GNU Taler

Christian Grothoff

Berner Fachhochschule

10.6.2022
Learning Objectives

- Blind Signatures
- Real world surveillance
- The Bank’s Problem
- Introduction to GNU Taler
- Real-World Crypto
- Retail Central Bank Digital Currencies
- Taler Cryptography
- Digital Change with Cut-and-choose
- References
Reminder: RSA

Pick $p, q$ prime and $e$ such that

$$GCD((p - 1)(q - 1), e) = 1$$  \hspace{1cm} (1)

- Define $n = pq$,  
- compute $d$ such that $ed \equiv 1 \mod (p - 1)(q - 1)$.
- Let $s := m^d \mod n$.
- Then $m \equiv s^e \mod n$. 
RSA Summary

- Public key: $n, e$
- Private key: $d \equiv e^{-1} \mod \phi(n)$ where $\phi(n) = (p - 1) \cdot (q - 1)$
- Encryption: $c \equiv m^e \mod n$
- Decryption: $m \equiv c^d \mod n$
- Signing: $s \equiv m^d \mod n$
- Verifying: $m \equiv s^e \mod n$?
Low Encryption Exponent Attack

- $e$ is known
- $M$ maybe small
- $C = M^e < n$?
- If so, can compute $M = \sqrt[e]{C}$
- $\Rightarrow$ Small $e$ can be bad!
Padding and RSA Symmetry

- Padding can be used to avoid low exponent issues (and issues with \( m = 0 \) or \( m = 1 \))
- Randomized padding defeats chosen plaintext attacks
- Padding breaks RSA symmetry:

\[
D_{A_{priv}}(D_{B_{priv}}(E_{A_{pub}}(E_{B_{pub}}(M)))) \neq M
\]  

(2)

- PKCS#1 / RFC 3447 define a padding standard
Blind signatures with RSA [?] 

1. Obtain public key
   \((e, n)\)
2. Compute
   \(f := FDH(m), \quad f < n.\)
3. Pick blinding factor
   \(b \in \mathbb{Z}_n\)
4. Transmit
   \(f' := fb^e \mod n\)
Blind signatures with RSA

1. Obtain public key $(e, n)$
2. Compute
   $f := FDH(m)$,
   $f < n$.
3. Pick blinding factor $b \in \mathbb{Z}_n$
4. Transmit
   $f' := fb^e \mod n$

1. Receive $f'$.
2. Compute
   $s' := f'^d \mod n$.
3. Send $s'$. 
Blind signatures with RSA [?

1. Obtain public key
   \((e, n)\)

2. Compute
   \(f := \text{FDH}(m), \quad f < n\).

3. Pick blinding factor
   \(b \in \mathbb{Z}_n\)

4. Transmit
   \(f' := fb^e \mod n\)

1. Receive \(f'\).

2. Compute
   \(s' := f'^d \mod n\).

3. Send \(s'\).

1. Receive \(s'\).

2. Compute
   \(s := s'b^{-1} \mod n\)
What domain of digital communication should we be most concerned about?
Surveillance concerns

- Everybody knows about Internet surveillance.
- But is it *that* bad?
Surveillance concerns

- Everybody knows about Internet surveillance.
- But is it **that** bad?
  - You can choose when and where to use the Internet
  - You can anonymously access the Web using Tor
  - You can find open access points that do not require authentication
  - IP packets do not include your precise location or name
  - ISPs typically store this meta data for days, weeks or months
Where is it worse?

This was a question posed to RAND researchers in 1971:

“Suppose you were an advisor to the head of the KGB, the Soviet Secret Police. Suppose you are given the assignment of designing a system for the surveillance of all citizens and visitors within the boundaries of the USSR. The system is not to be too obtrusive or obvious. What would be your decision?”
Where is it worse?

This was a question posed to RAND researchers in 1971:

“Suppose you were an advisor to the head of the KGB, the Soviet Secret Police. Suppose you are given the assignment of designing a system for the surveillance of all citizens and visitors within the boundaries of the USSR. The system is not to be too obtrusive or obvious. What would be your decision?”
What is worse:

- When you pay by CC, the information includes your name
- When you pay in person with CC, your location is also known
- You often have no alternative payment methods available
- You hardly ever can use someone else’s CC
- Anonymous prepaid cards are difficult to get and expensive
- Payment information is typically stored for at least 6 years
Banks have Problems, too!

3D secure ("verified by visa") is a nightmare:

- Complicated process
- Shifts liability to consumer
- Significant latency
- Can refuse valid requests
- Legal vendors excluded
- No privacy for buyers

Online credit card payments will be replaced, but with what?
The Bank’s Problem

- Global tech companies push oligopolies
- Privacy and federated finance are at risk
- Economic sovereignty is in danger
Predicting the Future

- Google and Apple will be your bank and run your payment system
- They can target advertising based on your purchase history, location and your ability to pay
- They will provide more usable, faster and broadly available payment solutions; our federated banking system will be history
- After they dominate the payment sector, they will start to charge fees befitting their oligopoly size
- Competitors and vendors not aligning with their corporate “values” will be excluded by policy and go bankrupt
- The imperium will have another major tool for its financial warfare
Do you want to live under total surveillance?
The Bank of International Settlements
The Emergency Act of Canada

https://www.youtube.com/watch?v=NehMAj492SA (2'2022)

1Speech by Premier Kenney, Alberta, February 2022
Break
GNU Taler

Digital cash, made socially responsible.

Privacy-Preserving, Practical, Taxable, Free Software, Efficient
What is Taler?
https://taler.net/en/features.html

Taler is

▶ a Free/Libre software *payment system* infrastructure project
▶ ... with a surrounding software ecosystem
▶ ... and a company (Taler Systems S.A.) and community that wants to deploy it as widely as possible.

However, Taler is

▶ *not* a currency
▶ *not* a long-term store of value
▶ *not* a network or instance of a system
▶ *not* decentralized
▶ *not* based on proof-of-work or proof-of-stake
▶ *not* a speculative asset / “get-rich-quick scheme”
The Taler Software Ecosystem
https://taler.net/en/docs.html

Taler is based on modular components that work together to provide a complete payment system:

- **Exchange:** Service provider for digital cash
  - Core exchange software (cryptography, database)
  - Air-gapped key management, real-time **auditing**
  - LibEuFin: Modular integration with banking systems

- **Merchant:** Integration service for existing businesses
  - Core merchant backend software (cryptography, database)
  - Back-office interface for staff
  - Frontend integration (E-commerce, Point-of-sale)

- **Wallet:** Consumer-controlled applications for e-cash
  - Multi-platform wallet software (for browsers & mobile phones)
  - Wallet backup storage providers
  - **Anastasis:** Recovery of lost wallets based on secret splitting
Taler: Unique Regulatory Features for CBs

https://www.snb.ch/en/mmr/papers/id/working_paper_2021_03

- Central bank issues digital coins equivalent to issuing cash
  ⇒ monetary policy remains under CB control
- Architecture with consumer accounts at commercial banks
  ⇒ no competition for commercial banking (S&L)
  ⇒ CB does not have to manage KYC, customer support
- Withdrawal limits and denomination expiration
  ⇒ protects against bank runs and hoarding
- Income transparency and possibility to set fees
  ⇒ additional insights into economy and new policy options
- Revocation protocols and loss limitations
  ⇒ exit strategy and handles catastrophic security incidents
- Privacy by cryptographic design not organizational compliance
  ⇒ CB cannot be forced to facilitate mass-surveillance
Design goals for the GNU Taler Payment System

GNU Taler must ...

1. ... be implemented as free software.
2. ... protect the privacy of buyers.
3. ... must enable the state to tax income and crack down on illegal business activities.
4. ... prevent payment fraud.
5. ... only disclose the minimal amount of information necessary.
6. ... be usable.
7. ... be efficient.
8. ... avoid single points of failure.
9. ... foster competition.
Taler Overview

- **Customer**
  - withdraw coins
  - spend coins

- **Exchange**
  - verify
  - deposit coins

- **Merchant**
  - spend coins
Architecture of Taler

1. Pay exchange
2. Wire transfer
3. Withdraw coins
4. Spend coins
5. Deposit coins
6. Wire transfer
7. View balance

Exchange's Bank
Customer's Bank
Merchant's Bank
Database
Fees
Browser/Mobile Wallet
Customer
Webshop
Merchant
Architecture of Taler

1. pay exchange
2. wire transfer
3. withdraw coins
4. spend coins
5. deposit coins
6. wire transfer
7. view balance

⇒ Convenient, taxable, privacy-enhancing, & resource friendly!
Usability of Taler

https://demo.taler.net/

1. Install Web extension.
2. Visit the bank.demo.taler.net to withdraw coins.
3. Visit the shop.demo.taler.net to spend coins.
Example: The Taler Snack Machine

Integration of a MDB/ICP to Taler gateway.
Implementation of a NFC or QR-Code to Taler wallet interface.

\[\text{Taler} \quad \text{Backend}\]

\[\text{MDB/ICP} \quad \text{Rest API} \quad \text{USB} \quad \text{NFC} \quad \text{Wallet}\]

---

\(^2\)By M. Boss and D. Hofer
Software architecture for the Taler Snack Machine

Application

GNU:net  libnfc  libqrencode  <Taler>

Raspbian

Raspberry Pi

MDB  NFC  TFT

TCP/IP
User story: Install App on Android

https://wallet.taler.net/
User story: Withdraw e-cash
User story: Use machine!
CBDC Initiatives and Taler

Many initiatives are currently at the level of requirements discussion:

▶ ECB: Report on a Digital Euro / Eurosystm report on the public consultation on a Digital Euro
▶ Bank of England: Just initiated a task force

Taler can serve as the foundation for a *bearer-based retail CBDC*.

▶ Taler replicates physical cash rather than bank deposits
▶ Taler has unique design principles and regulatory features that align with CBDC requirements
▶ ECB survey has identified privacy as a primary requirement of end users
Central bank issues digital coins equivalent to issuing cash
⇒ monetary policy remains under CB control

Architecture with consumer accounts at commercial banks
⇒ no competition for commercial banking (S&L)
⇒ CB does not have to manage KYC, customer support

Withdrawal limits and denomination expiration
⇒ protects against bank runs and hoarding

Income transparency and possibility to set fees
⇒ additional insights into economy and new policy options

Revocation protocols and loss limitations
⇒ exit strategy and handles catastrophic security incidents

Privacy by cryptographic design not organizational compliance
⇒ CB cannot be forced to facilitate mass-surveillance
Offline capabilities are often cited as a requirement for CBDC. All implementations must either use restrictive hardware elements and/or introduce counterparty risk.

- Permanent offline features weaken a CBDC solution (privacy, security)
- Introduces unwarranted competition for physical cash (endangers emergency-preparedness).

We recommend a tiered approach:

1. Online-first, bearer-based CBDC
2. (Optional:) Limited offline mode for network outages
3. Physical cash for emergencies (power outage, catastrophic cyber incidents)
Taxability

We say Taler is taxable because:

- Merchant’s income is visible from deposits.
- Hash of contract is part of deposit data.
- State can trace income and enforce taxation.
Taxability

We say Taler is taxable because:

▶ Merchant’s income is visible from deposits.
▶ Hash of contract is part of deposit data.
▶ State can trace income and enforce taxation.

Limitations:

▶ withdraw loophole
▶ sharing coins among family and friends
How does it work?

We use a few ancient constructions:

- Cryptographic hash function (1989)
- Blind signature (1983)
- Schnorr signature (1989)
- Diffie-Hellman key exchange (1976)
- Cut-and-choose zero-knowledge proof (1985)

But of course we use modern instantiations.
Exchange setup: Create a denomination key (RSA)

1. Pick random primes $p$, $q$.
2. Compute $n := pq$,
   $$\phi(n) = (p - 1)(q - 1)$$
3. Pick small $e < \phi(n)$ such that $d := e^{-1} \mod \phi(n)$ exists.
4. Publish public key $(e, n)$. 
Merchant: Create a signing key (EdDSA)

- Pick random $m \mod o$ as private key
- $M = mG$ public key

**Capability:** $m \Rightarrow M$
Customer: Create a planchet (EdDSA)

- Pick random $c \mod o$ private key
- $C = cG$ public key

Capability: $c \Rightarrow$
1. Obtain public key \((e, n)\)
2. Compute \(f := FDH(C)\), \(f < n\).
3. Pick blinding factor \(b \in \mathbb{Z}_n\)
4. Transmit \(f' := fb^e \mod n\)
Exchange: Blind sign (RSA)

1. Receive $f'$.
2. Compute $s' := f'^d \mod n$.
3. Send signature $s'$. 

Customer
Customer: Unblind coin (RSA)

1. Receive $s'$.
2. Compute $s := s' b^{-1}$ mod $n$
Withdrawing coins on the Web

1. User authentication
2. Send account portal
3. Initiate withdrawal (specify amount and exchange)
4. Request coin denomination keys and wire transfer data
5. Send coin denomination keys and wire transfer data
6. Execute withdrawal

Opt
7. Request transaction authorization
8. Transaction authorization
9. Withdrawal confirmation

10. Execute wire transfer

Customer Browser

Bank Site

Taler (Withdraw coins)

Taler Exchange

Wire transfer

Customer Browser

Bank Site

Taler Exchange
Customer: Build shopping cart

www

Merchant

transmit

Merchant
Merchant: Propose contract (EdDSA)

1. Complete proposal $D$.
2. Send $D$, $EdDSA_m(D)$
Customer: Spend coin (EdDSA)

1. Receive proposal $D$, $EdDSA_m(D)$.
2. Send $s$, $C$, $EdDSA_c(D)$
Merchant and Exchange: Verify coin (RSA)

\[ s^e \equiv FDH(C) \mod n \]
Payment processing with Taler

1. Choose goods by navigating to offer URL
2. Send signed digital contract proposal
3. Select Taler payment method (skippable with auto-detection)
4. Affirm contract
5. Navigate to fulfillment URL
6. Send hash of digital contract and payment information
7. Send payment
8. Forward payment
9. Confirm payment
10. Confirm payment
11. Reload fulfillment URL for delivery
12. Provide product resource
Warranting deposit safety

Exchange has another online signing key \( W = wG \):

Sends \( \text{EdDSA}_w(M, H(D), FDH(C)) \) to the merchant.

This signature means that \( M \) was the first to deposit \( C \) and that the exchange thus must pay \( M \).

Without this, an evil exchange could renege on the deposit confirmation and claim double-spending if a coin were deposited twice, and then not pay either merchant!
Online keys

- The exchange needs $d$ and $w$ to be available for online signing.
- The corresponding public keys $W$ and $(e, n)$ are certified using Taler’s public key infrastructure (which uses offline-only keys).

What happens if those private keys are compromised?
Denomination key \((e, n)\) compromise

- An attacker who learns \(d\) can sign an arbitrary number of illicit coins into existence and deposit them.
- Auditor and exchange can detect this once the total number of deposits (illicit and legitimate) exceeds the number of legitimate coins the exchange created.
- At this point, \((e, n)\) is revoked. Users of unspent legitimate coins reveal \(b\) from their withdrawal operation and obtain a refund.
- The financial loss of the exchange is bounded by the number of legitimate coins signed with \(d\).

⇒ Taler frequently rotates denomination signing keys and deletes \(d\) after the signing period of the respective key expires.
Online signing key $W$ compromise

- An attacker who learns $w$ can sign deposit confirmations.
- Attacker sets up two (or more) merchants and customer(s) which double-spend legitimate coins at both merchants.
- The merchants only deposit each coin once at the exchange and get paid once.
- The attacker then uses $w$ to fake deposit confirmations for the double-spent transactions.
- The attacker uses the faked deposit confirmations to complain to the auditor that the exchange did not honor the (faked) deposit confirmations.

The auditor can then detect the double-spending, but cannot tell who is to blame, and (likely) would presume an evil exchange, forcing it to pay both merchants.
Break
Giving change

It would be inefficient to pay EUR 100 with 1 cent coins!

- Denomination key represents value of a coin.
- Exchange may offer various denominations for coins.
- Wallet may not have exact change!
- Usability requires ability to pay given sufficient total funds.
Giving change

It would be inefficient to pay EUR 100 with 1 cent coins!
▶ Denomination key represents value of a coin.
▶ Exchange may offer various denominations for coins.
▶ Wallet may not have exact change!
▶ Usability requires ability to pay given sufficient total funds.

Key goals:
▶ maintain unlinkability
▶ maintain taxability of transactions
Giving change

It would be inefficient to pay EUR 100 with 1 cent coins!

- Denomination key represents value of a coin.
- Exchange may offer various denominations for coins.
- Wallet may not have exact change!
- Usability requires ability to pay given sufficient total funds.

Key goals:

- maintain unlinkability
- maintain taxability of transactions

Method:

- Contract can specify to only pay *partial value* of a coin.
- Exchange allows wallet to obtain *unlinkable change* for remaining coin value.
Diffie-Hellman (ECDH)

1. Create private keys $c$, $t$ mod $o$
2. Define $C = cG$
3. Define $T = tG$
4. Compute DH
   
   $cT = c(tG) = t(cG) = tC$
Strawman solution

Given partially spent private coin key $c_{old}$:

1. Pick random $c_{new}$ mod $o$ private key
2. $C_{new} = c_{new} G$ public key
3. Pick random $b_{new}$
4. Compute $f_{new} := FDH(C_{new})$, $m < n$. 
5. Transmit $f'_{new} := f_{new} b_{new}^e$ mod $n$

... and sign request for change with $c_{old}$. 
Strawman solution

Given partially spent private coin key $c_{old}$:

1. Pick random $c_{new}$ mod o private key
2. $C_{new} = c_{new}G$ public key
3. Pick random $b_{new}$
4. Compute $f_{new} := FDH(C_{new})$, $m < n$. 
5. Transmit $f_{new}' := f_{new}b_{new}^e$ mod $n$

... and sign request for change with $c_{old}$.

Problem: Owner of $c_{new}$ may differ from owner of $c_{old}$!
Customer: Transfer key setup (ECDH)

Given partially spent private coin key $c_{old}$:

1. Let $C_{old} := c_{old}G$ (as before)
2. Create random private transfer key $t \mod o$
3. Compute $T := tG$
4. Compute $X := c_{old}(tG) = t(c_{old}G) = tC_{old}$
5. Derive $c_{new}$ and $b_{new}$ from $X$
6. Compute $C_{new} := c_{new}G$
7. Compute $f_{new} := FDH(C_{new})$
8. Transmit $f'_{new} := f_{new}b_{new}^e$
Cut-and-Choose

$t_1 \rightarrow \text{old} \rightarrow \text{new} \rightarrow \text{transmit} \rightarrow \text{Exchange}

$t_2 \rightarrow \text{old} \rightarrow \text{new} \rightarrow \text{transmit} \rightarrow \text{Exchange}

$t_3 \rightarrow \text{old} \rightarrow \text{new} \rightarrow \text{transmit} \rightarrow \text{Exchange}
Exchange: Choose!

Exchange sends back random $\gamma \in \{1, 2, 3\}$ to the customer.
1. If $\gamma = 1$, send $t_2, t_3$ to exchange
2. If $\gamma = 2$, send $t_1, t_3$ to exchange
3. If $\gamma = 3$, send $t_1, t_2$ to exchange
Exchange: Verify ($\gamma = 2$)
Exchange: Blind sign change (RSA)

1. Take $f'_{new, \gamma}$.
2. Compute $s' := f'_{new, \gamma}^d \mod n$.
3. Send signature $s'$.
Customer: Unblind change (RSA)

1. Receive \( s' \).
2. Compute \( s := s' b_{new, \gamma}^{-1} \mod n \).
Exchange: Allow linking change

Given \( C_{old} \)

return \( T_\gamma \) and

\[
s := s' b_{new,\gamma}^{-1} \mod n.
\]
1. Have $c_{old}$.
2. Obtain $T_{\gamma}, s$ from exchange
3. Compute $X_{\gamma} = c_{old} T_{\gamma}$
4. Derive $c_{new,\gamma}$ and $b_{new,\gamma}$ from $X_{\gamma}$
5. Unblind $s := s' b_{new,\gamma}^{-1} \mod n$
Refresh protocol summary

- Customer asks exchange to convert old coin to new coin
- Protocol ensures new coins can be recovered from old coin
  ⇒ New coins are owned by the same entity!

Thus, the refresh protocol allows:
- To give unlinkable change.
- To give refunds to an anonymous customer.
- To expire old keys and migrate coins to new ones.
- To handle protocol aborts.

Transactions via refresh are equivalent to sharing a wallet.
Summary

- We can design protocols that fail *soft*.
- GNU Taler’s design limits financial damage even in the case private keys are compromised.
- GNU Taler does:
  - Gives change, can provide refunds
  - Integrates nicely with HTTP, handles network failures
  - High performance
  - Free Software
  - Formal security proofs
GNU Taler: Next Steps

- Implementation still needs:
  - Demonstration Taler can sustain 100k transactions/second
  - Wallet-to-wallet payments
  - Payments with zero-knowledge age verification
  - Payments via smart watch
  - Improved design and usability for illiterate and innumerate users
  - Internationalization ⇒ https://weblate.taler.net/
  - Porting to more platforms (Web shops, iOS, ...)

- Regulatory approval (withdraw and deposit limits, KYC/AML process validation)
Visions

- Be paid to read advertising, starting with spam
- Give welfare without intermediaries taking huge cuts
- Forster regional trade via regional currencies
- Eliminate corruption by making all income visible
- Stop the mining by making crypto-currencies useless for anything but crime