AKADEEMIKUTE VALIMINE 2021 ESILDISTE ALUSEL

Tehnika- ja arvutiteadused

Peeter LAUD

ESITAJAD
Akadeemikud J. Vilo, T. Uustalu, Ü. Jaaksoo ja Cybernetica AS nõukogu

SÜNDINUD 06. aprillil 1977

HARIDUS, TEADUSKRAAD
1997 Tartu ülikool (informaatika)
1998 MSc (informaatika), Tartu ülikool
2002 PhD (inseneriteadused), Saarimaa ülikool, Saksamaa

TEENISTUSKÄIK
1998–1999 Cybernetica ASi teadur, 2002-2008 vanemteadur, 2008-2021 teadusdirektor, alates 2021 vanemteadur; 1999-2000 Saarimaa ülikooli teaduslik töötaja; 2002-2012 Tartu ülikooli erakorraline teadur, vanemteadur, dotsent, professor, alates 2019 külalisprofessor

ENESETÄIENDAMINE VÄLISMAAL
1999–2002 Saarimaa ülikool, doktorantuur

PEAMISED UURIMISVALDKONNAD
Programmide, protokollide, suurte süsteemide turvalisus ja privaatsus - analüüs ja konstruktsioonid; diferentsiaalprivaatsus; turvalised ühisarvutused

KEHTIVAD PROJEKTID
PROVENANCE - Proofs and Verifications between Governments and Citizens
Eesti IKT tippkeskus EXCITE (SA Archimedes)
CyberSec4Europe (Euroopa Komisjon, H2020)
Nullteadmustõestused ja suveräänidentiteet (Cybernetica AS)

JUHENDAMINE (kaitstud väitekirjade arv)
4 doktorit, 15 magistrit

ÜHISKONDLIK TEGEVUS
Riigi infosüsteemi ameti ja kaitseministeeriumi tellitud infoturbe-alaste aruannete koostamine (nn krüptouuringud)
Praktikutele suunatud ettekanded konkreetsete tulemuste või projektide kohta (enamjaolt Mobiil-ID turvaanalüüsist)

TUNNUSTUSED
2011 Parima artikli auhind (infosüsteemide ala) konverentsil ACM Symposium on Applied Computing 2011
2011 Vabariigi Presidendi kultuurirahastu noore teadlase preemia
2003 Euroopa programmeerimiskeelte ja -süsteemide (EAPLS) auhind parima artikli eest kobarkonverentsil ETAPS '03

BIBLIOMEETRILISED ANDMED

Otsingutulemused seisuga 06.10.2021

Publikatsioonide arv, viidete arv, h-indeks (esildise alusel)	***Web of Science*** 1990–2021 ––––––––––––– ***Google Scholar*** (kõik)			***Web of Science*** 2011–2021	
	Publ. arv	Viidete arv	H-indeks	Publ. arv	Viidete arv
kokku 103	59 / 112	402 / 1889	10 / 22	39	67

KÜMME TÄHTSAMAT PUBLIKATSIOONI

Publikatsioonide üldarv: 103

Dumas, M., García-Bañuelos, L., Jääger, J., Laud, P., Matulevičius, R., Pankova, A., Pettai, M., Pullonen-Raudvere, P., Toots, A., Tuuling, R., Yerokhin, M. Multi-level privacy analysis of business processes: the Pleak toolset. − International Journal on Software Tools for Technology Transfer, 2021. https://doi.org/10.1007/s10009-021-00636-w

Laud, P., Pankova, A., Pettai, M. A framework of metrics for differential privacy from local sensitivity. − Proceedings on Privacy Enhancing Technologies, 2020, 2, 175-208. https://doi.org/10.2478/popets-2020-0023

Buldas, A., Kalu, A., Laud, P., Oruaas, M. Server-supported RSA signatures for mobile devices. − Foley, S.N. *et al*. (eds). Computer Security - ESORICS 2017 : 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part I, 10492. Cham: Springer, 2017, 315–333. (Lecture Notes in Computer Science; 10492). https://doi.org/10.1007/978-3-319-66402-6_19

Laud, P., Pankova, A., Jagomägis, R. Preprocessing based verification of multiparty protocols with honest majority. − Proceedings on Privacy Enhancing Technologies, 2017, 4, 23-76. https://doi.org/10.1515/popets-2017-0038

Laud, P. Parallel oblivious array access for secure multiparty computation and privacy-preserving minimum spanning trees. − Proceedings on Privacy Enhancing Technologies, 2015, (2), 188–205. https://doi.org/10.1515/popets-2015-0011

Laud, P., Randmets, J. A domain-specific language for low-level secure multiparty computation protocols. − Kruegel, C., Li, N. (eds). 22nd ACM Conference on Computer and Communications Security, Denver, CO, USA, October 12th-16th, 2015. ACM, 2015, 1492−1503. https://doi.org/10.1145/2810103.2813664

Pankova, A., Laud, P. Symbolic analysis of cryptographic protocols containing bilinear pairings. − Cortier, V., Zdancewic, S. (eds). 25th Computer Security Foundations Symposium (CSF), Cambridge MA, USA, June 25-27, 2012. IEEE Computer Society Press, 2012. 63−77. https://doi.org/10.1109/CSF.2012.10

Laud, P. Symmetric encryption in automatic analyses for confidentiality against active adversaries. − IEEE Symposium on Security and Privacy. Proceedings. Berkeley, CA, USA, 9-12.05 2004. Los Alamitos, 2004, 71-85. https://doi.org/10.1109/SECPRI.2004.1301316

Laud, P. Semantics and program analysis of computationally secure information flow. − Programming Languages and Systems, Proceedings, 2001, 2028, 77-91. https://doi.org/10.1007/3-540-45309-1_6

Buldas, A., Laud, P., Lipmaa, H., Willemson, J. Time-stamping with binary linking schemes. − Advances in Cryptology - CRYPTO '98, 1998, 1462, 486-501. (Lecture Notes in Comouter Science). https://doi.org/10.1007/BFb0055749