A PC-based CAD system for training digital test
Ubar, Raimund-Johannes; **Buldas, Ahto**; Paomets, Priidu; Raik, Jaan; **Tulit, Viljar** The Fifth EUROCHIP Workshop on VLSI Design Training, 17-18-19 October 1994, Dresden, Germany 1994 / p. 152-157: ill

A semi-formal method for security estimation
Buldas, Ahto; Priisalu, Jaan Databases and information systems : proceedings of the Second International Baltic Workshop : Tallinn, June 12-14, 1996. Volume 1, Research track 1996 / p. 206-212

A VLSI implementation of RSA and IDEA encryption engine
Buldas, Ahto; **Põldre, Jüri** Proceedings [of the] 15th NORCHIP Conference, Tallinn, 10-11 November 1997 1997 / p. 281-288: ill

Ajatembeldusel on maailmas tulevikku : [küsimustele vastab noore teadlase preemia pälvinud Ahto Buldas]
Sootak, Varje; **Buldas, Ahto** Universitas Tartuensis 2002 / 20. dets., lk. 5 : fot

Ajatemplid digitaaldokumentidel
Buldas, Ahto; Lipmaa, Helger Arvutimaailm 1998 / 2, lk. 45-47: ill

Ajatemplisüsteemid : avalik loeng 30. mail 2001 TTÜs
Buldas, Ahto Tallinna Tehnikaülikooli aastaraamat 2001 2003 / lk. 308-312

Algoritmid ja diagonaalsed tõestused
Buldas, Ahto Arvutustehnika ja Andmetöötlus 1995 / 1, lk. 5-10

Allkirjad elektroonilistel dokumentidel : vääramatu tõenduse algoritmidest
Buldas, Ahto A & A 2000 / 6, lk. 36-40

An algebraic approach to the structure of graphs
Buldas, Ahto 1999 http://www.ester.ee/record=b1273064*est

Are the current system engineering practices sufficient to meet cyber crime?
Buldas, Ahto; Saarepera, Märt Human Aspects of Information Security, Privacy and Trust : 5th International Conference, HAS 2017 : held as part of HCI International 2017, Vancouver, BC, Canada, July 9–14, 2017 : proceedings 2017 / p. 451-463 https://doi.org/10.1007/978-3-319-58460-7_31 Conference proceedings at Scopus Article at Scopus Article at WOS

Attribute evaluation on attack trees with incomplete information
Buldas, Ahto; Gadyatskaya, Olga; **Lenin, Aleksandr**; **Mauw, Sjouke**; **Trujillo-Rasua, Roland** Computers & Security 2020 / art. 101630, 17 p. : ill https://doi.org/10.1016/j.cose.2019.101630 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Attribute evaluation on attack trees with incomplete information : a preprint
Buldas, Ahto; Gadyatskaya, Olga; **Lenin, Aleksandr**; Mauw, Sjouke; Trujillo-Rasua, Roland arXiv.org 2019 / 21 p. : ill http://arxiv.org/abs/1812.10754

Black-box separations and their adaptability to the non-uniform model
Buldas, Ahto; Niitsoo, Margus Information security and privacy : 18th Australasian Conference, ACISP 2013, Brisbane, Australia, July 1-3, 2013 : proceedings 2013 / p. 152-167 https://doi.org/10.1007/978-3-642-39059-3_11 Conference Proceedings at Scopus Article at Scopus

Blockchain technology: Intrinsic technological and socio-economic barriers: FDSE'2020 Keynote
Buldas, Ahto; **Draheim, Dirk**; Nagumo, Takehiko; **Vedešin, Anton** Future Data and Security Engineering. Big Data, Security and Privacy, Smart City and Industry 4.0 Applications : 7th International Conference, FDSE 2020, Quy Nhon, Vietnam, November 25–27, 2020 : proceedings 2020 / p. 3-27 https://doi.org/10.1007/978-3-030-63924-2_1 Conference Proceedings at Scopus Article at Scopus

A blockchain-assisted hash-based signature scheme
Buldas, Ahto; **Laanoja, Risto**; **Truu, Ahto** Secure IT Systems : 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28–30, 2018 : proceedings 2018 / p. 138–153 : ill https://doi.org/10.1007/978-3-030-03638-6_9 Conference Proceedings at Scopus Article at Scopus Conference Proceedings at WOS Article at WOS

Bounded pre-image awareness and the security of hash-tree keyless signatures
Buldas, Ahto; **Laanoja, Risto**; Laud, Peeter; Truu, Ahto Provable security : 8th International Conference, ProvSec 2014, Hong Kong, China, October 9-10, 2014 : proceedings 2014 / p. 130-145 : ill https://doi.org/10.1007/978-3-319-12475-9_10 Conference proceeding at Scopus Article at Scopus Conference proceeding at WOS Article at WOS

Comparability graphs and the structure of finite graphs
Buldas, Ahto Proceedings of the Estonian Academy of Sciences. Physics. Mathematics 1996 / 2/3, p. 117-127

Congruence lattice of a graph
Buldas, Ahto Proceedings of the Estonian Academy of Sciences. Physics. Mathematics 1997 / 3, p. 155-170: ill

Does secure time-staming imply collision-free hash functions
Buldas, Ahto; **Jürgenson, Aivo** Info- ja kommunikatsioonitehnoloogia doktorikooli IKTDK kolmanda aastakonverentsi artiklite kogumik : 25.-26. aprill 2008, Voore külalistemaja 2008 / p. 59-63 : ill

Does secure time-stamping imply collision-free hash functions?
Buldas, Ahto; Jürgenson, Aivo Lecture notes in computer science 2007 / p. 138-150

Eesti Vabariigi 2018. aasta teaduspreemia laureaadid TTÜst
Vähi, Kersti; **Buldas, Ahto**; **Kotta, Ülle**; **Kurnitski, Jarek**; **Raudla, Ringa** Mente et Manu 2018 / lk. 26-27 : portr
https://www.ttu.ee/ttu-uudised/ajaleht-mente-et-manu/mente-et-manu/ http://www.ester.ee/record=b1242496*est
https://artiklid.elnet.ee/record=b2836028*est

Eestis arendatud plokiahel soovib saada maailmaturu liidriks
Rumm, Hannes Eesti Ekspress 2023 / lk. 30-33 https://dea.digar.ee/article/eestiekspress/2023/05/10/13.6

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

Efficient long-term validation of digital signatures
Ansper, A.; **Buldas, Ahto**; Roos, Meelis; Willemson, Jan Public Key Cryptography : 4th International Workshop on Practice and Theory in Public Key Cryptosystems : PKC 2001 : Cheju Island, Korea, February 13-15, 2001 : proceedings 2001 / p. 13-15

Efficient semantics of parallel and serial models of attack trees = Ründepuude paralleel- ja jadamudelite efektiivsed semantikad
Jürgenson, Aivo 2010 https://www.ester.ee/record=b2604924*est

Electronic signature system with small number of private keys
Buldas, Ahto; Saarepera, Märt 2nd Annual PKI Research Workshop Pre-Proceedings : Gaithersburg, Maryland, USA, April 28-29, 2003 2003 / p. 96-108 https://www.researchgate.net/publication/2869630_Electronic_Signature_System_with_Small_Number_of_Private_Keys

Elektrondokumendid tõendusmaterjalina
Buldas, Ahto Arvutimaailm 1997 / 8, lk. 23-25: ill

Eliminating counterevidence with applications to accountable certificate management
Buldas, Ahto; Laud, Peeter; Lipmaa, Helger Journal of computer security 2002 / 3, p. 273-296
https://content.iospress.com/articles/journal-of-computer-security/jcs161

Goodsteini teoreemist
Buldas, Ahto Arvutustehnika ja Andmetöötlus 1995 / 4, lk. 2-6

Graafid
Buldas, Ahto; Laud, Peeter; Villemson, Jan 2003 https://www.ester.ee/record=b1804744*est

Graafid
Buldas, Ahto; Laud, Peeter; Villemson, Jan 2008 https://www.ester.ee/record=b2345899*est

Graafid ja järjestused
Buldas, Ahto Arvutustehnika ja Andmetöötlus 1995 / 2, lk. 2-8: ill

Graphs and lattice varieties
Buldas, Ahto Proceedings of the Estonian Academy of Sciences. Physics. Mathematics 1998 / 2, p. 100-109

Hash-based server-assisted digital signature solutions = Räsifunktsioonidel põhinevad serveri toega digitaalse signeerimise lahendused
Truu, Ahto 2020 https://digikogu.taltech.ee/et/Item/a972cc4b-53ec-4c82-8de0-b3e941cce345

Improving the availability of time-stamping services
Ansper, A.; **Buldas, Ahto**; Saarepera, Märt; Willemson, Jan Information Security and Privacy : 6th Australian Conference : ACISP 2001 : Sydney, Australia, July 11-13, 2001 : proceedings 2001 / p. 360-375 https://link.springer.com/chapter/10.1007/3-540-47719-5_29

Infosüsteemide turve
Hanson, Vello; **Buldas, Ahto** 1997 https://www.ester.ee/record=b1059903*est

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

Keyless signature infrastructure and PKI : hash-tree signatures in pre- and post-quantum world
Buldas, Ahto; **Laanoja, Risto**; **Truu, Ahto** International journal of services technology and management 2017 / p. 117-130 : ill https://doi.org/10.1504/IJSTM.2017.10002708 Journal metrics at Scopus Article at Scopus

Keyless signatures' infrastructure: How to build global distributed hash-trees
Buldas, Ahto; Kroonmaa, Andres; **Laanoja, Risto** Secure IT Systems : 18th Nordic Conference, NordSec 2013, Ilulissat, Greenland, October 18-21, 2013, Proceedings 2013 / p. 313 - 320 https://doi.org/10.1007/978-3-642-41488-6_21 Conference Proceedings at Scopus Article at Scopus

Knowledge-binding commitments with applications in time-stamping
Buldas, Ahto; Laur, Sven Lecture notes in computer science 2007 / p. 150-165 https://eprint.iacr.org/2007/071

Krüptoloogia. Miks ja kuidas?
Buldas, Ahto Arvutimaailm 1994 / 3, lk. 14-15

Laboratory course for training "Digital design and test"
Ubar, Raimund-Johannes; **Tulit, Viljar**; Buldas, Ahto; **Saarepera, Märt** Fourth EUROCHIP Workshop on VLSI Design Training, 29 September to 1 October 1993, Toledo : [proceedings] 1993 / p. 112-117: ill

Limiting adversarial budget in quantitative security assessment
Lenin, Aleksandr; **Buldas, Ahto** Decision and Game Theory for Security : 5th International Conference, GameSec 2014, Los Angeles, CA, USA, November 6-7, 2014 : proceedings 2014 / p. 155-174 : ill https://doi.org/10.1007/978-3-319-12601-2_9 Conference proceedings at Scopus Article at Scopus Conference proceedings at WOS Article at WOS

Long term archiving of electronic signatures
Buldas, Ahto; Freudenthal, Margus Baltic ITAMPT review 2004 / 1, p. 69-74 : ill

Long-term secure commitments via extractable-binding commitments
Buldas, Ahto; Geihs, Matthias; Buchmann, Johannes Information Security and Privacy : 22nd Australasian Conference, ACISP 2017, Auckland, New Zealand, July 3–5, 2017 : Proceedings, Part I 2017 / p. 65-81 https://doi.org/10.1007/978-3-319-60055-0_4 Conference proceedings at Scopus Article at Scopus Article at WOS

Long-term secure time-stamping using preimage-aware hash functions : (short version)
Buldas, Ahto; Geihs, Matthias; Buchmann, Johannes Provable Security : 11th International Conference, ProvSec 2017, Xi'an, China, October 23–25, 2017 : proceedings 2017 / p. 251-260 : ill http://doi.org/10.1007/978-3-319-68637-0_15 Conference proceedings at Scopus Article at Scopus Article at WOS

Loogikaskeemid ja binaardiagrammid
Buldas, Ahto Aastaraamat 1994 - 1996 / Eesti Matemaatika Selts 1999 / lk. 6-11

Mikroarvuti plastkaardis
Buldas, Ahto; Lakspere, Enn; Priisalu, Jaan Arvutimaailm 1994 / 4, lk. 52-55; 5, lk. 28-31; 6, lk. 42-43; 7, lk. 51-53 https://artiklid.elnet.ee/record=b2019361*est

Mis on p-aadilised arvud?
Buldas, Ahto Arvutustehnika ja Andmetöötlus 1995 / 9, lk. 2-8

A New approach to constructing digital dignature schemes
Buldas, Ahto; **Frisov, Denis**; **Laanoja, Risto**; Lakk, Henri; **Truu, Ahto** Advances in Information and Computer Security : 14th International Workshop on Security, IWSEC 2019, Tokyo, Japan, August 28–30, 2019 : proceedings 2019 / p. 363-373 https://doi.org/10.1007/978-3-030-26834-3_21 Conference proceeding at Scopus Article at Scopus Conference proceeding at WOS Article at WOS

New efficient utility upper bounds for the fully adaptive model of attack trees
Buldas, Ahto; **Lenin, Aleksandr** Decision and game theory for security : 4th International Conference, GameSec 2013, Fort Worth, TX, USA, November 11-12, 2013 : proceedings 2013 / p. 192-205 : ill https://doi.org/10.1007/978-3-319-02786-9_12 Computer Proceedings metrics at Scopus Article at Scopus

New linking schemes for digital time-stamping
Buldas, Ahto; Laud, Peeter Proceedings of the CISC'98, Seoul, Korea 1998 / p. 112-123 https://citeseerx.ist.psu.edu/document?

repid=rep1&type=pdf&doi=d3a005fb546ff78abc6ee453af4ee91aa6267c50

On provably secure time-stamping schemes
Buldas, Ahto; Saarepera, Märt Advances in cryptology - ASIACRYPT 2004 : 10th International Conference on the Theory and Application of Cryptology and Information Security : Jeju Island, Korea, December 5-9, 2004 : proceedings 2004 / p. 500-514 : ill https://link.springer.com/chapter/10.1007/978-3-540-30539-2_35

Oracle separation in the non-uniform model
Buldas, Ahto; Laur, Sven; Niitsoo, Margus Provable Security : Third International Conference : ProvSec 2009 : Guangzhou, China, November 11-13, 2009 : proceedings 2009 / p. 230-244 https://link.springer.com/content/pdf/10.1007/978-3-642-04642-1_19.pdf

Practical security analysis of e-voting systems
Buldas, Ahto; Mägi, Triinu Lecture notes in computer science 2007 / p. 320-335

Preemia olulise sotsiaal-majandusliku mõjuga innovaatilise tooteni viinud teaduslikul avastusel põhineva teadus- ja arendustöö eest : Ahto Buldas. Minu teadus : usaldus, saladused, aeg ja plokiahelad
Buldas, Ahto Eesti Vabariigi preemiad 2018 : teadus. F. J. Wiedemanni keeleauhind. Kultuur. Sport 2018 / lk. 64-75 : portr

Rational choice of security measures via multi-parameter attack trees
Buldas, Ahto; Laud, Peeter; Priisalu, Jaan; Saarepera, Märt; Willemson, Jan 1st International Workshop on Critical Information Infrastructures Security : Samos Island, Greece, August 30 - September 2, 2006 2006 / p. 232-243 https://link.springer.com/chapter/10.1007/11962977_19

Reliable and efficient determination of the likelihood of rational attacks = Ratsionaalsete rünnete tõepära efektiivne ja usaldusväärne kindlakstegemine
Lenin, Aleksandr 2015 https://www.ester.ee/record=b4530005*est

Secure and efficient implementation of electronic money
Buldas, Ahto; **Draheim, Dirk**; Saarepera, Märt Future Data and Security Engineering : Big Data, Security and Privacy, Smart City and Industry 4.0 Applications : 9th International Conference, FDSE 2022, Ho Chi Minh City, Vietnam, November 23-25, 2022 : proceedings 2022 / p. 34-51 https://doi.org/10.1007/978-981-19-8069-5_3 Conference proceedings at Scopus Article at Scopus Article at WOS

Security proofs for hash tree time-stamping using hash functions with small output size
Buldas, Ahto; **Laanoja, Risto** Information security and privacy : 18th Australasian Conference, ACISP 2013, Brisbane, Australia, July 1-3, 2013 : proceedings 2013 / p. 235-250 : ill https://doi.org/10.1007/978-3-642-39059-3_16 Conference Proceedings at Scopus Article at Scopus

A server-assisted hash-based signature scheme
Buldas, Ahto; **Laanoja, Risto**; **Truu, Ahto** Secure IT Systems : 22nd Nordic Conference, NordSec 2017, Tartu, Estonia, November 8-10, 2017 : proceedings 2017 / p. 3-17 : ill https://doi.org/10.1007/978-3-319-70290-2_1 Conference proceedings at Scopus Article at Scopus Article at WOS

Server-supported RSA signatures for mobile devices
Buldas, Ahto; Kalu, Aivo; Laud, Peeter; Oruaas, Mart Computer Security - ESORICS 2017 : 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11–15, 2017 : proceedings, part I 2017 / p. 315-333 : ill https://doi.org/10.1007/978-3-319-66402-6_19 Conference proceedings at Scopus Article at Scopus Article at WOS

Simple infeasibility certificates for attack trees
Buldas, Ahto; **Lenin, Aleksandr**; Villemson, Jan; **Charnamord, Anton** Advances in Information and Computer Security : 12th International Workshop on Security, IWSEC 2017, Hiroshima, Japan, August 30 – September 1, 2017 : proceedings 2017 / p. 39-55 : ill https://doi.org/10.1007/978-3-319-64200-0_3 Conference proceedings at Scopus Article at Scopus Article at WOS

Sissejuhatus matroidide teooriasse
Buldas, Ahto Arvutustehnika ja Andmetöötlus 1995 / 3, lk. 2-5: ill

A systematic approach to offensive volunteer cyber militia
Ottis, Rain 2011 http://www.ester.ee/record=b2685353*est

Teadusest, ärist ja impeeriumi pärandusest
Buldas, Ahto A & A 2001 / 4, lk. 5-8 https://www.ester.ee/record=b1071898*est

A theory of secure and efficient implementation of electronic money
Buldas, Ahto; **Draheim, Dirk**; Saarepera, Märt SN Computer Science 2023 / art. 861, 25 p. : ill https://doi.org/10.1007/s42979-023-02232-y Journal metrics at Scopus Article at Scopus

Time-stamping with binary linking schemes
Buldas, Ahto; Laud, Peeter; Lipmaa, Helger; Willemson, Jan Advances in Cryptology : CRYPTO'98 : 18th Annual International Cryptology Conference, Santa Barbara, California, USA August 23–27, 1998 : proceedings 1998 / p. 486-501 : ill

Towards a foundation of Web3
Buldas, Ahto; **Draheim, Dirk**; Gault, Mike; Saarepera, Märt Future Data and Security Engineering : Big Data, Security and Privacy, Smart City and Industry 4.0 Applications : 9th International Conference, FDSE 2022, Ho Chi Minh City, Vietnam, November 23-25, 2022 : proceedings 2022 / p. 3-18 https://doi.org/10.1007/978-981-19-8069-5_1 Conference proceedings at Scopus Article at Scopus Article at WOS

TURBO TESTER : a set of software tools for CAD of test for digital circuits
Ubar, Raimund-Johannes; **Tulit, Viljar**; **Buldas, Ahto**; **Saarepera, Märt** Fourth EUROCHIP Workshop on VLSI Design Training, 29 September to 1 October 1993, [Toledo] 1993 / p. 396

An ultra-scalable blockchain platform for universal asset tokenization : design and implementation
Buldas, Ahto; **Draheim, Dirk**; Gault, Mike; Laanoja, Risto; Nagumo, Takehiko; Saarepera, Märt; Shah, Syed Attique; Simm, Joosep; Steiner, Jamie; **Tammet, Tanel**; Truu, Ahto IEEE Access 2022 / p. 77284-77322 : ill https://doi.org/10.1109/ACCESS.2022.3192837 Journal metrics at Scopus Article at Scopus Journal metrics at WOS Article at WOS

Undeniable replies for database queries
Buldas, Ahto; Roos, Meelis; Willemson, Jan Databases and information systems : proceedings of the Fifth International Baltic Conference : Baltic DB & IS 2002 : Tallinn, June 3-6, 2002. Vol. 2 2002 / p. 215-226 : ill

Undeniable replies for database queries
Buldas, Ahto; Roos, Meelis; Willemson, Jan Databases and information systems. II, Fifth International Baltic Conference : Baltic DB & IS'2002 : Tallinn, Estonia, June 3-6, 2002 : selected papers 2002 / p. 43-54 : ill

A unifying theory of electronic money and payment systems
Buldas, Ahto; Saarepera, Märt; Steiner, Jamie; **Draheim, Dirk** techrxiv.org 2021 https://doi.org/10.36227/techrxiv.14994558.v2

Universally composable time-stamping schemes with audit
Buldas, Ahto; Laud, Peeter; Saarepera, Märt; Villemson, Jan Lecture notes in computer science 2005 / p. 359-373 https://link.springer.com/chapter/10.1007/11556992_26

Vastab Eesti parim noor teadlane anno 2002 [Ahto Buldas]
Buldas, Ahto; **Ummelas, Mart** Mente et Manu 2002 / 19. nov., lk. 1, 2 https://www.ester.ee/record=b1242496*est

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

Ühispanga tõhus toetus ülikoolispordile : [31. okt. sõlmisid TTÜ ja Eesti Ühispank ülikoolisporti toetava sponsorlepingu : leping allkirjastati digitaalallkirjaga : kommenteerivad Gunnar Valge ja Ahto Buldas]
Valge, Gunnar; **Buldas, Ahto** Mente et Manu 2002 / 5. nov., lk. 1 : ill https://www.ester.ee/record=b1242496*est

Ühissalastuse skeemid
Buldas, Ahto; **Leibak, Alar** Arvutimaailm 1997 / 2, lk. 30-31