

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](#)

BLT+L : efficient signatures from timestamping and endorsements

Firsov, Denis; Lakk, Henri; Laur, Sven; Truu, Ahto Proceedings of the 18th International Conference on Security and Cryptography - SECRIPT. Vol. 1 2021 / p. 75-86 <https://doi.org/10.5220/0010530000750086>

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

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>

Informaatikaolümpiaad

Truu, Ahto Horisont 2018 / lk. 59 : fot https://www.ester.ee/record=b1072243*est <http://www.horisont.ee/arhiiv-2018/Horisont-6-2018.pdf>

Informaatikavõistlused

Truu, Ahto Horisont 2018 / lk. 56 : fot https://www.ester.ee/record=b1072243*est <http://www.horisont.ee/arhiiv-2018/Horisont-2-2018.pdf>

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 <http://dx.doi.org/10.1504/IJSTM.2017.10002708>

A New approach to constructing digital signature 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](#)

Nupunurk

Truu, Ahto A & A 1998 / 1, lk. 57-61; 2, lk. 55-59; 5, lk. 61

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

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](#)

Verified multiple-time signature scheme from one-time signatures and timestamping

Firsov, Denis; Lakk, Henri; Truu, Ahto 2021 IEEE 34th Computer Security Foundations Symposium (CSF) : June 21-25, 2021, Virtual Conference : proceedings 2021 / 13 p <https://doi.org/10.1109/CSF51468.2021.00051>

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 / p. 244-257 <https://doi.org/10.1145/3372885.3373828>

Winter of Code'i võitis Skype'i koosolekutahvel : [üliõpilaste tarkvaraprojektide konkursil 2. ja 3. koha koha võitsid TTÜ võistkonnad]

Truu, Ahto Arvutimaailm 2007 / lk. 60-61 : fot https://artiklid.elnet.ee/record=b2370929*est

Üliõpilaste tarkvaraprojektide konkursi Winter of Code võitjad : [ka TTÜ võistkonnad]

Truu, Ahto Mente et Manu 2007 / 23. mai, lk. 2 : fot https://www.ester.ee/record=b1242496*est