P2P Cooperative System to combat double spending with Lattice-based blind signatures

Aditya Bhardwaj
Neptun Code - BCEW1E

Supervisor: Dr. Péter Kutas

June 28, 2024

Budapest

P2P Cooperative System to combat double spending with Lattice-based blind signatures

Contents

- Tool - Lattice-based Blind signatures
- Problem - Double spending
- Solution - P2P system

Post-quantum security

- Lattice - basics
- Lattice - hard problems
- Lattice cryptography - the idea

P2P Cooperative System to combat double spending with Lattice-based blind signatures

Lattices - Why?

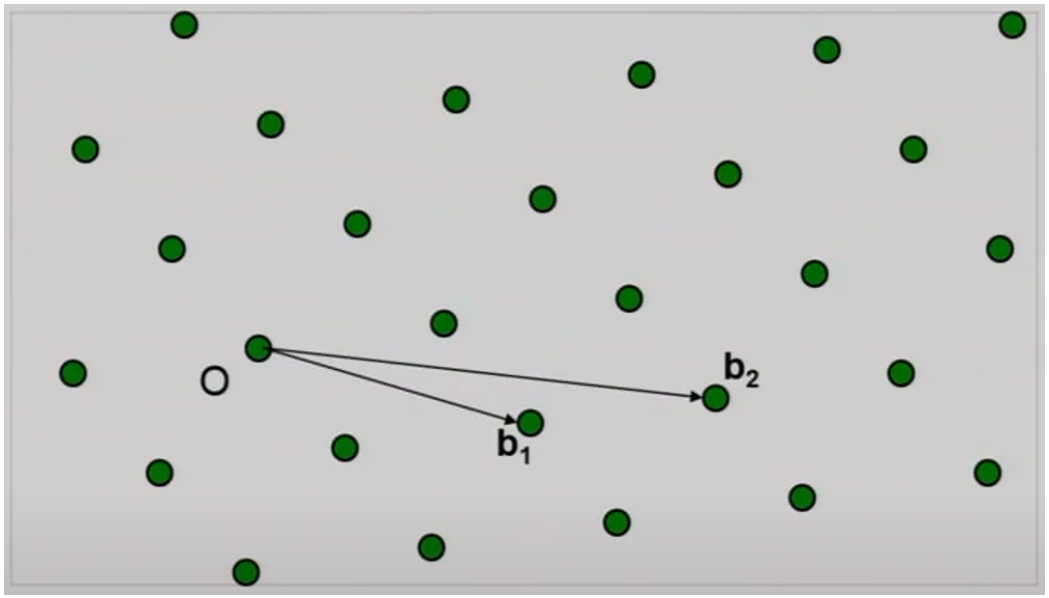
Out of the schemes chosen for NIST standardization

- Public-key encryption scheme
- Signature schemes - 2/3 are lattice-based

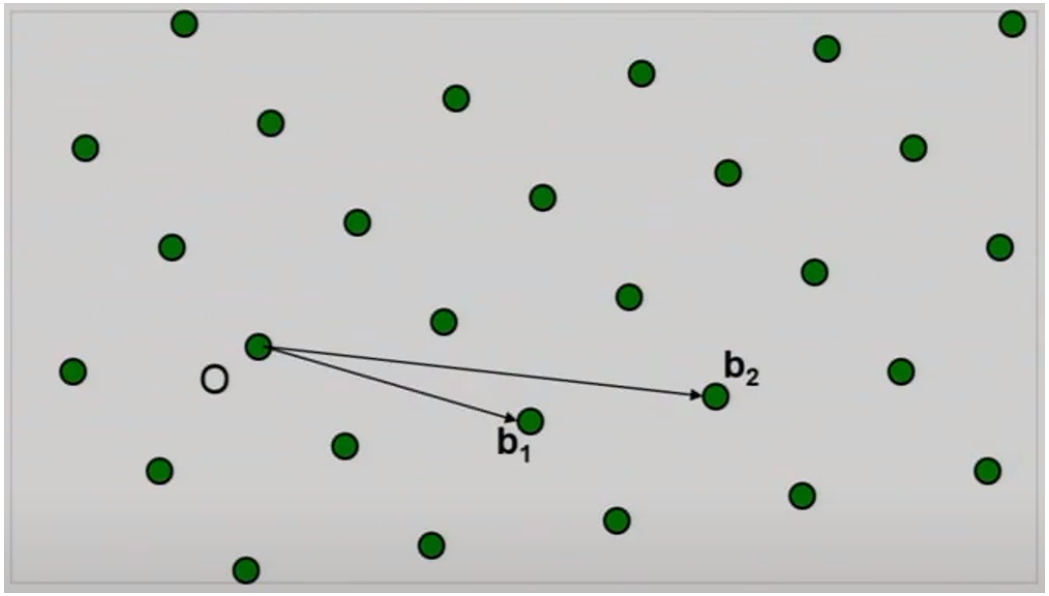
PKE - CRYSTALS-Kyber

Signature schemes - CRYSTALS-Dilithium, FALCON

Lattices

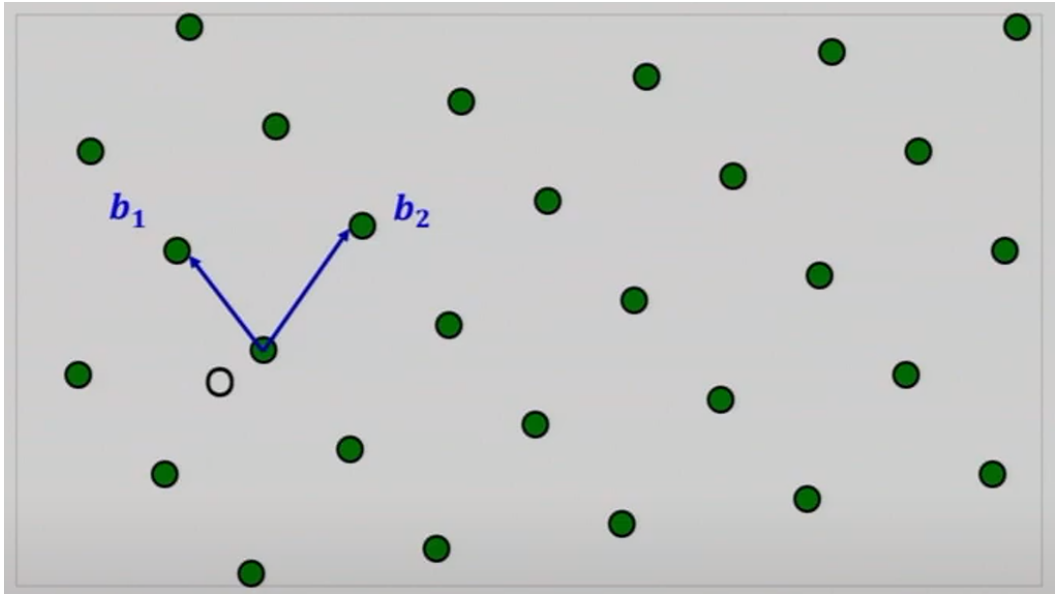


Lattices



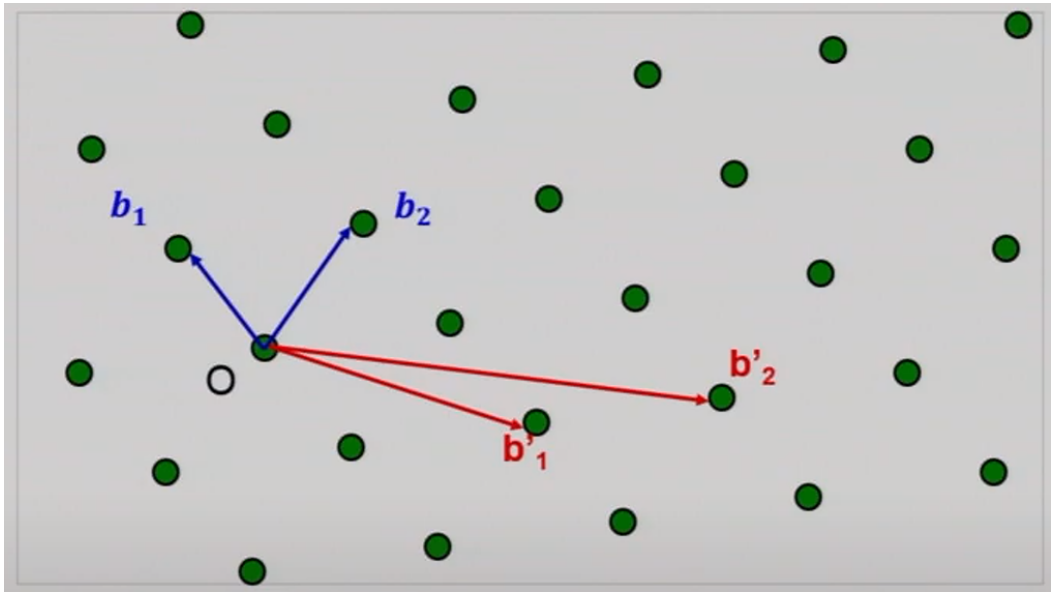
All integer linear combinations of n basis vectors $b_1, b_2, \ldots b_n$

Lattices



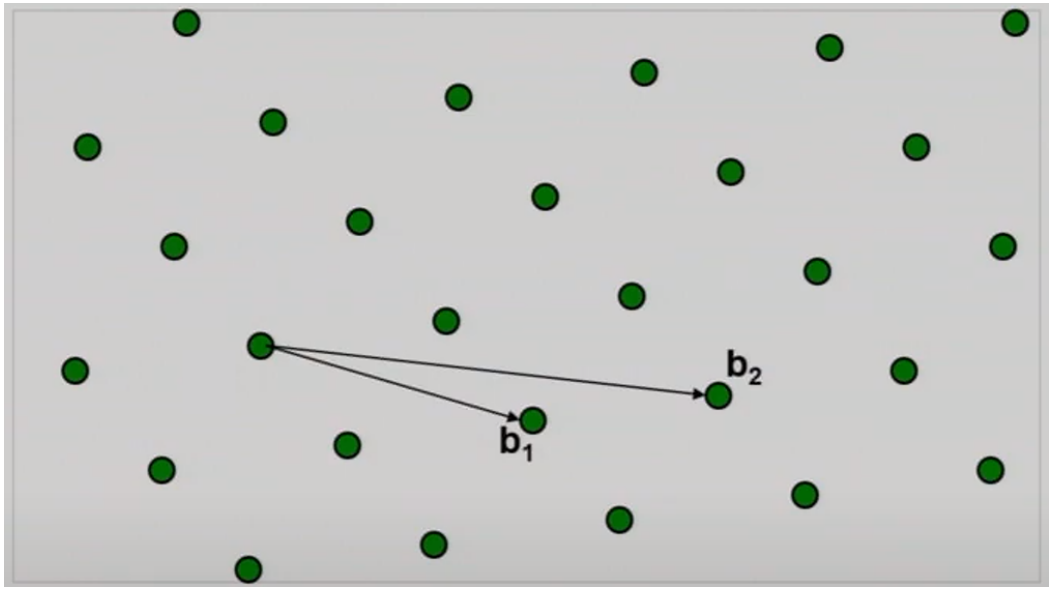
$\boldsymbol{b}_1, \boldsymbol{b}_2$ is a good basis

Lattices



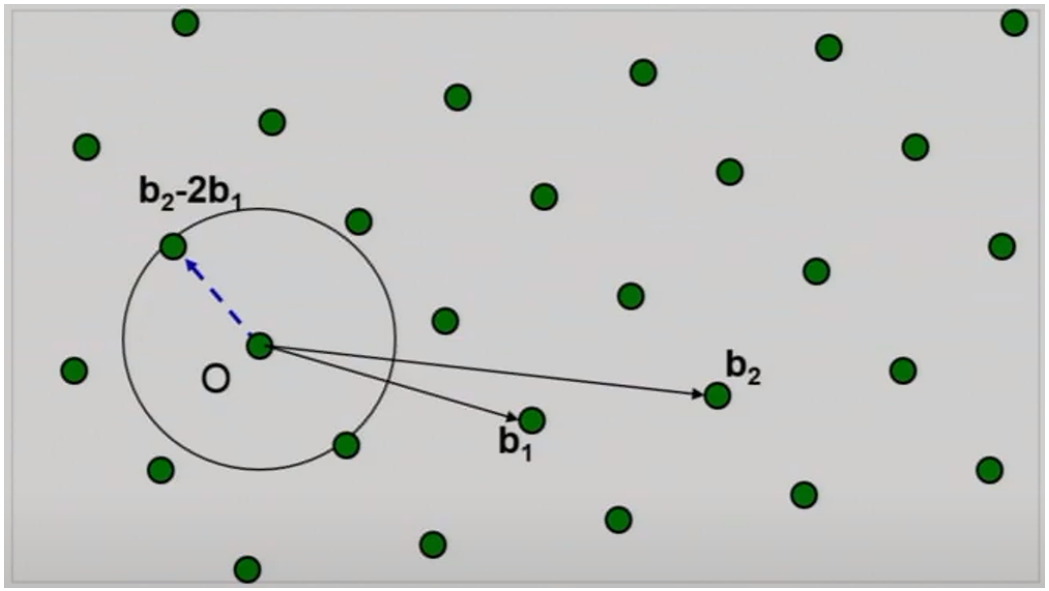
$\boldsymbol{b'}_1, \boldsymbol{b'}_2$ is a good basis

Lattices



Given the basis $\boldsymbol{b}_1, \boldsymbol{b}_2$ what are the hard problems?

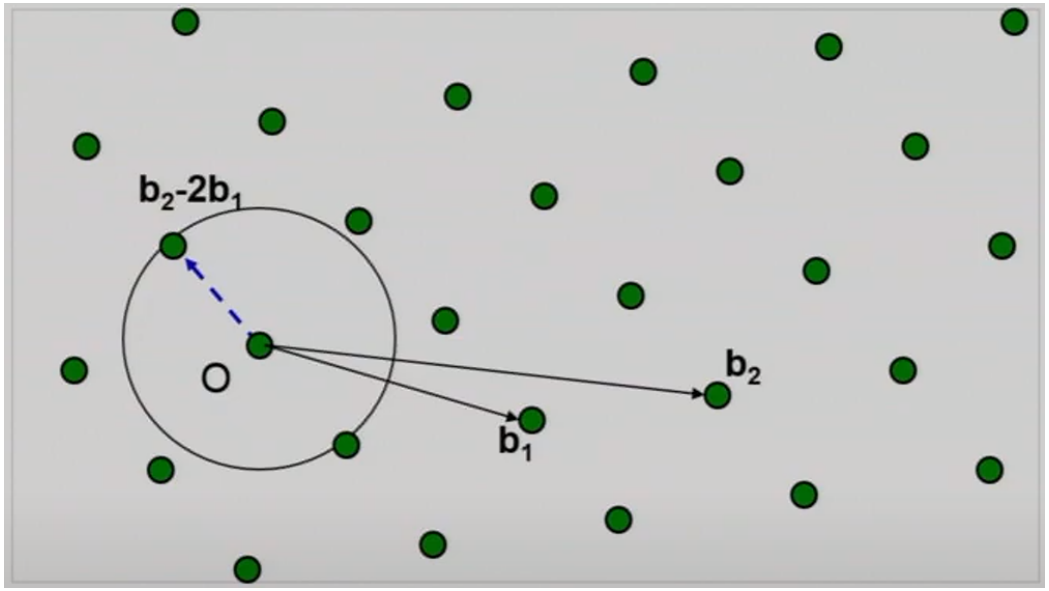
Lattices



$\lambda_1 =$ length of shortest non-zero vector

Shortest Vector Problem

Lattices



$\lambda_1 =$ length of shortest non-zero vector

Shortest Vector Problem

Given the basis $\boldsymbol{b}_1, \boldsymbol{b}_2$, find a shortest non-zero vector v

$$\|\mathbf{v}\| \leq \lambda_1$$

Short Integer Solution - $SIS_{q,n,m,\beta}$

$\mathbb{Z}_q^n = n$-dimensional vectors modulo q

- Let $A \in \mathbb{Z}_q^{n \times m}$ be an $n \times m$ matrix

$$\begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} \quad \begin{pmatrix} | \\ \mathbf{a}_2 \\ | \end{pmatrix} \quad \cdots \quad \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} \quad \in \mathbb{Z}_q^n$$

What is the goal?

Short Integer Solution - $SIS_{q,n,m,\beta}$

- Let $A \in \mathbb{Z}_q^{n \times m}$ be an $n \times m$ matrix

$$\begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} \quad \begin{pmatrix} | \\ \mathbf{a}_2 \\ | \end{pmatrix} \quad \cdots \quad \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} \quad \in \mathbb{Z}_q^n$$

Goal Find small $z_1, \cdots, z_m \in \mathbb{Z}$

Short Integer Solution - $SIS_{q,n,m,\beta}$

- Let $A \in \mathbb{Z}_q^{n \times m}$ be an $n \times m$ matrix

$$z_1 \cdot \begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} + z_2 \cdot \begin{pmatrix} | \\ \mathbf{a}_2 \\ | \end{pmatrix} + \cdots + z_m \cdot \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} = \begin{pmatrix} | \\ 0 \\ | \end{pmatrix} \in \mathbb{Z}_q^n$$

Goal Find small $\boldsymbol{z_1}, \cdots, \boldsymbol{z}_m \in \mathbb{Z}$ such that $A\boldsymbol{z} = \mathbf{0} \in \mathbb{Z}_q^n$.

Short Integer Solution - $SIS_{q,n,m,\beta}$

Goal Find small $z_1, \cdots, z_m \in \mathbb{Z}$ such that:

$$z_1 \cdot \begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} + z_2 \cdot \begin{pmatrix} | \\ \mathbf{a}_2 \\ | \end{pmatrix} + \cdots + z_m \cdot \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} = \begin{pmatrix} | \\ 0 \\ | \end{pmatrix} \in \mathbb{Z}_q^n$$

Short Integer Solution - $SIS_{q,n,m,\beta}$

Goal Find short $\boldsymbol{z} \in \mathbb{Z}^m$ such that:

$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \begin{pmatrix} \\ \mathbf{z} \\ \\ \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

Short Integer Solution - $SIS_{q,n,m,\beta}$

Goal Find short $\boldsymbol{z} \in \mathbb{Z}^m$ such that:

$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \begin{pmatrix} \\ \mathbf{z} \\ \\ \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

A solution to SIS without the condition ($\|\boldsymbol{z}\| \leq \beta$) is easy to compute by using Gaussian elimination technique.

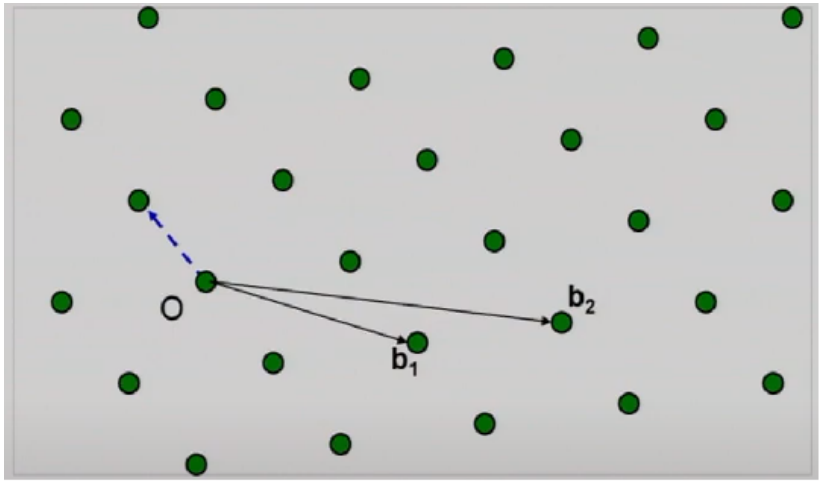
Short Integer Solution - $SIS_{q,n,m,\beta}$

Goal Find short $\boldsymbol{z} \in \mathbb{Z}^m$ such that:

$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \begin{pmatrix} \\ \mathbf{z} \\ \\ \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

A solution to SIS without the condition ($\|\boldsymbol{z}\| \leq \beta$) is easy to compute by using Gaussian elimination technique.
We also require $\beta < q$, otherwise $\boldsymbol{x} = (q, 0, \ldots, 0) \in \mathbb{Z}^m$ is a trivial solution.
- $\beta \geq \sqrt{n \log q}$, and
- $m \geq n \log q$

Lattice-based cryptography

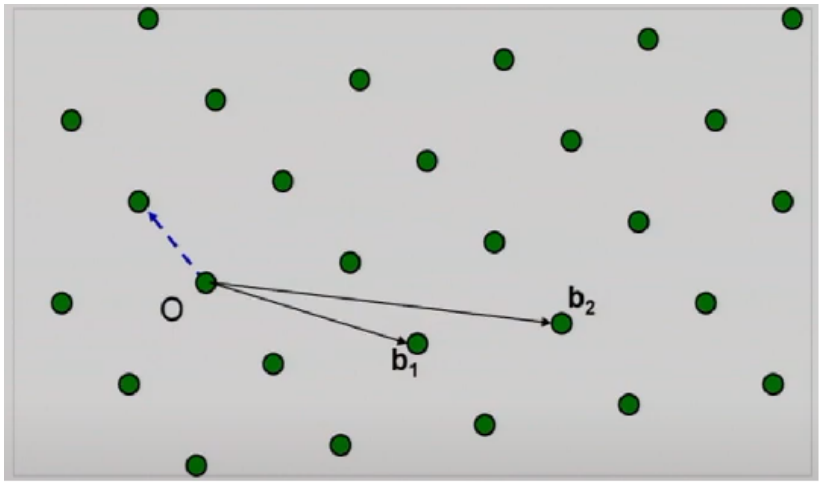


Lattice Basis B

Approx. short vector

v ∈ Lattice(B)

Lattice-based cryptography



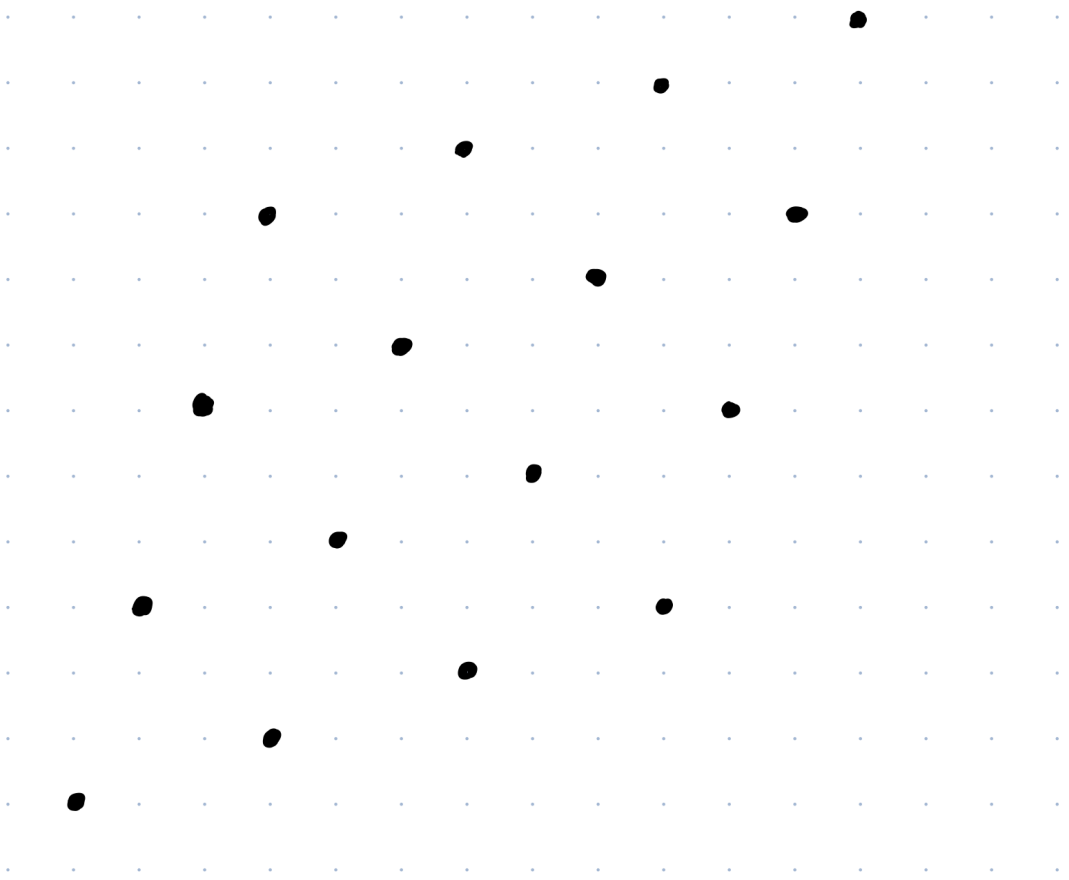
$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \begin{pmatrix} \\ \mathbf{z} \\ \\ \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

Lattice Basis B ⇨ **SIS instance for A**

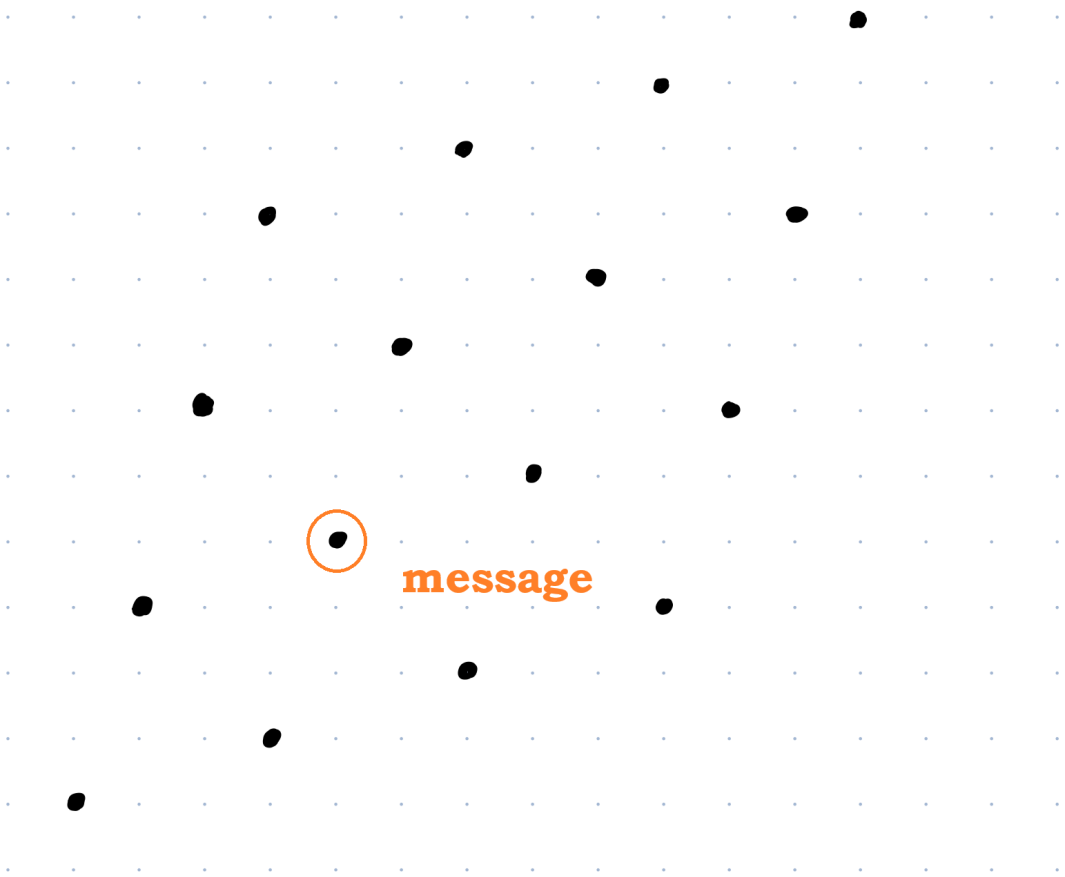
Approx. short vector
v ∈ Lattice(B) ⇦ **SIS solution z**

Ajtai - *"Generating hard instances of lattice problems."* - 1996

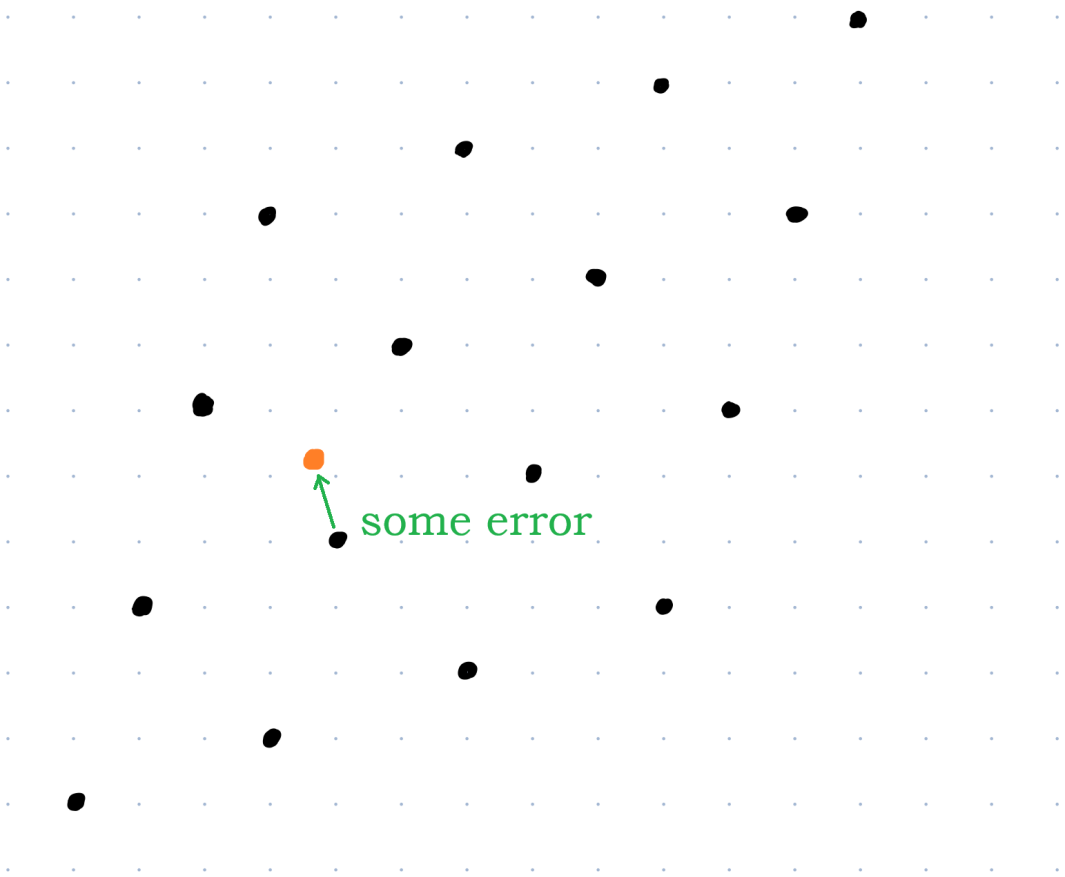
Lattice-based cryptography



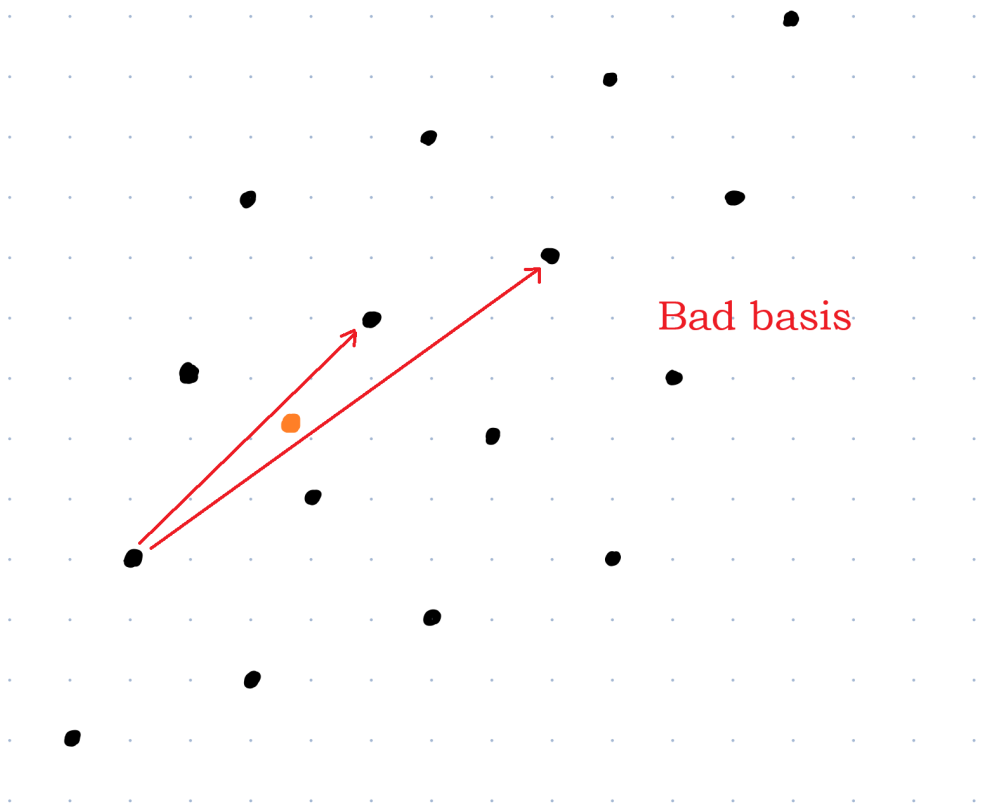
Lattice-based cryptography



Lattice-based cryptography

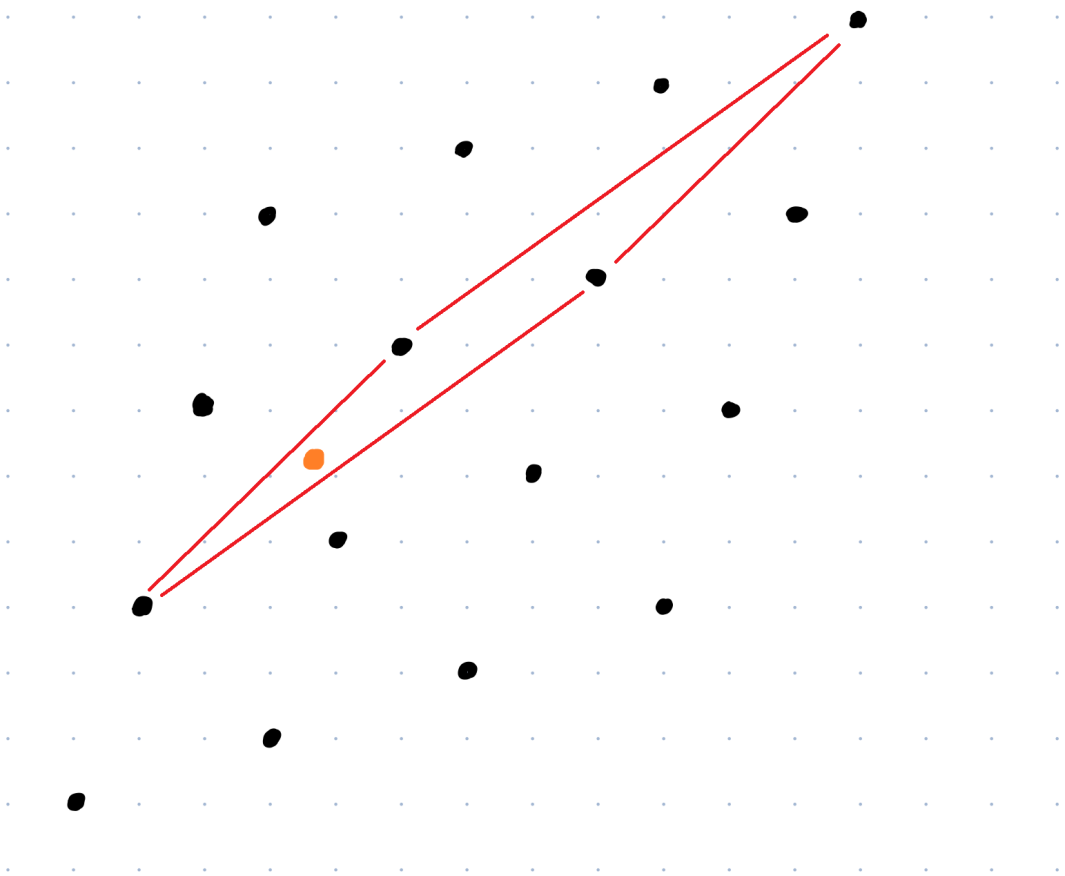


Lattice-based cryptography

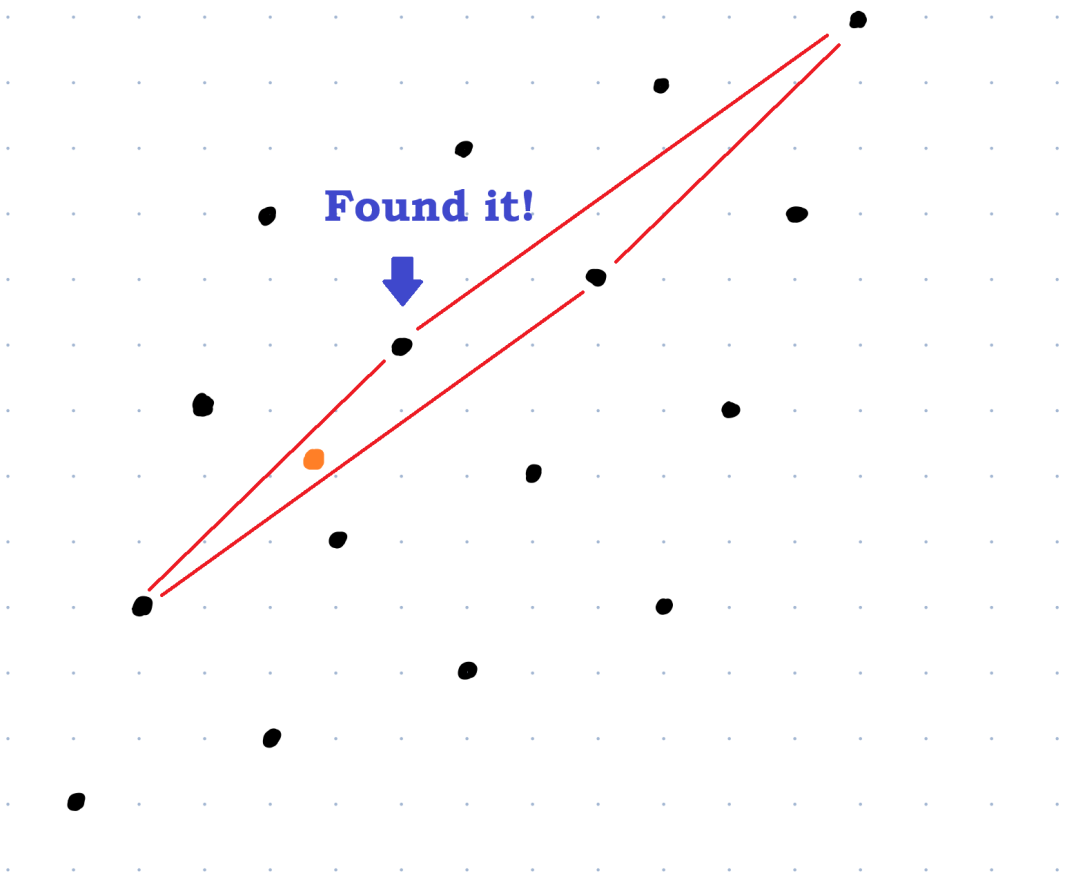


Bad basis $\rightarrow$ Solver

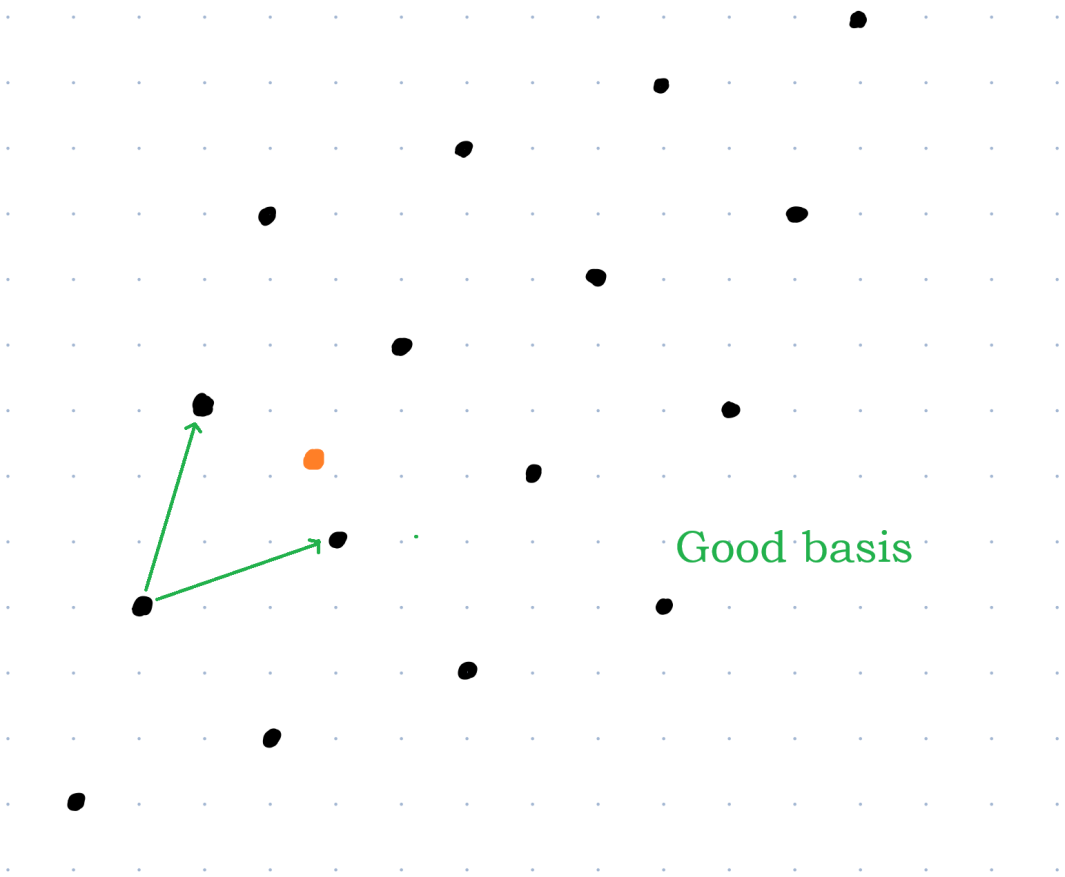
Lattice-based cryptography



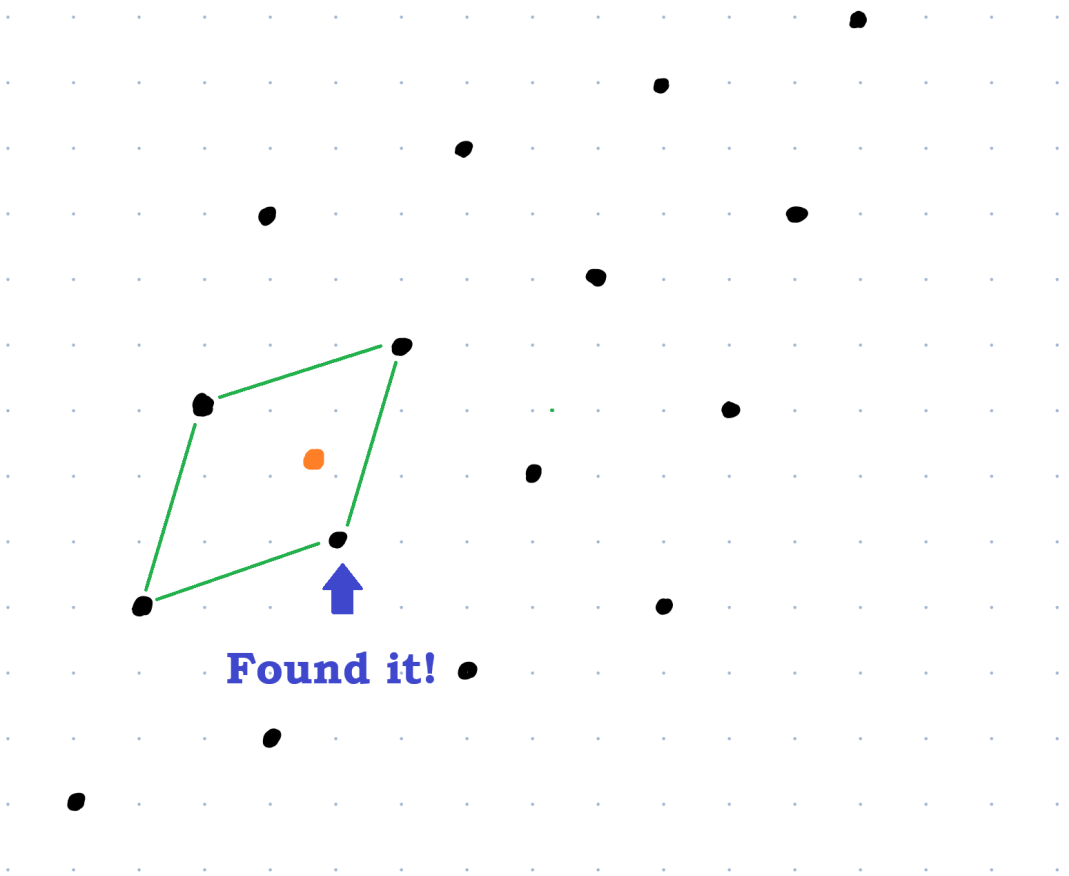
Lattice-based cryptography



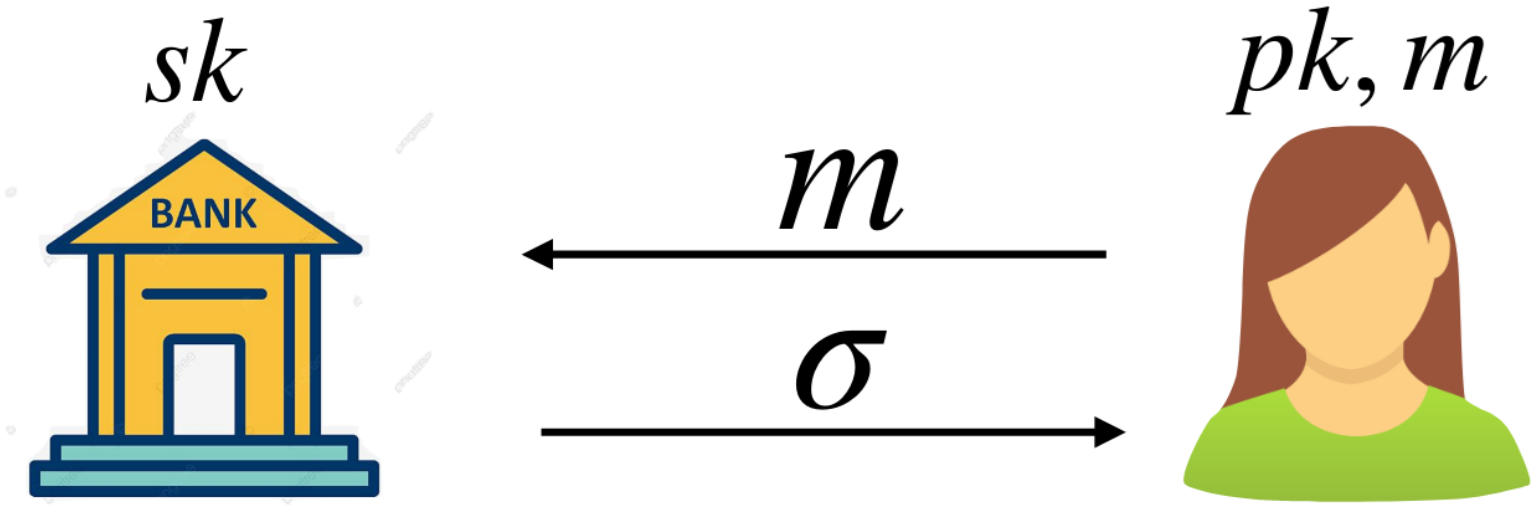
Lattice-based cryptography



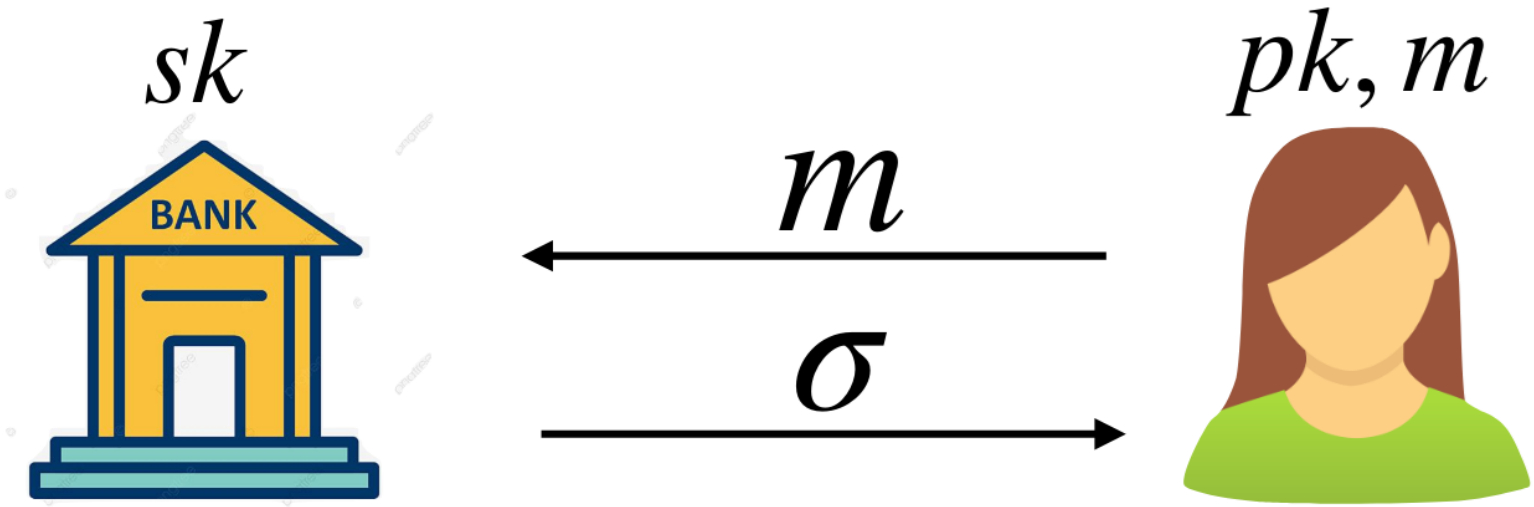
Lattice-based cryptography



Blind signatures



Blind signatures



Signer should not know about m

Schnorr signatures

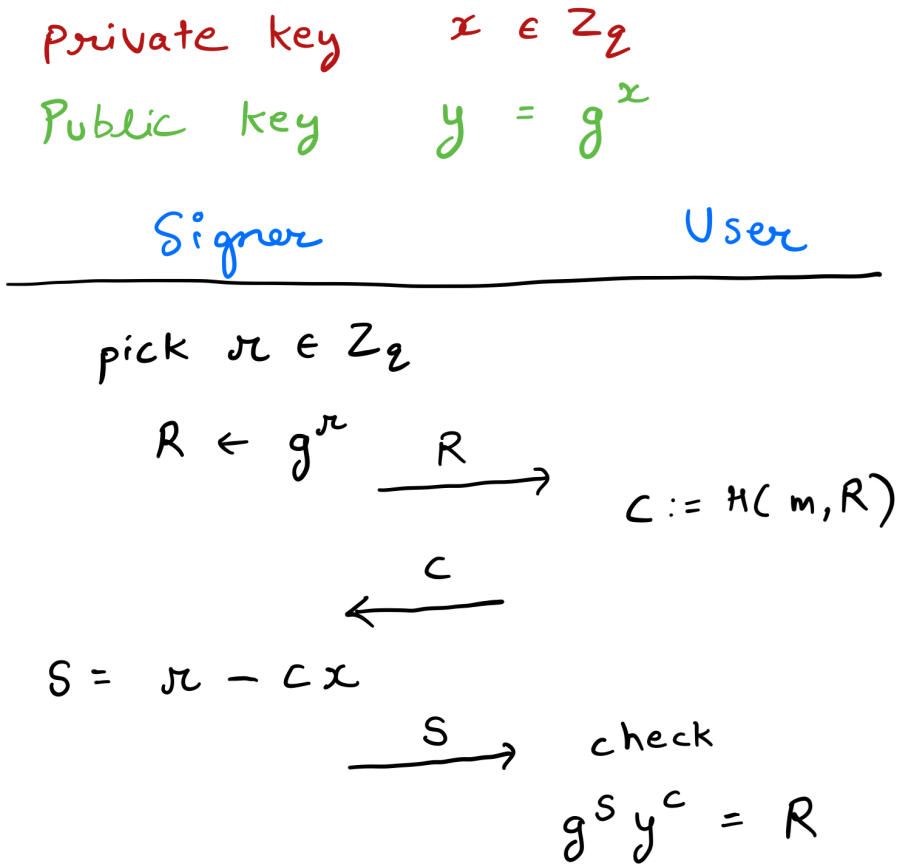
Prime q and a generator $g \in G$ of order q

Private key $x \in Z_q$

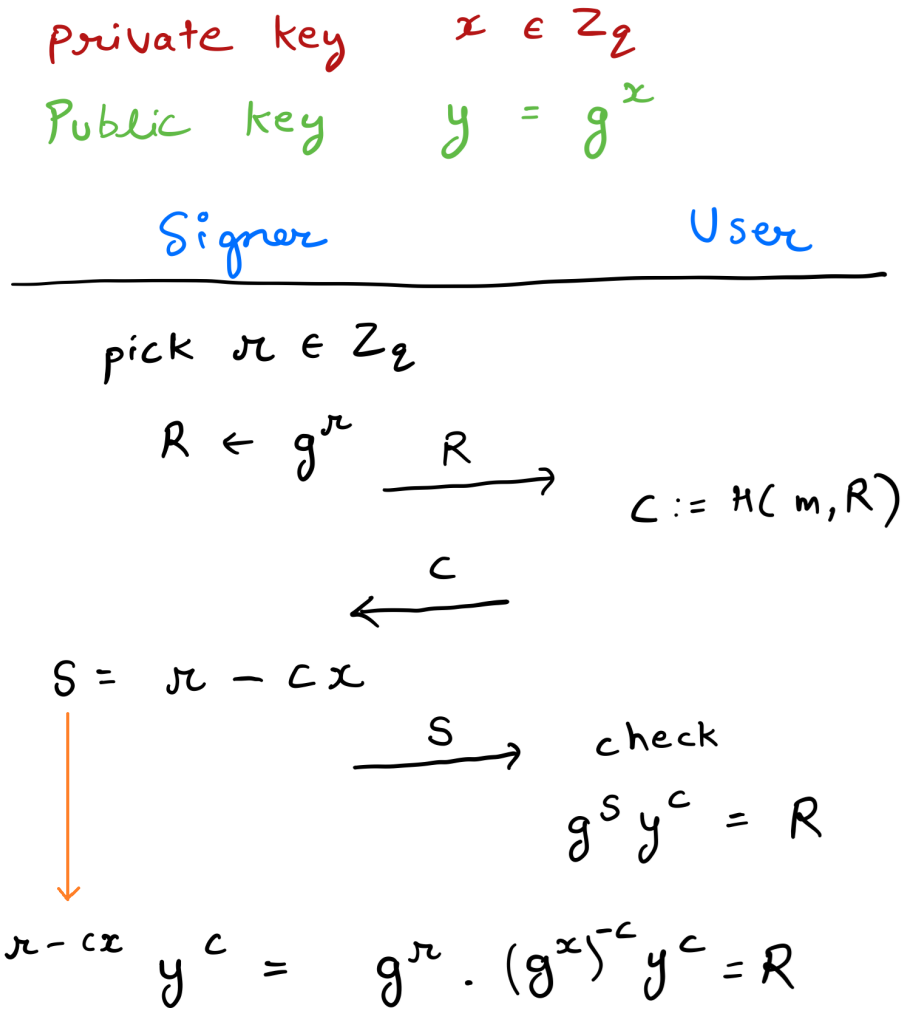
Public key $y = g^x$

Signer | User

Schnorr signatures



Schnorr signatures

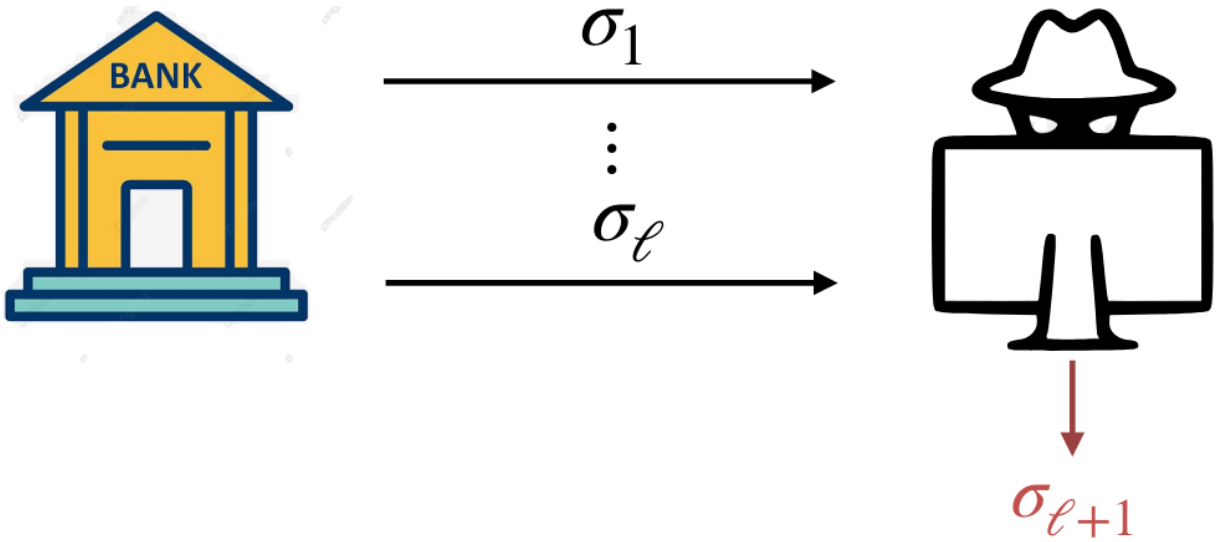


Security

Attack against Blind Schnorr signatures which does not depend on the generator g or the public key $y = g^x$.

- An attacker interacts some l times with a legitimate signer and produces from these interactions $l + 1$ signatures.

Security



- ROS problem: Find an **o**verdetermined, **s**olvable system of linear equations modulo q with **r**andom inhomogenities.

Security - ROS attack

- Oracle random function $F : \mathbf{Z}_q^l \rightarrow \mathbf{Z}_q$
- Find coefficients $a_{k,\ell} \in \mathbf{Z}_q$
- And a solvable system of $l + 1$ distinct equations in the unknowns $c_1, \ldots, c_l$ over $\mathbf{Z}_q$
- $t >> l$

$$a_{k,1}c_1 + \ldots + a_{k,l}c_l = F\left(a_{k,1}, \ldots, a_{k,l}\right) \text{ for } k = 1, \ldots, t$$

Security - ROS attack

Peter Schnorr shows:

If ROS is solvable $\rightarrow$ $l+1$ forger succeeds

- But doesn't give any algorithm
- Problem is known since 2001
- Fabrice Benhamouda et al. "On the (in) security of ROS" 2022, shows practical attack

Security - ROS attack

Number of schemes are affected:

- Multi-signature, partially-blind signature, conditionally blind signature
- pROS attacks more 3-round schemes

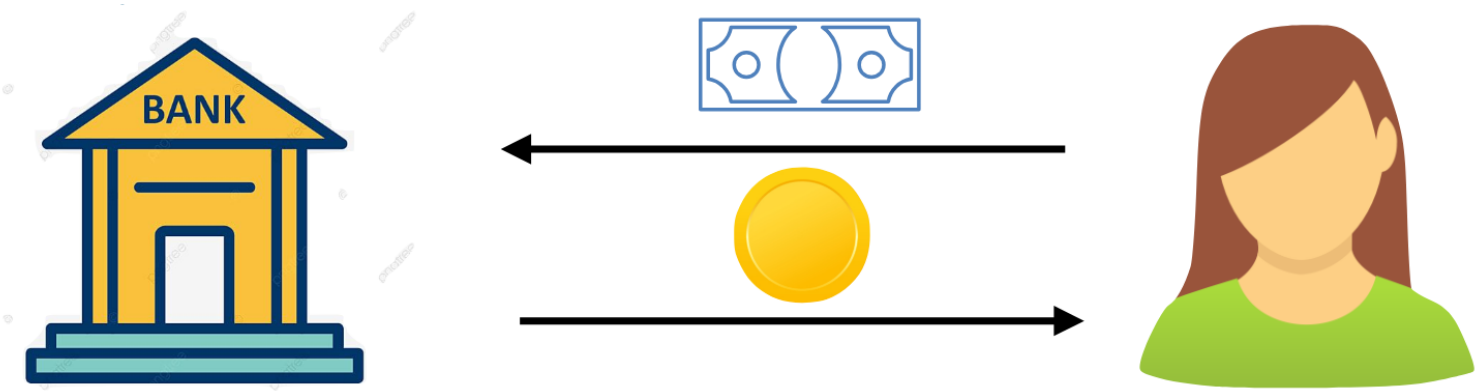
Shuichi Katsumata, Yi-Fu Lai, and Michael Reichle. *"Breaking parallel ROS: implication for isogeny and lattice-based blind signatures"* - 2024

Current state

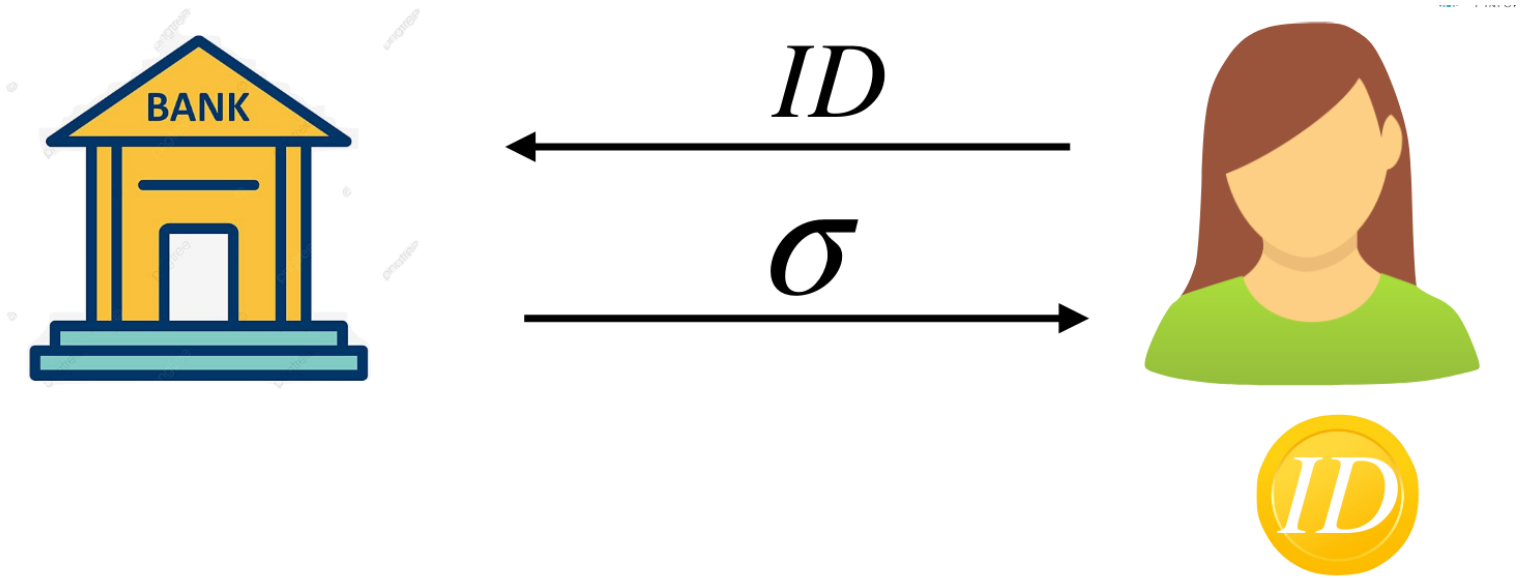
- Round-optimal schemes (2-move)
- No issue of concurrency
- Unbounded number of signatures

First provably secure lattice blind signature scheme 7.9 $MB \rightarrow$ 22 KB now.

Blind signatures for ecash



Blind signatures for ecash



P2P Cooperative System to combat double spending with Lattice-based blind signatures

Double spending

Spending the same money twice

Double spending - Physical cash

- Physical cash - hard to counterfeit
- Measures - Watermarks, specific printers, ink
- Highly controlled and secured

Double spending - Digital cash

- Digital cash - it is piece of data

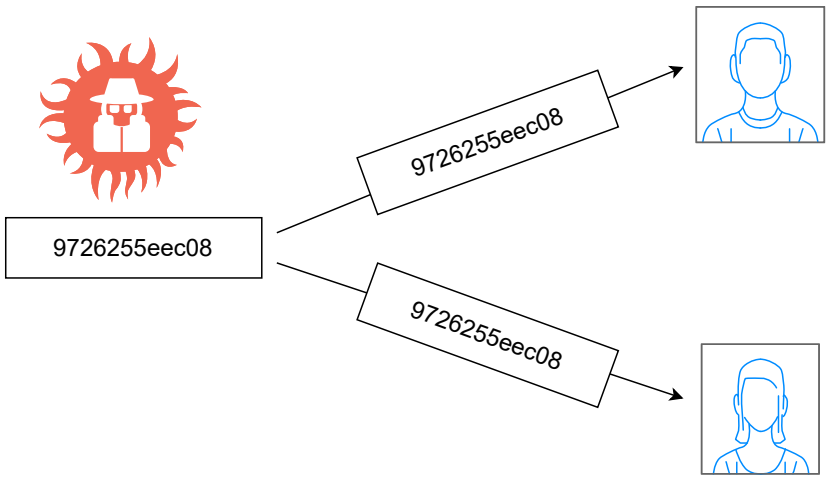
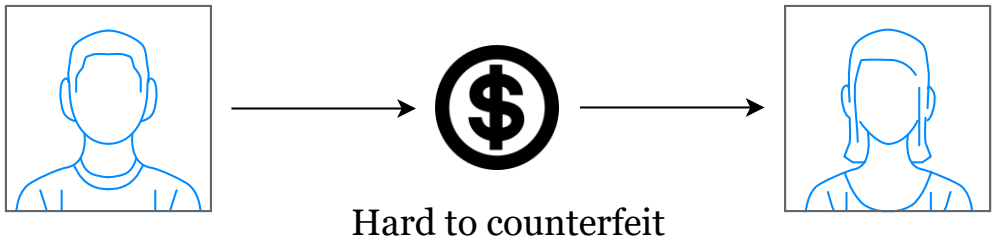
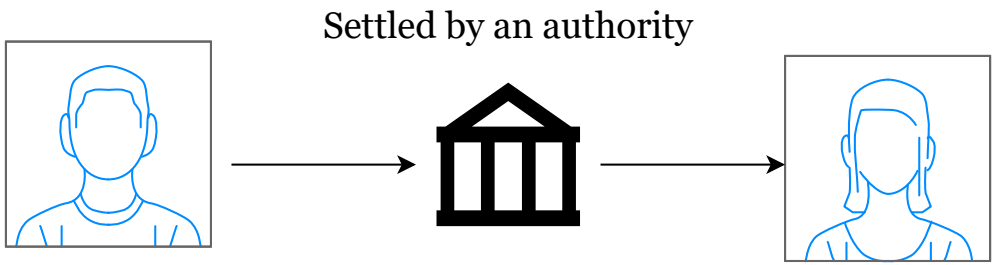


Figure: Bits are easier to copy than paper

Double spending - ways to combat





P2P Cooperative System to combat double spending with Lattice-based blind signatures

P2P $\rightarrow$ *Peer-to-Peer*

A peer-to-peer network

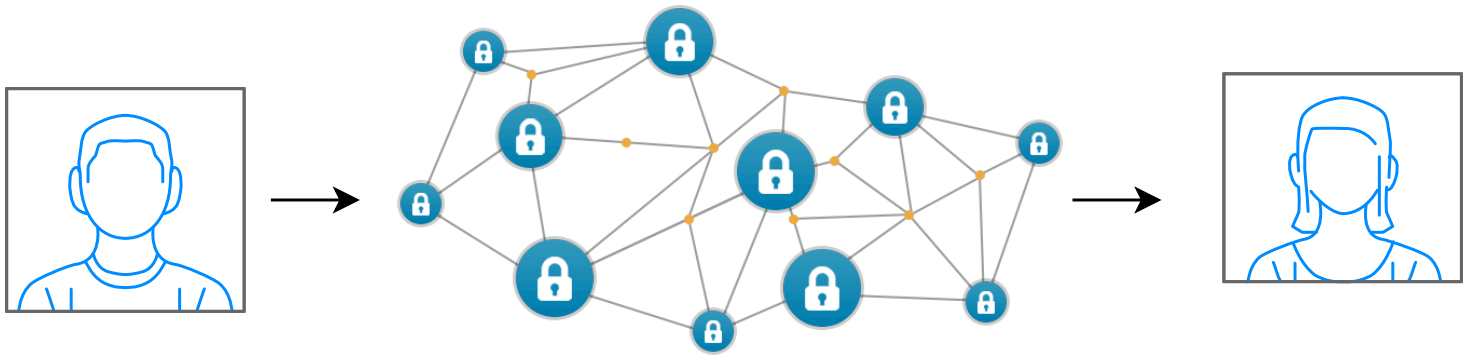


Figure: Transactions are verified by nodes in peer-to-peer network

But why all this?

Observations

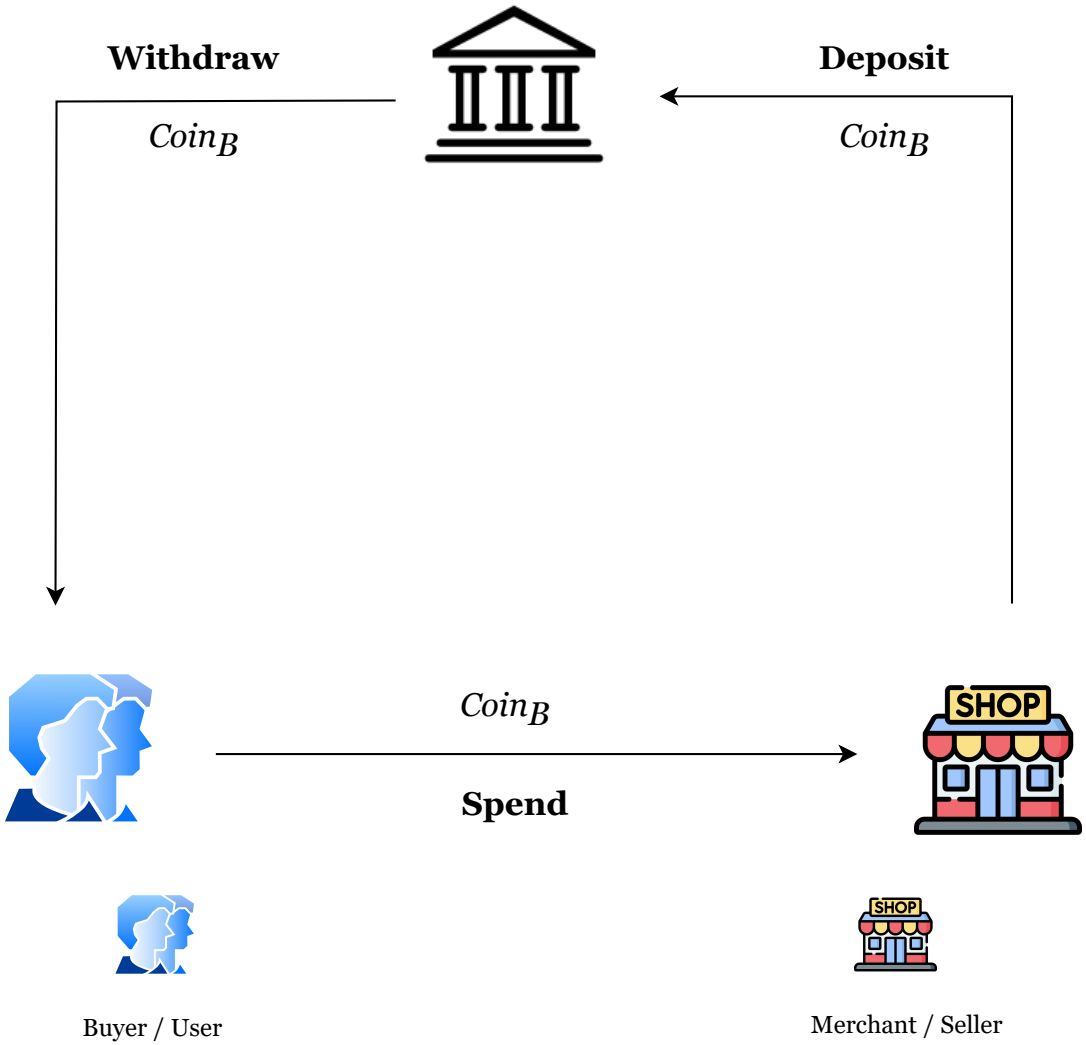
- Blind signature - Chaum first idea was ecash
- Double spending - still an important problem
- Combating in online setting - Easy

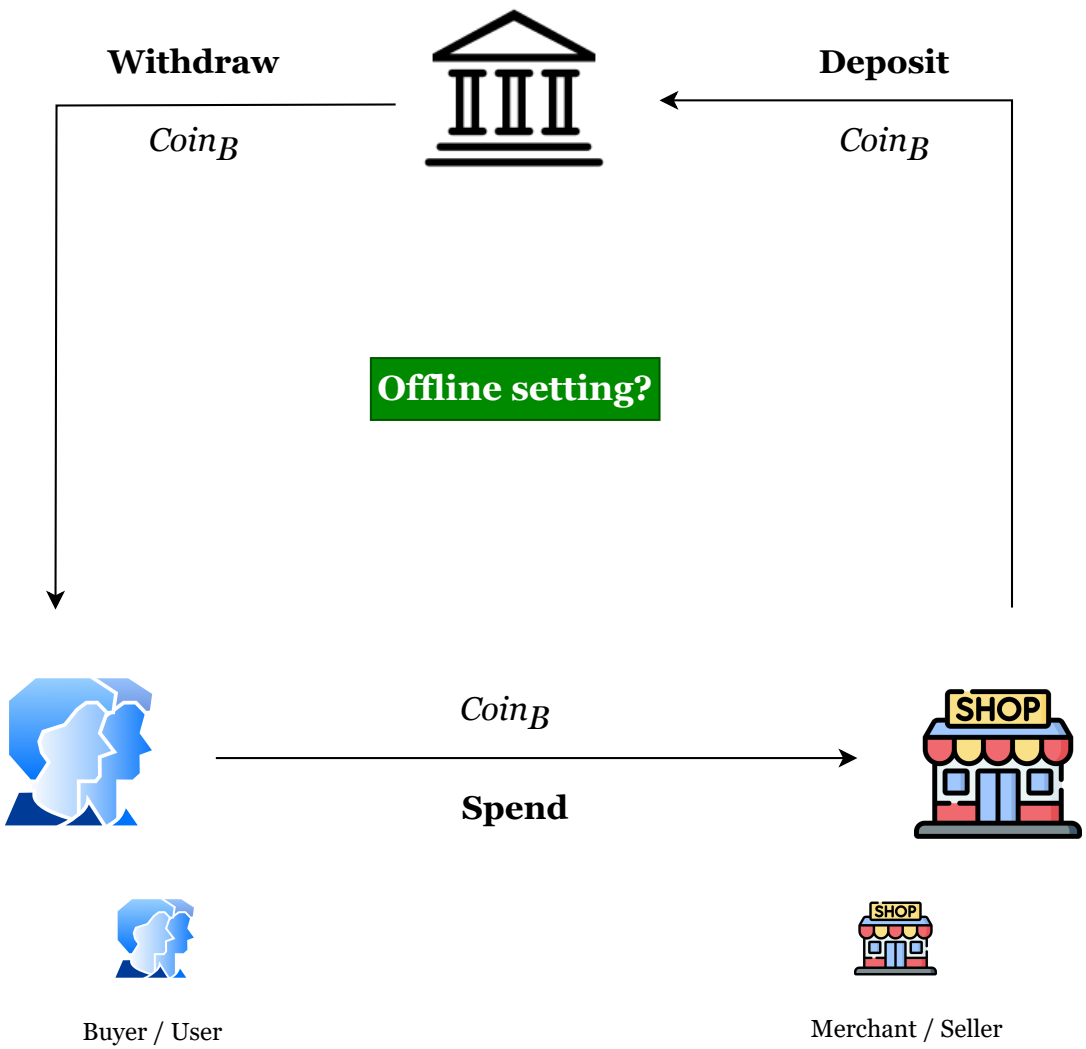
  Combating double spending offline?

A practical Lattice-based ecash scheme

Amit Deo et al. *"Lattice-based E-cash, revisited"* - 2020

- A good starting point
- Gave construction of secure ecash scheme


Withdraw
$Coin_B$
Deposit
$Coin_B$
$Coin_B$
Spend
SHOP
SHOP
Buyer / User
Merchant / Seller


Withdraw
$Coin_B$
Deposit
$Coin_B$
Offline setting?
$Coin_B$
Spend
SHOP
SHOP
Buyer / User
Merchant / Seller

Offline Ecash

"Combating double-spending using cooperative P2P system" - Ivan Osipkov et al. - 2007

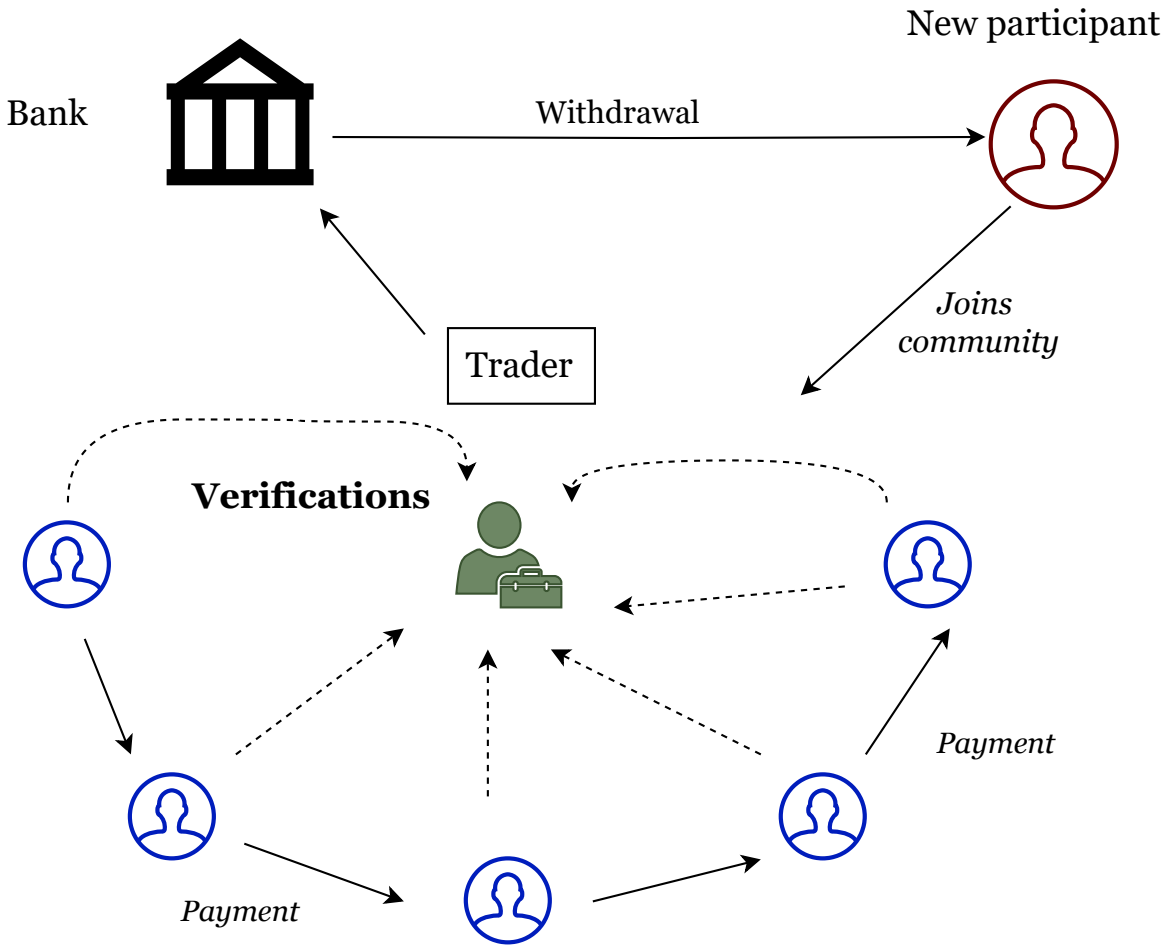
- A coin is assigned a *witness* who signs it before it is considered valid to spend.
- Value of coin is fixed.
- Amounts of $2.59 ?

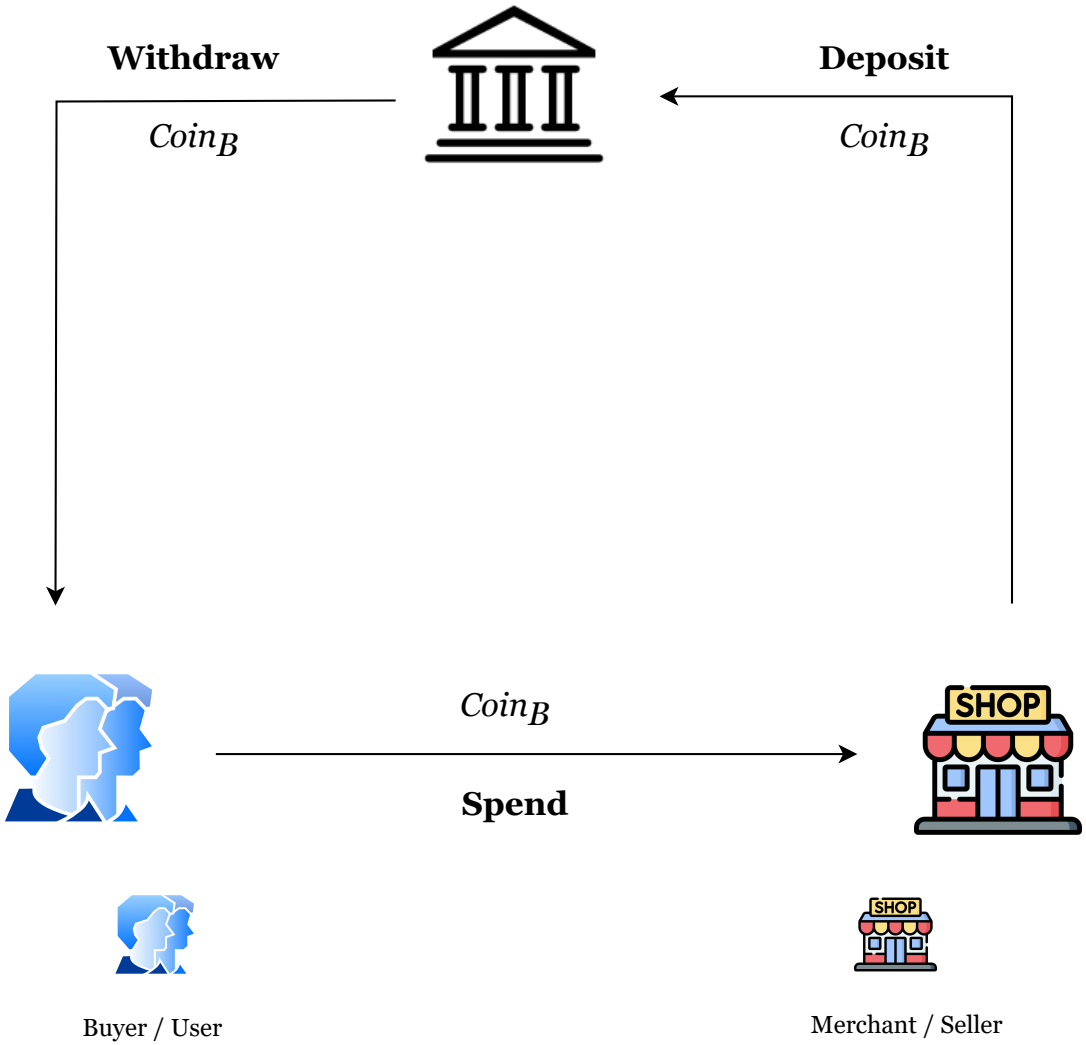
Offline Ecash

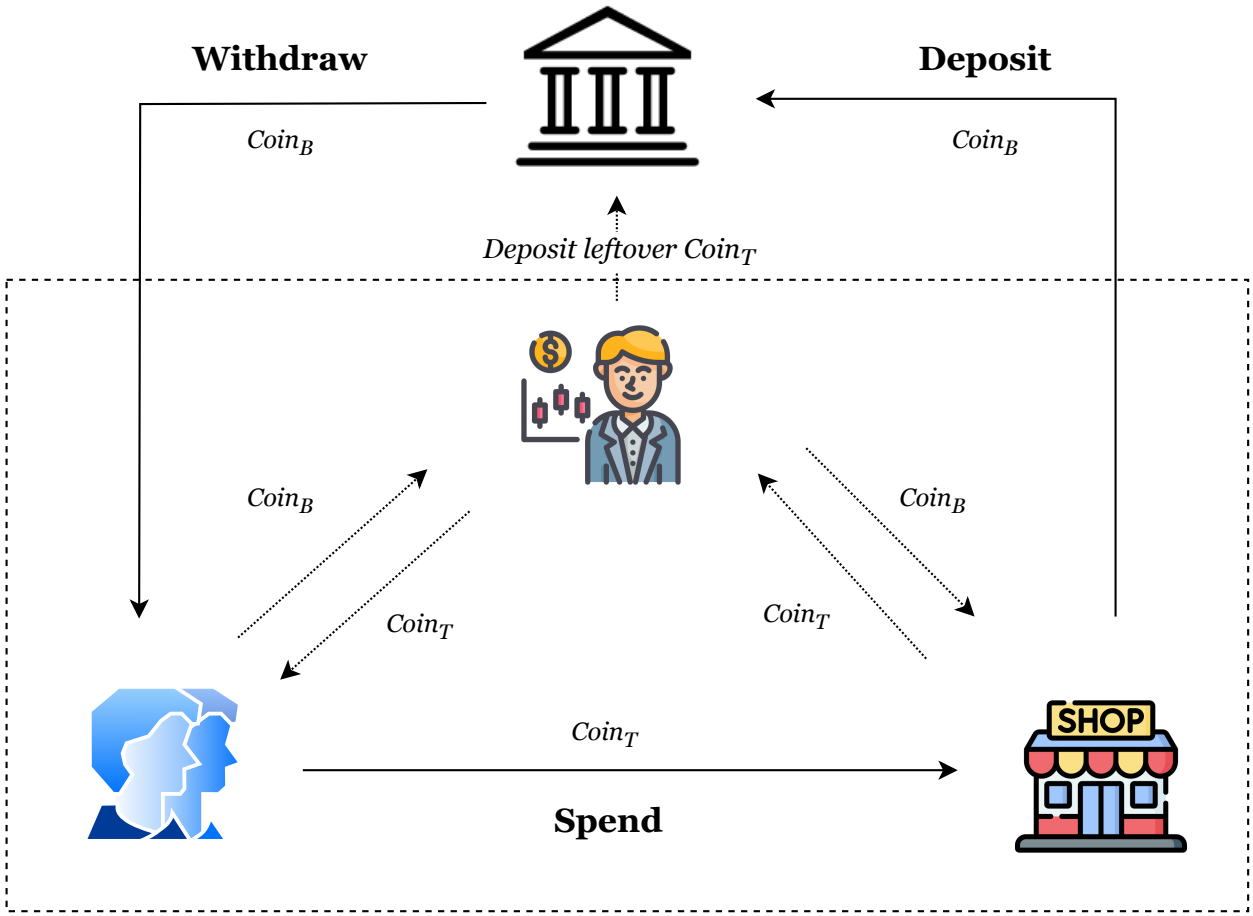
"Double spending protection for e-cash based on risk management
Everaere et al. - 2010

- Divisible ecash
- Trusted 3rd-party - Trader
- People in community - Trader can issue coins and maintains local database

Bank is not online $\rightarrow$ Trader is online


New participant
Bank
Withdrawal
Joins
community
Trader
Verifications
Payment
Payment


Withdraw
$Coin_B$
Deposit
$Coin_B$
$Coin_B$
Spend
SHOP
SHOP
Buyer / User
Merchant / Seller



Buyer / User

Trader

Merchant / Seller

Closing remarks

Thesis - Focuses on the theory and reviewing state of the art

Presentation - Focuses on the **intuition**

Lattices $\rightarrow$ Blind signatures $\rightarrow$ Problem of double spending $\rightarrow$ P2P cooperative system

P2P Cooperative System to combat double spending with Lattice-based blind signatures


Vinod Vaikuntanathan, MIT
Mathematics of Lattice I-II
Cryptography Boot Camp, Simons Institute.


Fabrice Benhamouda et al.
On the (in)Security of ROS
https://doi.org/10.1007/s00145-022-09436-0, 2022.


Everaere et al.
Double spending protection for e-cash based on risk management
International Conference on Information Security, 2010.


Deo et al.
Lattice-Based E-Cash, Revisited
Cryptology ePrint Archive, 2020.