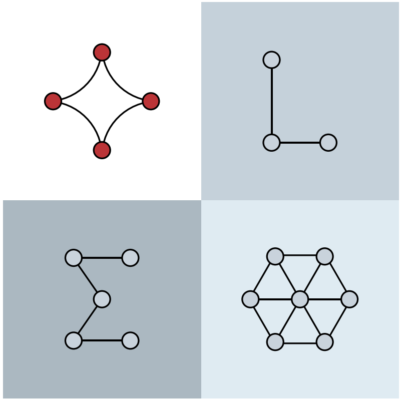
Research

Privacy is about staying one step ahead. The team behind Firo is responsible for some of the most significant blockchain privacy protocols on record, and all that tech is distilled into Firo.

lelantus spark

Lelantus Spark Technology

Lelantus Spark greatly improves over its predecessor Lelantus with flexible Spark addresses that hide all transaction amounts, are not searchable on the blockchain while allowing efficient threshold signatures and both incoming and outgoing view key support. Spark also has a modular structure allowing components to be upgraded as better technology arises while simplifying security analysis. It retains the benefits of Lelantus with no trusted setup, an easy to understand construction and based on well established cryptographic assumptions.



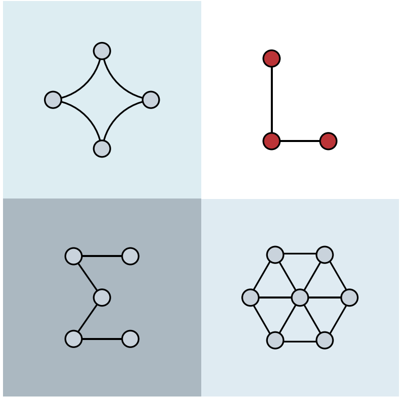
Academic Papers

Lelantus Spark: Secure and Flexible Private Transactions

We propose a modification to the Lelantus private transaction protocol to provide recipient privacy, improved security, and additional usability features. Our decentralized anonymous payment (DAP) construction, Spark, enables non-interactive one-time addressing to hide recipient addresses in transactions. The modified address format permits flexibility in transaction visibility. Address owners can securely provide third parties with opt-in visibility into incoming transactions or all transactions associated to the address; this functionality allows for offloading chain scanning and balance computation without delegating spend authority. It is also possible to delegate expensive proving operations without compromising spend authority when generating transactions. Further, the design is compatible with straightforward linear multisignature operations to allow mutually non-trusting parties to cooperatively receive and generate transactions associated to a multisignature address. We prove that Spark satisfies formal DAP security properties of balance, non-malleability, and ledger indistinguishability.

lelantus

Lelantus Technology



Lelantus is a next-generation privacy protocol developed by Aram Jivanyan at Firo. Lelantus allows you to burn your coins, which hides them in an anonymity set of over 65,000. The receiver can redeem it from this anonymity pool, which breaks the links from your transaction and all the previous ones it has been through.

Academic Papers

Lelantus: Private transactions with hidden origins and amounts based on DDH (Aram Jivanyan)

Lelantus is Firo's next generation privacy protocol which improves on Sigma by removing the requirement of fixed denominations allowing people to burn arbitrary amounts and redeem partial amounts without revealing values or the source. Lelantus doesn't require any trusted setup and uses only DDH assumptions. It also supports untraceable direct anonymous payments by allowing people to pass the right to redeem to someone else. Lelantus is Firo's own innovation.

Hierarchical One-out-of-Many Proofs With Applications to Blockchain Privacy and Ring Signatures (Aram Jivanyan)

In this work, we introduce a new method of instantiating one-out-of-many proofs which reduces the proof generation time by an order of magnitude. In certain practical applications our method also helps to fasten the verification process of multiple simultaneously generated proofs. Our approach still results in shorter proofs comprised of simultaneously generated proofs. Our approach still results in shorter proofs comprised of only a logarithmic number of commitments and does not compromise the highly efficient batch verification properties endemic to the original construction. We believe this work can also foster further research towards building more efficient one-out-of-many proofs which are extremely useful constructions in the blockchain privacy space and beyond.

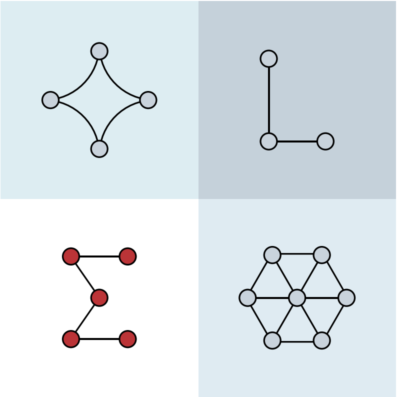
Audits

Lelantus cryptographic library audit by Trail of Bits

Lelantus cryptography audit by ABDK Consulting

sigma

Sigma Technology



We believe the whole purpose of blockchain is to build systems that do not require trust, and that same principle applies to our privacy system itself. This is why we built Sigma for Zcoin in 2018. Sigma uses 256 bit ECC curves for proof sizes of just 1.5 kB - a 17x improvement on then-current technology. Sigma was a precursor to Lelantus, and set many stepping stones to get us where we are today.

Academic Papers

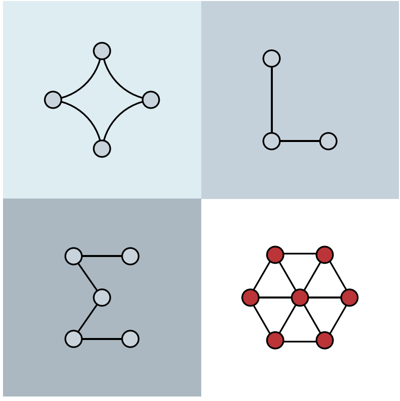
One-out-of-Many Proofs: Or How to Leak a Secret and Spend a Coin (Jens Groth et al)

One out of Many Proofs forms the foundation of Sigma which improves on Zerocoin by removing trusted setup and reducing proof sizes. Firo is also applying some further efficiency modifications to the original paper. Sigma is in development and is slated to be released in Q1 2019.

MTP

Decentralized and fair security

Firo’s Merkle Tree Proof (MTP) mining algorithm further strengthens the practical anonymity of transactions. MTP is memory-intensive, preventing miner centralization. Nodes, however, can bypass this memory requirement. A Zcoin-sponsored audit in 2017 proved the effectiveness of this two-pronged approach.



MTP: Egalitarian Computing (Alex Biryukov, Dmitry Khovratovich) (revision and improvement funded by Firo)

MTP is the Proof of Work algorithm that Firo uses that promotes egalitarian mining while maintaining quick verification. The original paper had flaws as identified by Dinur and

Nadler. Firo organized a bounty to harden MTP and also funded research to solve these issues as reflected in the linked paper. MTP was coded from the ground up by Firo and switched to the MTP algorithm in December 2018.

resources

Github

Sourceforge

Branding

Vulnerability Program

Explorer

website

Privacy Policy

Terms Of Service

newsletter

If you want to subscribe to our newsletter, please submit the form.

Email*

SUBSCRIBE

communication

ENGLISH ▾