

Reflection, rewinding, and coin-toss in EasyCrypt

Firsov, Denis; Unruh, Dominique CPP 2022 - Proceedings of the 11th ACM SIGPLAN International Conference on Certified Programs and Proofs, co-located with POPL 2022 2022 / p. 166-179 <https://doi.org/10.1145/3497775.3503693>

Zero-knowledge in EasyCrypt

Firsov, Denis; Unruh, Dominique 2023 IEEE 36th Computer Security Foundations Symposium : CSF 2023 : proceedings 2023 / 16 p. <https://doi.org/10.1109/CSF57540.2023.00015>

Unsatisfiability of comparison-based non-malleability for commitments

Firsov, Denis; Laur, Sven; **Zhuchko, Ekaterina** Theoretical Aspects of Computing - ICTAC 2022 : 19th International Colloquium, Tbilisi, Georgia, September 27-30, 2022 : proceedings 2022 / p. 188–194 https://doi.org/10.1007/978-3-031-17715-6_13 [Conference Proceedings at Scopus](#) [Article at Scopus](#)

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) 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 2020 / p. 244-257 <https://doi.org/10.1145/3372885.3373828>