Anonymous Post-quantum Cryptocash

Huang Zhang, Fangguo Zhang, Haibo tian

Sun Yat-sen University, Guangzhou, China

Man Ho Au

The Hong Kong Polytechnic University, Hong Kong, China

E-mail: isszhfg@mail.sysu.edu.cn

Curaçao, FC2018, March 01

Outline

- **Backgrounds and Motivations**

  What is Cryptocash?

  Why Cryptocash from ring signatures?

  Why Post-quantum cryptocash ?

- **Basic tool:**

  Linkable Ring Signature Based on Ideal-Lattices

- **Post-quantum cryptocash from ring signatures**

- **Conclusion**

Cryptocash

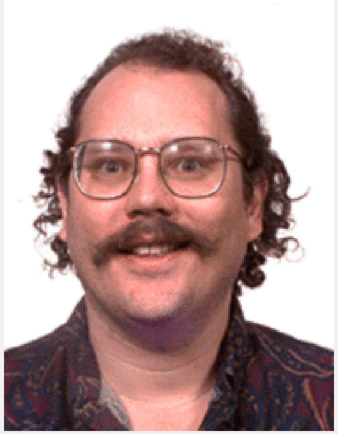
- **Example**
  - Bitcoin
- **Security requirements**
  - Anonymity
  - Unforgeability
  - Avoiding Double-spending
- **Decentralization**
  - POW, POS…

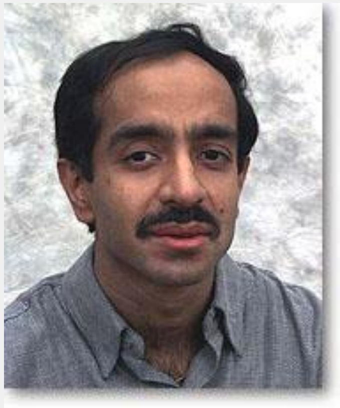
Cryptocash based on signatures VS ring signatures

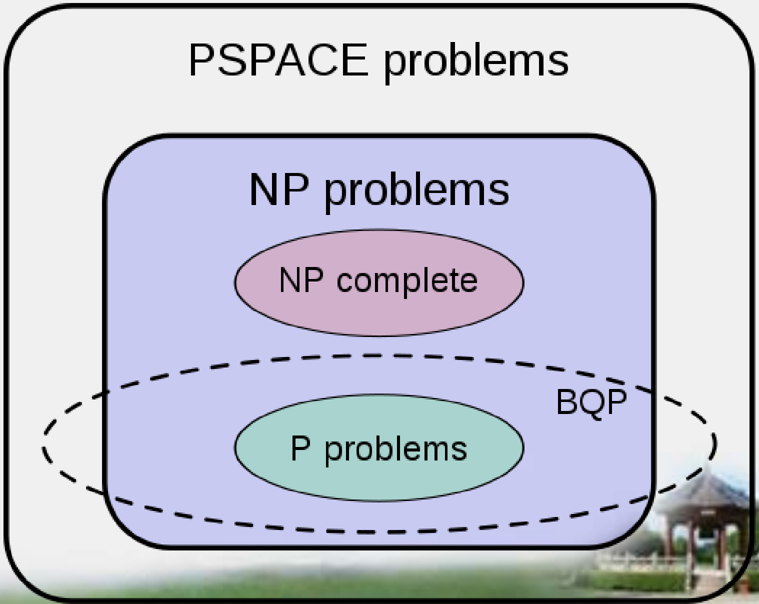
- **Bitcoin——Classic signatures**
  - Relatively weaker anonymity [OKJ2013], [RS2013]
  - Allowance for key reusage
- **Monero (CryptNote)——Ring signatures**
  - Relatively stronger anonymity
  - Enforcement of one-time keys
  - Tradeoff between efficiency and anonymity

Quantum Algorithms

- 1994, Shor's algorithm [S1994]:
  - for solving IF and DLP
  - Quantum Fourier transformation
- 1995, Grover's Algorithm:
  - Quadratic speedup for searching
- The problem class BQP:
  - "Bounded-error Quantum Polynomial time"
  - IF, DLP∈BQP

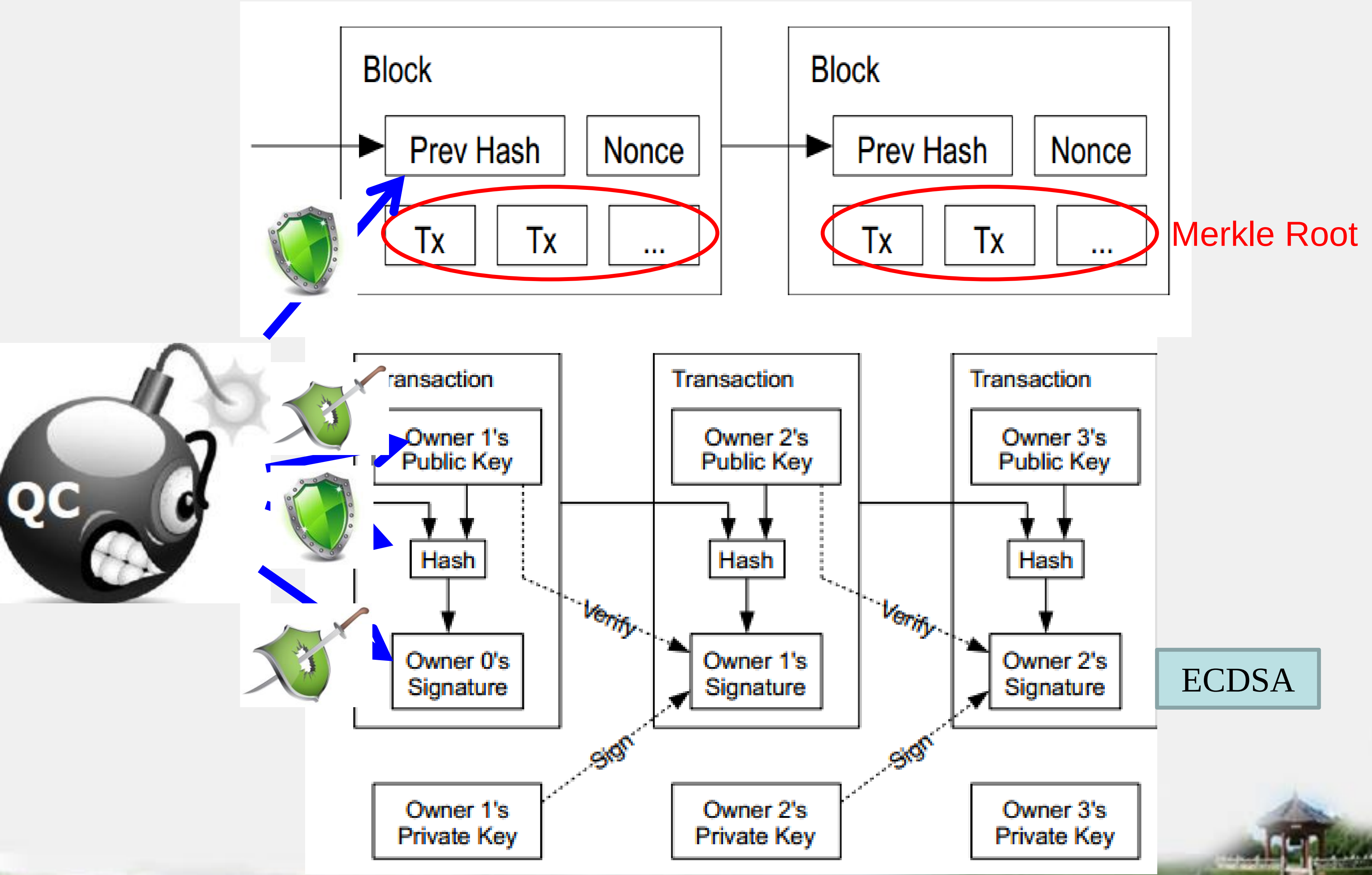






Cryptography is not over yet！

Why Post-quantum cryptocash?



How Post-quantum cryptocash?

- **Double Hash size**
- **Replace ECDSA using post-quantum signature**
- **Traditional cryptography schemes → Post quantum schemes, if necessary**

Post-quantum Cryptography

- Hash-based
- Code-based
- Lattice-based
- Multivariate-quadratic-polynomial-based
- Elliptic-Curve-Isogeny-based
- Symmetric cryptography (AES)

NIST
National Institute of Standards and Technology

NISTIR 8105

Report on Post-Quantum Cryptography

Lily Chen
Stephen Jordan
Yi-Kai Liu
Dustin Moody
Rene Peralta
Ray Perlner
Daniel Smith-Tone

Why lattice?

The similarity between ISIS and DLP：

ISIS problem:
$\mathbf{Ay} = \mathbf{b}$

DL problem:
$g^y = b$

$||y||<\delta$

Implementation	Security	Signature Size	SK Size	PK Size	Sign (ms)	Sign/s	Verify (ms)	Verify/s
BLISS-0	$\leqslant$ 60 bits	3.3 kb	1.5 kb	3.3 kb	0.241	4k	0.017	59k
BLISS-I	128 bits	5.6 kb	2 kb	7 kb	0.124	8k	0.030	33k
BLISS-II	128 bits	5 kb	2 kb	7 kb	0.480	2k	0.030	33k
BLISS-III	160 bits	6 kb	3 kb	7 kb	0.203	5k	0.031	32k
BLISS-IV	192 bits	6.5 kb	3 kb	7 kb	0.375	2.5k	0.032	31k
RSA 1024	72-80 bits	1 kb	1 kb	1 kb	0.167	6k	0.004	91k
RSA 2048	103-112 bits	2 kb	2 kb	2 kb	1.180	0.8k	0.038	27k
RSA 4096	$\geqslant$ 128 bits	4 kb	4 kb	4 kb	8.660	0.1k	0.138	7.5k
ECDSA[1] 160	80 bits	0.32 kb	0.16 kb	0.16 kb	0.058	17k	0.205	5k
ECDSA 256	128 bits	0.5 kb	0.25 kb	0.25 kb	0.106	9.5k	0.384	2.5k
ECDSA 384	192 bits	0.75 kb	0.37 kb	0.37 kb	0.195	5k	0.853	1k

Table 1. Benchmarking on a desktop computer (Intel Core i7 at 3.4Ghz, 32GB RAM) with openssl 1.0.1c

Signatures from lattice and DLP

Lyubashevsky's lattice-based signature

Signing key: **S**

Verifying key: **A, b=AS**

Sign:
1. randomness $\mathbf{y} \leftarrow D_{Z^m,\sigma}$
2. compute $\mathbf{c} \leftarrow H(\mathbf{Ay}, msg)$
3. compute $\mathbf{z} \leftarrow \mathbf{Sc}+\mathbf{y}$
4. output $(\mathbf{z}, \mathbf{c})$ with some probability

Verify:
1. $\mathbf{z}$ is short enough
2. test $\mathbf{c} = H(\mathbf{Az}-\mathbf{bc}, msg)$

Schnorr's signature

Signing key: S

Verifying key: g, $b=g^S$

Sign:
1. randomness $y \leftarrow Z_q$
2. compute $c \leftarrow H(g^y, msg)$
3. compute $z \leftarrow Sc+y \bmod q$
4. output (z, c)

Verify:
test $c=H(g^z/b^c, msg)$

Why linkable ring signature?

- **Ring signature**
  - Hiding the real signing key
  - Whether it signing again --- Double spending
- **Linkable ring signature**
  - Signatures generated by the same signing key
  - Detect!

Main Contribution

- A linkable ring signature from ideal lattices
- A key-generation protocol to support stealth addresses
- Post quantum cryptocash

Linkable ring signature from ideal lattices

- Depending on the work of Groth and Kohlweiss [GK15]
  - Signature size: O(log N)
  - Homomorphic commitments
- Based on ideal lattices
  - $R=\mathbb{Z}_q[x]/<f>$
  - f is monic in $\mathbb{Z}[x]$
  - Lattice $\mathcal{L} = \{ g \bmod f : g \in \mathcal{I} \}, \mathcal{I} \in R$
  - $D=\{g \in R, \|g\| < t\}$, polynomials with small infinite norms
  - $D'=\{g \in R, \|g\| < t-1\}$

Linkable ring signature from ideal lattices

- **Gernalized knapsack function[M02]**
  - $\mathbf{A}^T\mathbf{X} = \mathbf{B}$, $\mathbf{A} \in R^m$, $\mathbf{X} \in D^m$
- **The output distribution [M02]**
  - If $\mathbf{X}$ is uniformly distributed in D^m, then $\mathbf{B}$ is uniformly distributed in R
- **Collision problem [LM06]**
  - given $\mathbf{A}$, to find $\mathbf{X_1}$, $\mathbf{X}_2$ such that $\mathbf{A}^T\mathbf{X}_1 = \mathbf{A}^T\mathbf{X}_2$ is difficult
  - Collision problem is as hard as the SVP in an ideal lattice

Linkable ring signature from ideal lattices

Pedersen Commitment	Counterpart from ideal lattices
$C = Gm + Hr$	$C = GM + HR$

Hiding:
$r \leftarrow \mathcal{U}(\mathbb{Z}_p)$
Then
$Hr \leftarrow \mathcal{U}(\mathbb{G})$
So is C

Hiding: For particular parameters
$R \leftarrow \mathcal{U}((S^n)^m)$
Then
$HR \leftarrow \mathcal{U}(\mathbb{F}^n)$
So is C

Binding:
$Gm_1 + Hr_1 = Gm_2 + Hr_2$
Then
$G = H\,(r_2 - r_1) / (m_1 - m_2)$
Solving
$\log_G H$

Binding:
$GM_1 + HR_1 = GM_2 + HR_2$
Then
$H(R_1 - R_2) = G(M_2 - M_1)$
Solving
Collision problem

Linkable ring signature from ideal lattices

- Constructing a NIZK for the commitment to 0 or 1
- Fixing that the signer is the lth user
  - The ring involves N user, and requires log N bits to represent it
  - Repeating the forgoing NIZK log N times to fix l
- Proving that the signer holds the lth secret key
  - Generating a value which can only be computed from the parameters to fix l and the lth secret key
- Adding a value for Linking
  - The validity of the value for Linking is ensured in the verification process

Linkable ring signature from ideal lattices

l^{th} user | verifier

$pk_i = \mathbf{Y}_i = \mathbf{G}\mathbf{X}_i$ $\quad L=(\mathbf{Y}_0,\ldots,\mathbf{Y}_{N-1})$

$sk_l = \mathbf{X}_l \in D^{m\times m}$ $\quad M = \log N$

$\mathbf{V}_j$ is the commitment for 0 or 1

Initial messsage

For 1 = 1,…, M

$\mathbf{K}_j, \mathbf{C}_j, \mathbf{D}_j, \mathbf{E}_j \leftarrow D^{m\times m}$

$\mathbf{B}_j \leftarrow D^{m\times m}$, if $l_j = 0$

$\mathbf{B}_j \leftarrow D'^{m\times m}$, if $l_j = 1$

$\mathbf{V}_j \leftarrow \mathbf{H}(l_j\mathbf{I}) + \mathbf{G}\mathbf{K}_j$

$\mathbf{V}_{aj} = \mathbf{H}\mathbf{B}_j + \mathbf{G}\mathbf{C}_j$

$\mathbf{V}_{bj} = \mathbf{H}(l_j\mathbf{B}_j) + \mathbf{G}\mathbf{D}_j$

$\mathbf{V}_{dk} = \Sigma_i \mathbf{Y}_i \mathbf{P}_{i,k} + \mathbf{G}\mathbf{E}_k$

$\mathbf{V'}_{dk} = \mathbf{H}\mathbf{E}_k$

$\mathbf{R}_l = \mathbf{H}\mathbf{X}_l$

Fiat-Shamir challenge

$S_1 = \{\mathbf{V}_j, \mathbf{V}_{aj}, \mathbf{V}_{bj}, \mathbf{V}_{dj-1}, \mathbf{V'}_{dj-1}\}_j$

$x = H(pp, u, L, S_1, \mathbf{R}_l)$

Response

For j = 1,…,M

$\mathbf{W}_j = l_j x\mathbf{I} + \mathbf{B}_j$

$\mathbf{Z}_{aj} = \mathbf{K}_j(x\mathbf{I}) + \mathbf{C}_j$

$\mathbf{Z}_{bj} = \mathbf{K}_j(x\mathbf{I} - \mathbf{W}_j) + \mathbf{D}_j$

$S_2 = \{\mathbf{W}_j, \mathbf{Z}_{aj}, \mathbf{Z}_{bj}\}_j$

$\mathbf{Z}_d = \mathbf{X}_l(x^M\mathbf{I}) - \Sigma_k \mathbf{E}_k x^k$

$S_1, S_2, \mathbf{Z}_d, \mathbf{R}_l, L \rightarrow$

Verification

For j = 1,…,M

$\mathbf{V}_j(x\mathbf{I}) + \mathbf{V}_{aj} = \mathbf{H}\mathbf{W}_j + \mathbf{G}\mathbf{Z}_{aj}$

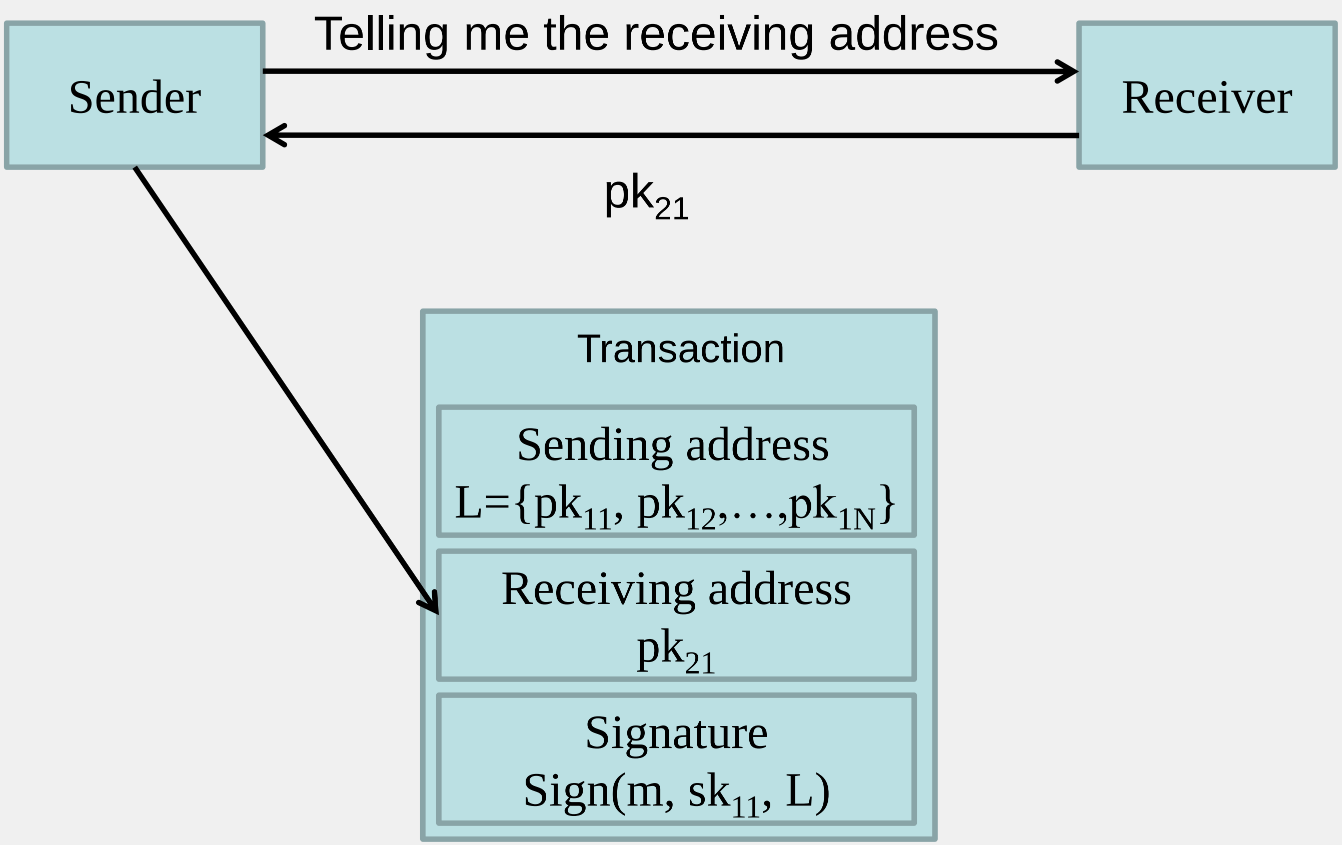
$\mathbf{V}_j(x\mathbf{I} - \mathbf{W}_j) + \mathbf{V}_{bj} = \mathbf{G}\mathbf{Z}_{bj}$

$\mathbf{W}_j, \mathbf{Z}_{aj}, \mathbf{Z}_{bj}$, are short

$\Sigma_i(\mathbf{Y}_i \prod_j \mathbf{W}_{j,i_j}) + \Sigma_k \mathbf{V}_{dk}(-x^k) = \mathbf{G}\mathbf{Z}_d$

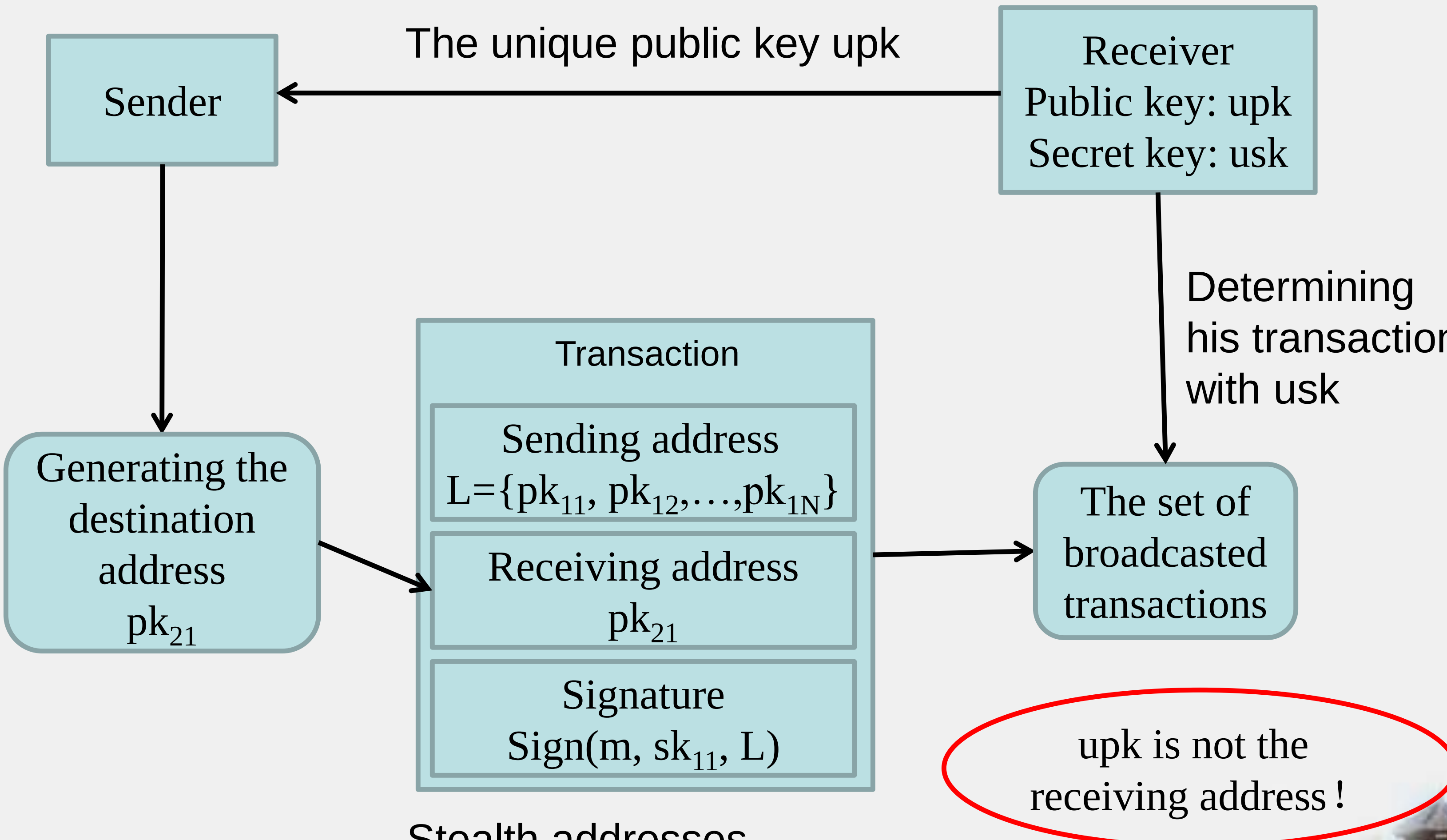
$\mathbf{R}_l(x^M\mathbf{I}) + \Sigma_k \mathbf{V'}_{dk}(-x^k) = \mathbf{H}\mathbf{Z}_d$

Stealth addresses



The traditional method to select receiving address

Stealth addresses

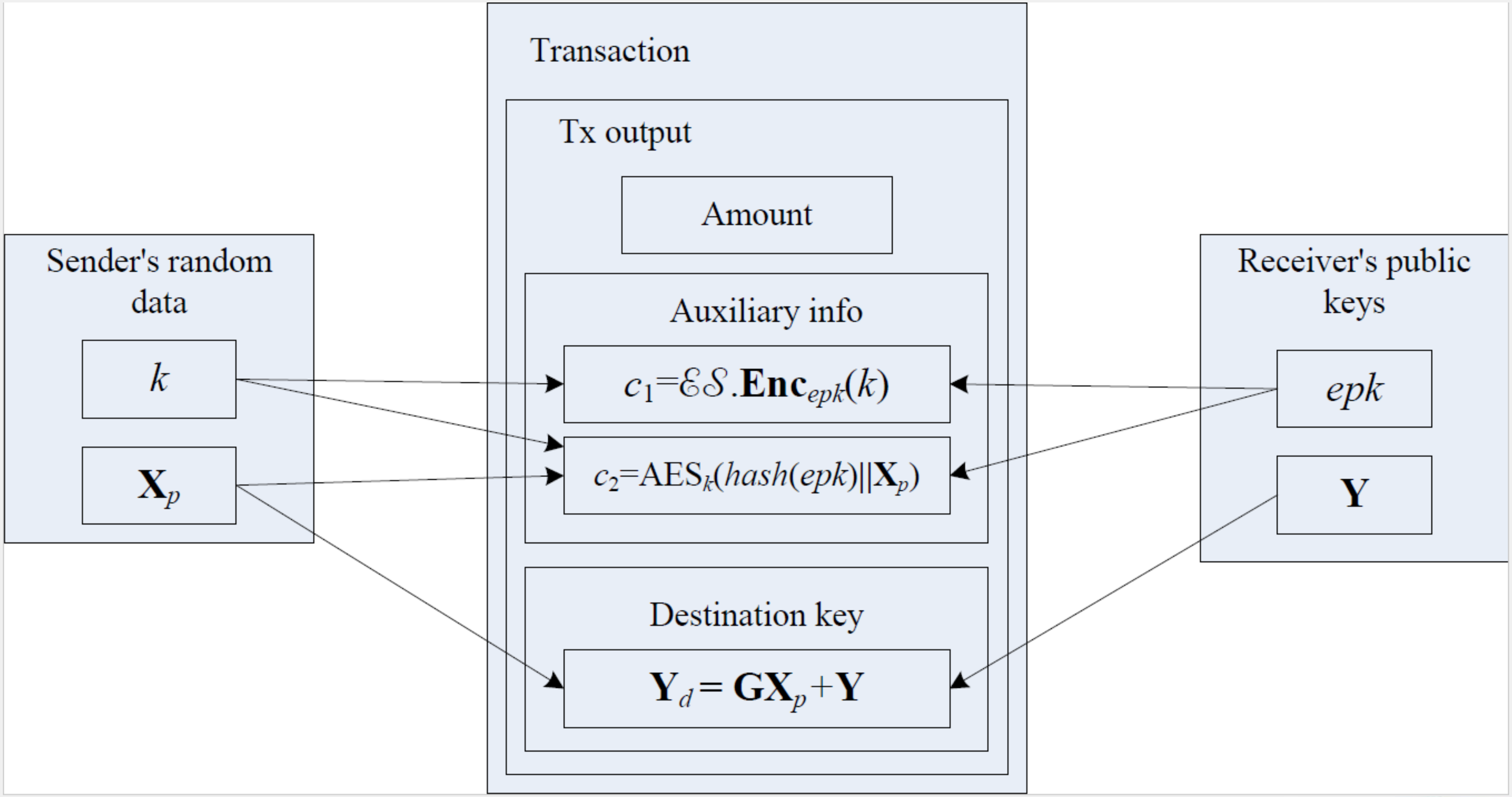


Stealth addresses

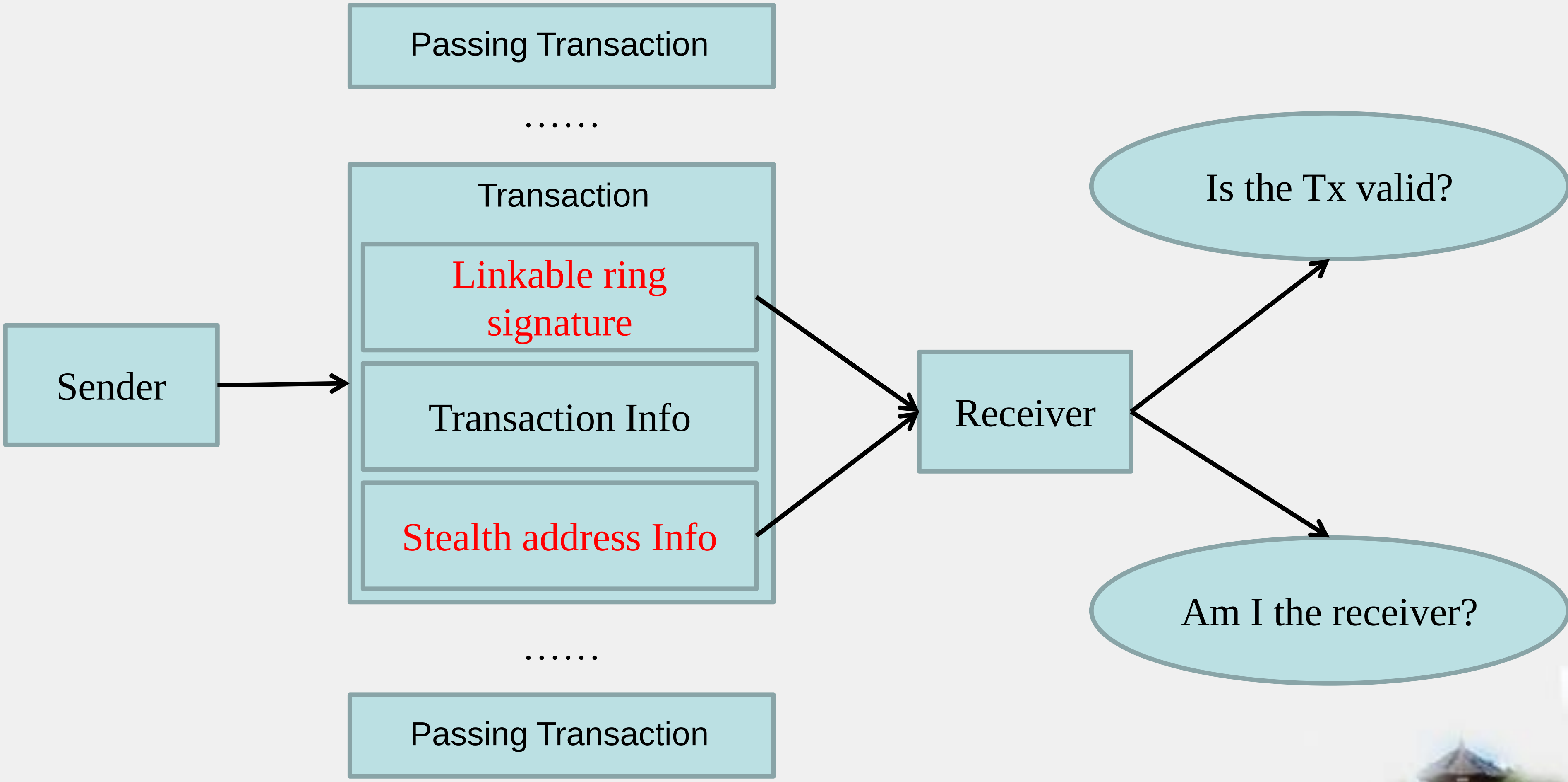
Stealth addresses

- **The idea in CryptoNote**
  - Diffie-Hellman key exchange
  - The shared key is distributed uniformly at random
- **Our requirements**
  - The partial key : matrix with small norm

Stealth addresses (Generation)



Post-quantum cryptocash from ring signatures



Post-quantum cryptocash from ring signatures

- **Advantages**
  - Quantum resilient
  - Relatively strong anonymity
  - Short signature size
- **Disadvantages**
  - No implementation
  - No confidential transactions
- **The ECDLP based version(full version of FC paper)**
  - Confidential transaction
  - Boolberry v2

Boolberry v2

- **Linkable ring signature from ECDLP**
  - Signature size: O(log N)
- **Stealth addresses**
  - The same as that of Monero (slight modifications)
- **Compact Confidential transaction**
  - Proof of sum: the same as RingCT in Monero
  - Range proof: Bulletproofs [BBBP+2017]
- **Multi-signatures**
  - Without a script
  - Adapt to ring signatures

Conclusion

- **A short linkable ring signature from ideal lattices**
- **A key-generation protocol to support stealth addresses**
- **Post quantum cryptocash**

Thank you!

We are grateful to receive suggestion and questions!

E-mail: isszhfg@mail.sysu.edu.cn