

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>