

### **A user interface for a game-based protocol verification tool**

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

### **Application of dependency graphs to security protocol analysis**

**Tšahhirov, Ilja**; Laud, Peeter Symposium on Trustworthy Global Computing : Sophia-Antipolis, France, November 5-6, 2007 2007 / ? p [https://link.springer.com/chapter/10.1007/978-3-540-78663-4\\_20](https://link.springer.com/chapter/10.1007/978-3-540-78663-4_20)

### **Application of dependency graphs to security protocol analysis**

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

### **Attribute-based encryption for named data networking**

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

### **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](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](#)

### **CACS: A cloud privacy-preserving attribute management system**

Kalu, Aivo; Kus, Burak Can; Laud, Peeter; Leung, Kin Long; **Snetkov, Nikita**; **Vakarjuk, Jelizaveta** Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES), Benevento Italy, 29 August 2023 - 1 September, 2023 2023 / art. 122, p. 1-9 <https://doi.org/10.1145/3600160.3605022>

### **A comparison-based methodology for the security assurance of novel systems**

**Laud, Peeter**; **Vakarjuk, Jelizaveta** ESORICS 2022: Computer Security. ESORICS 2022 International Workshops : conference proceedings 2023 / p. 625-644 [https://doi.org/10.1007/978-3-031-25460-4\\_36](https://doi.org/10.1007/978-3-031-25460-4_36)

### **Digital signature in automatic analyses for confidentiality against active adversaries**

**Tšahhirov, Ilja**; Laud, Peeter NORDSEC 2005 : proceedings of the 10th Nordic Workshop on Secure IT Systems October 20-21, 2005, Tartu, Estonia 2005 / p. 29-41

### **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>

### **Elutähtsate teenuste ristsõltuvuse analüüs**

Laud, Peeter; **Bahsi, Hayretidin**; **Lenin, Aleksandr**; Mändmaa, Kalev; **Priisalu, Jaan**; Tuuling, Reedik Sõjateadlane 2020 / lk. 207-237 [https://www.ester.ee/record=b4555087\\*est](https://www.ester.ee/record=b4555087*est)

### **Graafid**

**Buldas, Ahto**; Laud, Peeter; Villemson, Jan 2003 [https://www.ester.ee/record=b1804744\\*est](https://www.ester.ee/record=b1804744*est)

### **Graafid**

**Buldas, Ahto**; Laud, Peeter; Villemson, Jan 2008 [https://www.ester.ee/record=b2345899\\*est](https://www.ester.ee/record=b2345899*est)

### **Identifying obstacles of PQC migration in e-Estonia**

**Vakarjuk, Jelizaveta**; **Snetkov, Nikita**; Laud, Peeter 2024 16th International Conference on Cyber Conflict: Over the Horizon (CyCon) 2024 / p. 63-81 <https://doi.org/10.23919/CyCon62501.2024.10685570> [Article at Scopus](#)

### **Mapping the information flows for the architecture of a nationwide situation awareness system : (Poster)**

**Bahsi, Hayretidin**; Dieves, Veiko; **Kangilaski, Taivo**; Laud, Peeter; **Mõtus, Leo**; Murumets, Jaan; Ploom, Illimar; **Priisalu, Jaan**; Seeba, Mari; **Täks, Ermo**; Tammel, Kaide; **Tamppuu, Piia**; **Taveter, Kuldar**; Trumm, Avo; Truusa, Tiia-Triin; Vihalemm, Triin Proceedings 2019 IEEE International Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA) : Las Vegas, NV, USA, 8-11 April 2019 2019 / p. 152–157 <https://doi.org/10.1109/COGSIMA.2019.8724167>

### **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>

### **Rational choice of security measures via multi-parameter attack trees**

**Buldas, Ahto**; Laud, Peeter; **Priisalu, Jaan**; Saarepera, Märt; Villemson, 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](https://link.springer.com/chapter/10.1007/11962977_19)

**Server-supported decryption for mobile devices**

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

**Server-supported RSA signatures for mobile devices**

**Buldas, Ahto**; Kalu, Aivo; Laud, Peeter; Oruaas, Mart Computer Security - ESORICS 2017 : 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11–15, 2017 : proceedings, part I 2017 / p. 315-333 : ill [https://doi.org/10.1007/978-3-319-66402-6\\_19](https://doi.org/10.1007/978-3-319-66402-6_19) [Conference proceedings at Scopus](#) [Article at Scopus](#) [Article at WOS](#)

**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

**TOPCOAT: towards practical two-party Crystals-Dilithium**

**Snetkov, Nikita**; **Vakarjuk, Jelizaveta**; Laud, Peeter Discover computing 2024 / art. 18, 31 p. <https://doi.org/10.1007/s10791-024-09449-2> [Journal metrics at Scopus](#) [Article at Scopus](#) [Article at WOS](#)

**Type systems equivalent to dataflow analyses for imperative languages**

Laud, Peeter; **Uustalu, Tarmo**; **Vene, Varmo** Proceedings of 3rd APPSEM II Workshop : APPSEM'05 : Frauenchiemsee, September 2005 2005 / [12] p <https://www.sciencedirect.com/science/article/pii/S0304397506005524>

**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](https://link.springer.com/chapter/10.1007/11556992_26)