[15] dalek cryptography. 2024. ed25519-dalek. https://github.com/dalek-cryptography/ed25519-dalek.
[16] Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. 2021. Poseidon: A New Hash Function for Zero-Knowledge Proof Systems. In *USENIX Security Symposium*. https://api.semanticscholar.org/CorpusID:221069468
[17] Sam Grierson, Konstantinos Chalkias, and William J Buchanan. 2023. Double Public Key Signing Function Oracle Attack on EdDSA Software Implementations. *arXiv preprint arXiv:2308.15009* (2023).
[18] Jens Groth. 2016. On the Size of Pairing-Based Non-interactive Arguments. 305–326. https://doi.org/10.1007/978-3-662-49896-5_11
[19] iden3. 2024. rapidsnark. https://github.com/iden3/rapidsnark.
[20] Kostas Kryptos. 2023. Blockchain research has advanced systems and cryptography. https://twitter.com/kostascrypto/status/1626983601572302848.
[21] Zhuolun Li, Alberto Sonnino, and Philipp Jovanovic. 2023. Performance of EdDSA and BLS Signatures in Committee-Based Consensus. In *Workshop on Advanced tools, programming languages, and PLatforms for Implementing and Evaluating algorithms for Distributed systems*.
[22] lurk-lab. 2024. neptune. https://github.com/lurk-lab/neptune.
[23] Nicholas D Matsakis and Felix S Klock. 2014. The rust language. *ACM SIGAda Ada Letters* 34, 3 (2014), 103–104.
[24] Mysten Labs. 2024. fastcrypto. https://github.com/MystenLabs/fastcrypto.
[25] NumPy Team. 2024. Numpy. https://numpy.org.
[26] Penumbra. 2024. ed25519-consensus. https://github.com/penumbra-zone/ed25519-consensus.
[27] Rust Bitcoin Community. 2024. rust-secp256k1. https://github.com/rust-bitcoin/rust-secp256k1/.
[28] RustCrypto. 2024. p256. https://github.com/RustCrypto/elliptic-curves/tree/master/p256.
[29] Rustsec. 2022. Double Public Key Signing Function Oracle Attack on ed25519-dalek. RUSTSEC-2022-0093: https://rustsec.org/advisories/RUSTSEC-2022-0093.
[30] Supranational. 2024. blst. https://github.com/supranational/blst.
[31] Gavin Wood et al. 2014. Ethereum: A secure decentralised generalised transaction ledger. , 32 pages.