Adding Schnorr‘s blind signature in Taler

Degree programme: BSc in Computer Science | Specialisation: IT Security
Thesis advisor: Prof. Dr. Emmanuel Benoist
Expert: Elektronikingenieur HTL Daniel Voisard

By adding support for Clause Blind Schnorr Signatures in GNU Taler, denomination signatures require significantly less CPU resources, storage space and bandwidth. During the thesis the Taler protocols were redesigned and implemented.

GNU Taler

GNU Taler is a digital payment system. It preserves user privacy while still allowing taxation of merchants and preventing fraud.
Blind Signatures, which are used for obtaining digital cash and change, are fundamental to preserve the customer‘s privacy in Taler. By blindly signing a coin during withdrawal, the exchange (Taler bank) doesn‘t get to see the coin it signs. This signature can then be unblinded and later be verified (during the payment process).
Taler uses Chaum‘s RSA Blind Signature Scheme, which requires large key sizes to achieve security properties that are strong enough.

The goal of our bachelor thesis is to implement a Blind Schnorr Signature Scheme based on elliptic curves into Taler and compare it with the existing scheme in terms of security, privacy protection, speed and storage requirements.

Clause Blind Schnorr Signature Scheme

The first result of this thesis is a redesign of all Taler protocols that are currently using the RSA Blind Signature Scheme. The signature scheme was replaced with the Clause Blind Schnorr Signature Scheme. Many aspects of the protocols were changed, the biggest was integrating the additional request during signature creation.
Further changes to the Taler protocols and the signature scheme were necessary, mainly to ensure abort-idempotency and atomicity.

The second result of this thesis is an implementation of the Clause Blind Schnorr Signature Scheme using Curve25519 written in C. This implementation is free software and is integrated into the GNUnet core repository, thus making it available for other projects.

Integrating the signature scheme and implementing the redesigned protocols into the Taler exchange is the third result of our thesis. A Taler exchange operator can now choose between RSA Blind Signatures and Clause Blind Schnorr Signatures. This offers cipher agility, meaning that in case a flaw in one of the signature schemes is discovered, operators can quickly switch to the other.

Performance Comparison

Compared to RSA Blind Signatures, Clause Blind Schnorr Signatures require significantly less CPU resources, storage space and bandwidth. This is due to the benefits of using a signature scheme based on elliptic curves instead of RSA. Using such a scheme decreases the CPU load of a Taler exchange, therefore offers better scalability.
The downside of the Clause Blind Schnorr Signature Scheme is an additional round trip in the withdraw and refresh protocol. Since withdrawing or refreshing coins should not be performed immediately before spending a coin (to prevent correlation), this doesn‘t have any immediate drawbacks regarding performance.

Gian Demarmels

Lucien Claude Heuzeveldt