *International Journal of Information Security*, 19 (1):71–81, February 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-019-00437-y`.

Tian:2009:LSN

[TLX09] Daxin Tian, Yanheng Liu, and Yang Xiang. Large-scale network intrusion detection based on distributed learning algorithm. *International Journal of Information Security*, 8(1):25–35, February 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-008-0061-2`.

Takahashi:2019:SSF

[TMM+19] Kenta Takahashi, Takahiro Matsuda, Takao Murakami, Goichiro Hanaoka, and Masakatsu Nishigaki. Signature schemes with a fuzzy private key. *International Journal of Information Security*, 18(5): 581–617, October 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-019-00428-z; http://link.springer.com/content/pdf/10.1007/s10207-019-00428-z.pdf`.

Tormo:2013:DAI

[TMP13] Ginés Dólera Tormo, Gabriel López Millán, and Gregorio Martínez Pérez. Definition of an advanced identity management infrastructure. *International Journal of Information Security*, 12 (3):173–200, June 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-012-0189-y`.

Tonicelli:2015:ITS

[TND+15] Rafael Tonicelli, Anderson C. A. Nascimento, Rafael Dowsley, Jörn Müller-Quade, Hideki Imai, Goichiro Hanaoka, and Akira Otsuka. Information-theoretically secure oblivious polynomial evaluation in the commodity-based model. *International Journal of Information Security*, 14 (1):73–84, February 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-014-0247-8`.

Toreini:2019:DEW

[TSMH19] Ehsan Toreini, Siamak F. Shahandashti, Maryam Mehrnezhad, and Feng Hao. DOMtegrity: ensuring web page integrity against malicious browser extensions. *International Journal of Information Security*, 18(6):801–814, December 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-019-00442-1; http://link.springer.com/content/pdf/10.1007/s10207-019-00442-1.pdf`.

Tsunoo:2006:ICA

[TTS+06] Yukiyasu Tsunoo, Etsuko Tsujihara, Maki Shigeri, Hiroyasu Kubo, and Kazuhiko Minematsu. Improving cache attacks by considering cipher structure. *International Journal of Information Security*, 5(3):166–176, July 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-005-0079-7`.

Tartary:2008:CAM

[TWP08] Christophe Tartary, Huaxiong Wang, and Josef Pieprzyk. A coding approach to the multicast stream authentication problem. *International Journal of Information Security*, 7(4): 265–283, August 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL

http://link.springer.com/article/10.1007/s10207-007-0048-4.

Teller:2004:UAC

[TZH04] David Teller, Pascal Zimmer, and Daniel Hirschkoff. Using ambients to control resources. *International Journal of Information Security*, 2(3–4):126–144, August 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0035-y.

Ustaoglu:2011:IIB

[Ust11] Berkant Ustaoğlu. Integrating identity-based and certificate-based authenticated key exchange protocols. *International Journal of Information Security*, 10(4):201–212, August 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0136-3.

Vajda:2016:ATA

[Vaj16] István Vajda. On the analysis of time-aware protocols in universal composability framework. *International Journal of Information Security*, 15(4):403–412, August 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0300-2.

Veeningen:2014:DMC

[VdWZ14] Meilof Veeningen, Benne de Weger, and Nicola Zannone. Data minimisation in communication protocols: a formal analysis framework and application to identity management. *International Journal of Information Security*, 13(6):529–569, November 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0235-z.

Vora:2019:KBP

[VH19] Aishwarya Vipul Vora and Saumya Hegde. Keyword-based private searching on cloud data along with keyword association and dissociation using cuckoo filter. *International Journal of Information Security*, 18(3):305–319, June 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0418-0.

Vasserman:2009:IKN

[VHT09] Eugene Y. Vasserman, Nicholas Hopper, and

James Tyra. SILENT-KNOCK: practical, provably undetectable authentication. *International Journal of Information Security*, 8(2):121–135, April 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-008-0070-1`.

Vrakas:2013:IDP

[VL13] Nikos Vrakas and Costas Lambrinoudakis. An intrusion detection and prevention system for IMS and VoIP services. *International Journal of Information Security*, 12 (3):201–217, June 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-012-0187-0`.

vonOheimb:2005:ASM

[vOLW05] David von Oheimb, Volkmar Lotz, and Georg Walter. Analyzing SLE 88 memory management security using Interacting State Machines. *International Journal of Information Security*, 4(3):155–171, June 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-004-0057-5`.

vanOorschot:2006:MSD

[vORM06] Paul C. van Oorschot, Jean-Marc Robert, and Miguel Vargas Martin. A monitoring system for detecting repeated packets with applications to computer worms. *International Journal of Information Security*, 5(3):186–199, July 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-006-0081-8`.

Vasiliadis:2015:GAM

[VPI15] Giorgos Vasiliadis, Michalis Polychronakis, and Sotiris Ioannidis. GPU-assisted malware. *International Journal of Information Security*, 14(3):289–297, June 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-014-0262-9`.

Vanrenen:2006:DSM

[VSM06] Gabriel Vanrenen, Sean Smith, and John Marchesini. Distributing security-mediated PKI. *International Journal of Information Security*, 5(1):3–17, January 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.`

com/article/10.1007/s10207-005-0076-x.

Valenzuela:2015:MAO

[VSR15] Michael Valenzuela, Ferenc Szidarovszky, and Jerzy Rozenblit. A multiresolution approach for optimal defense against random attacks. *International Journal of Information Security*, 14(1):61–72, February 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0245-x.

Wu:2009:IDV

[WAB+09] Yu-Sung Wu, Vinita Apte, Saurabh Bagchi, Sachin Garg, and Navjot Singh. Intrusion detection in voice over IP environments. *International Journal of Information Security*, 8(3):153–172, June 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-008-0071-0.

Waidner:2004:P

[Wai04] Michael Waidner. Preface. *International Journal of Information Security*, 3(1):1, October 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0051-y; http://link.springer.com/content/pdf/10.1007/s10207-004-0051-y.pdf.

Wang:2013:USM

[WGMB13] Pu Wang, Marta C. González, Ronaldo Menezes, and Albert-László Barabási. Understanding the spread of malicious mobile-phone programs and their damage potential. *International Journal of Information Security*, 12(5):383–392, October 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0203-z.

Wangen:2018:FEI

[WHS18] Gaute Wangen, Christoffer Hallstensen, and Einar Snekkenes. A framework for estimating information security risk assessment method completeness. *International Journal of Information Security*, 17(6):681–699, November 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0382-0; http://link.springer.com/content/pdf/10.1007/s10207-017-0382-0.pdf.

Wu:2014:SSP

[WLLW14] Tzong-Sun Wu, Ming-Lun Lee, Han-Yu Lin, and Chao-Yuan Wang. Shoulder-surfing-proof graphical password authentication scheme. *International Journal of Information Security*, 13(3):245–254, June 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0216-7.

Lye:2005:GSN

[wLW05] Kong wei Lye and Jeannette M. Wing. Game strategies in network security. *International Journal of Information Security*, 4(1–2):71–86, February 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-004-0060-x.

Wu:2019:TPP

[WMS+19] Ge Wu, Yi Mu, Willy Susilo, Fuchun Guo, and Futai Zhang. Threshold privacy-preserving cloud auditing with multiple uploaders. *International Journal of Information Security*, 18(3):321–331, June 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0420-6.

Wang:2018:VEC

[WPD18] Yujue Wang, HweeHwa Pang, and Robert H. Deng. Verifiably encrypted cascade-instantiable blank signatures to secure progressive decision management. *International Journal of Information Security*, 17(3):347–363, June 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0372-2.

Wang:2008:MLF

[WR08] XiaoFeng Wang and Michael K. Reiter. A multi-layer framework for puzzle-based denial-of-service defense. *International Journal of Information Security*, 7 (4):243–263, August 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0042-x.

Wei:2015:TPE

[WR15] Lei Wei and Michael K. Reiter. Toward practical encrypted email that supports private, regular-expression searches. *International Journal of Information Security*, 14(5): 397–416, October 2015.

CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0268-3; http://link.springer.com/content/pdf/10.1007/s10207-014-0268-3.pdf.

Wang:2016:SSE

[WT16] Yuyu Wang and Keisuke Tanaka. Strongly simulation-extractable leakage-resilient NIZK. *International Journal of Information Security*, 15(1):67–79, February 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0291-z.

Wu:2007:RFT

[WW07] Zhengping Wu and Alfred C. Weaver. Requirements of federated trust management for service-oriented architectures. *International Journal of Information Security*, 6(5):287–296, September 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0027-9.

Wang:2012:SGN

[WYL+12] Yuanzhuo Wang, Min Yu, Jingyuan Li, Kun Meng, Chuang Lin, and Xueqi Cheng. Stochastic game net and applications in security analysis for enterprise network. *International Journal of Information Security*, 11(1):41–52, February 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0148-z.

Wang:2007:HDA

[WZ07] Shujing Wang and Yan Zhang. Handling distributed authorization with delegation through answer set programming. *International Journal of Information Security*, 6(1):27–46, January 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-006-0008-4.

Xin:2012:RAA

[XCW+12] Zhi Xin, Huiyu Chen, Xinche Wang, Peng Liu, Sencun Zhu, Bing Mao, and Li Xie. Replacement attacks: automatically evading behavior-based software birthmark. *International Journal of Information Security*, 11(5):293–304, October 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL

http://link.springer.com/article/10.1007/s10207-012-0170-9.

Xu:2013:VBP

[XSA13] Wenjuan Xu, Mohamed Shehab, and Gail-Joon Ahn. Visualization-based policy analysis for SELinux: framework and user study. *International Journal of Information Security*, 12 (3):155–171, June 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0180-7.

Yu:2015:EPR

[YAM+15] Yong Yu, Man Ho Au, Yi Mu, Shaohua Tang, Jian Ren, Willy Susilo, and Liju Dong. Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage. *International Journal of Information Security*, 14(4):307–318, August 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0263-8.

Yu:2019:UUP

[YL19] Xiaoying Yu and Qi Liao. Understanding user passwords through password prefix and postfix (P3) graph analysis and visualization. *International Journal of Information Security*, 18(5): 647–663, October 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00432-3.

Yohan:2020:FSB

[YL20] Alexander Yohan and Nai-Wei Lo. FOTB: a secure blockchain-based firmware update framework for IoT environment. *International Journal of Information Security*, 19(3):257–278, June 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00467-6.

Yang:2018:NSS

[YLL+18] Zheng Yang, Chao Liu, Wanping Liu, Daigu Zhang, and Song Luo. A new strong security model for stateful authenticated group key exchange. *International Journal of Information Security*, 17(4): 423–440, August 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0373-1.

Yildirim:2019:EUI

[YM19] M. Yildirim and I. Mackie. Encouraging users to improve password security and memorability. *International Journal of Information Security*, 18(6): 741–759, December 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00429-y; http://link.springer.com/content/pdf/10.1007/s10207-019-00429-y.pdf.

Yoneyama:2018:FMR

[Yon18] Kazuki Yoneyama. Formal modeling of random oracle programmability and verification of signature unforgeability using task-PIOAs. *International Journal of Information Security*, 17(1):43–66, February 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0352-y.

Young:2006:CEU

[You06] Adam L. Young. Cryptoviral extortion using Microsoft's crypto API. *International Journal of Information Security*, 5(2): 67–76, April 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-006-0082-7.

Yoshino:2009:BMM

[YOV09] Masayuki Yoshino, Katsuyuki Okeya, and Camille Vuillaume. Bipartite modular multiplication with twice the bit-length of multipliers. *International Journal of Information Security*, 8(1):13–23, February 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-008-0060-3.

Yeo:2006:SWE

[YP06] Gary S.-W. Yeo and Raphael C.-W. Phan. On the security of the WinRAR encryption feature. *International Journal of Information Security*, 5 (2):115–123, April 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-006-0086-3.

Yaseen:2012:ITM

[YP12] Qussai Yaseen and Brajendra Panda. Insider threat mitigation: preventing unauthorized knowledge acquisition. *Inter-*

national Journal of Information Security, 11(4): 269–280, August 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0165-6.

Yasmin:2014:PSP

[YRW14] Rehana Yasmin, Eike Ritter, and Guilin Wang. Provable security of a pairing-free one-pass authenticated key establishment protocol for wireless sensor networks. *International Journal of Information Security*, 13(5): 453–465, October 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0224-7.

Yeh:2020:SIS

[YSD+20] Kuo-Hui Yeh, Chunhua Su, Robert H. Deng, Moti Yung, and Miroslaw Kutylowski. Special issue on security and privacy of blockchain technologies. *International Journal of Information Security*, 19 (3):243–244, June 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-020-00496-6; http://link.springer.com/content/pdf/10.1007/s10207-020-00496-6.pdf.

Yuen:2010:HCI

[YSM10] Tsz Hon Yuen, Willy Susilo, and Yi Mu. How to construct identity-based signatures without the key escrow problem. *International Journal of Information Security*, 9(4): 297–311, August 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-010-0110-5.

Yang:2016:MGE

[YSM16] Guomin Yang, Willy Susilo, and Yi Mu. Message from the Guest Editors. *International Journal of Information Security*, 15 (2):223–224, April 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0315-3; http://link.springer.com/content/pdf/10.1007/s10207-016-0315-3.pdf.

Yoneyama:2018:MCK

[YYK+18] Kazuki Yoneyama, Reo Yoshida, Yuto Kawahara, Tetsutaro Kobayashi, Hitoshi Fuji, and Tomohide Yamamoto. Multi-cast key

distribution: scalable, dynamic and provably secure construction. *International Journal of Information Security*, 17(5): 513–532, October 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0389-6.

Zhou:2006:MTI

[ZBD06] Jianying Zhou, Feng Bao, and Robert Deng. Minimizing TTP's involvement in signature validation. *International Journal of Information Security*, 5(1):37–47, January 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-005-0072-1.

Zhang:2007:FBT

[ZGC07] Jie Zhang, Ali A. Ghorbani, and Robin Cohen. A familiarity-based trust model for effective selection of sellers in multiagent e-commerce systems. *International Journal of Information Security*, 6(5): 333–344, September 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0025-y.

Zulkernine:2007:ISS

[ZGK07] Mohammad Zulkernine, Mathews Graves, and Muhammad Umair Ahmed Khan. Integrating software specifications into intrusion detection. *International Journal of Information Security*, 6(5): 345–357, September 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0023-0.

Zhou:2006:P

[ZL06] Jianying Zhou and Javier Lopez. Preface. *International Journal of Information Security*, 5(2): 65–66, April 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-006-0087-2.

Zhang:2019:FGA

[ZLGZ19] Tao Zhang, Wang Hao Lee, Mingyuan Gao, and Jianying Zhou. File Guard: automatic format-based media file sanitization. *International Journal of Information Security*, 18(6): 701–713, December 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.

com/article/10.1007/s10207-019-00440-3.

Zhou:2020:IFV

[ZLJW20] Yuanjian Zhou, Yining Liu, Chengshun Jiang, and Shulan Wang. An improved FOO voting scheme using blockchain. *International Journal of Information Security*, 19(3):303–310, June 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00457-8.

Zhou:2012:MGE

[ZLL12] Jianying Zhou, Xuejia Lai, and Hui Li. Message from the Guest Editors. *International Journal of Information Security*, 11(5): 291–292, October 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0172-7; http://link.springer.com/content/pdf/10.1007/s10207-012-0172-7.pdf.

Zheng:2007:DSL

[ZM07] Lantian Zheng and Andrew C. Myers. Dynamic security labels and static information flow control. *International Journal of Information Security*, 6(2–3):67–84, March 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-007-0019-9.

Zakerzadeh:2013:DSA

[ZO13] Hessam Zakerzadeh and Sylvia L. Osborn. Delay-sensitive approaches for anonymizing numerical streaming data. *International Journal of Information Security*, 12(5): 423–437, October 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-013-0196-7.

Zhang:2014:DFA

[ZRJ14] Meng Zhang, Anand Raghunathan, and Niraj K. Jha. A defense framework against malware and vulnerability exploits. *International Journal of Information Security*, 13(5): 439–452, October 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0233-1.

Zhou:2015:GCR

[ZVH15] Lan Zhou, Vijay Varadharajan, and Michael Hitchens. Generic constructions for role-based encryption. *Interna-*

tional Journal of Information Security, 14(5): 417–430, October 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0267-4.

Zhang:2017:CIB

[ZWQ+17] Lei Zhang, Qianhong Wu, Bo Qin, Hua Deng, Jiangtao Li, Jianwei Liu, and Wenchang Shi. Certificateless and identity-based authenticated asymmetric group key agreement. *International Journal of Information Security*, 16(5): 559–576, October 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0339-8.

Zhang:2020:CBE

[ZWX20] Shufan Zhang, Lili Wang, and Hu Xiong. Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability. *International Journal of Information Security*, 19 (3):323–341, June 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-019-00465-8.

Zhu:2011:SLA

[ZXZ+11] Wen Tao Zhu, Yang Xiang, Jianying Zhou, Robert H. Deng, and Feng Bao. Secure localization with attack detection in wireless sensor networks. *International Journal of Information Security*, 10 (3):155–171, June 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-011-0127-4.

Zheng:2019:IDR

[ZZG19] Jian-Wu Zheng, Jing Zhao, and Xin-Ping Guan. Identifier discrimination: realizing selective-ID HIBE with authorized delegation and dedicated encryption privacy. *International Journal of Information Security*, 18 (2):141–162, April 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0402-8.

Zhao:2008:NAP

[ZZH08] Chang-An Zhao, Fangguo Zhang, and Jiwu Huang. A note on the Ate pairing. *International Journal of Information Security*, 7(6): 379–382, November 2008. CODEN ???? ISSN

1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-008-0054-1.

Zheng:2010:AAB

[ZZW+10] Ruijuan Zheng, Mingchuan Zhang, Qingtao Wu, Shibao Sun, and Jiexin Pu. Analysis and application of Bio-Inspired Multi-Net Security Model. *International Journal of Information Security*, 9(1):1–17, February 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0091-4.