## GNU Taler

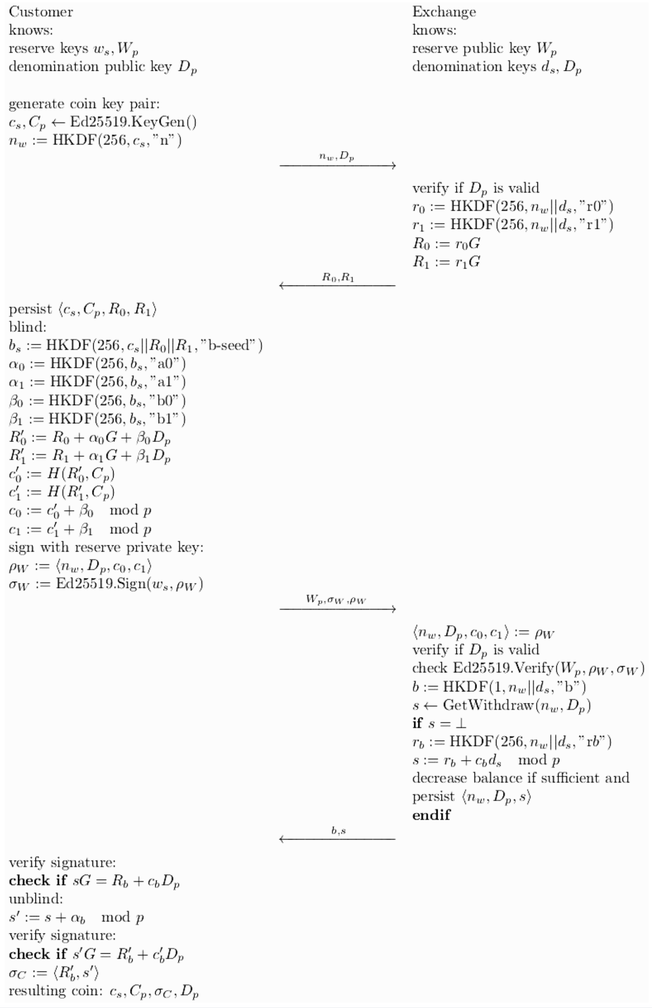
GNU Taler is a digital payment system implemented as free software. It preserves user privacy, while still allowing taxation of merchants and preventing fraud.
While being an intuitive and modern solution, Taler is based on well-known and proven cryptographic algorithms.

## Clause Blind Schnorr Signatures

The goal of this thesis is to add support for Blind Schnorr Signatures to Taler.
A blind signature scheme based on elliptic curves named Clause Blind Schnorr Signature scheme is used.
These signatures require less storage space and are faster, due to the smaller size.
To add support for Clause Blind Schnorr Signatures, all Taler protocols need to be redesigned and then implemented.
Furthermore, these protocols must ensure abort-idempotency and atomicity.

## Protocol Redesign

Due to the differences in the Clause Schnorr Blind Signature Scheme compared to the existing RSA Blind Signatures, various changes on Talers protocols were made. The withdraw protocol is included here to illustrate those changes. All the other protocols and the details can be found in the thesis document.




## Results

- Redesign of Taler protocols
- Implementation of the cryptographic routines for Clause Blind Schnorr Signatures using Curve25519 in GNUnet
- Implementation of the protocols in Taler's exchange
- Implemented as free software

A Taler exchange operator can now choose between RSA Blind Signatures or Clause Blind Schnorr Signatures. (cipher agility)

CS Signatures provide following benefits:
- Less CPU usage
- Less storage space required
- Less bandwith used

These benefits lead to better scalability.

Downside:
- Requires an extra request in the withdrawal/refresh protocols (+ 1 RTT).


Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

# Adding Schnorr's blind signature in Taler

Graduate(s): Gian Demarmels, Lucien Heuzeveldt
Professor: Emmanuel Benoist
Expert: Daniel Voisard

Bachelor Thesis 2022 Degree Programme Computer Science