HKU Coin: Towards Decentralized Privacy-Preserving Cryptocurrency with Accountability

Dr. Allen Au (allenau@cs.hku.hk)
Associate Professor
Department of Computer Science
Faculty of Engineering
Outline

• Background
• Requirements of HKU Coin
• Design Philosophy of HKU Coin
• Building Blocks
  • Homomorphic Encryption - Twisted ElGamal Encryption
  • Ring Signatures - DualRing
• Conclusion
Background
Privacy in Payment System

Alice → $100 → Bob

Privacy

- Sender Anonymity
- Transaction Confidentiality
- Receiver Anonymity
Accountability in Payment System
Centralized Payment System

- txs are kept on a private ledger managed by a central authority (e.g., bank)
- The authority is responsible for **validity check**, conduct **audit**, as well as **privacy protection**
Decentralized Payment System (Blockchain-Based Cryptocurrencies)

• txs are kept on a global distributed public ledger - blockchain
• To allow validity check by all nodes in the system, blockchain-based cryptocurrencies Bitcoin and Ethereum, among others, simply expose all tx information publicly, i.e., there is no privacy in these systems
Motivation of HKU Coin

- Privacy and Accountability are crucial in any financial system

Global Financial Crisis
Bankruptcy of Lehman Brothers

2008-2009

Ethereum
New cryptocurrencies emerge, including Ethereum

2016

Bitcoin
The birth of the first cryptocurrency, Bitcoin, and the first Bitcoin transaction occurred in 2009

Private cryptocurrencies
Privacy-oriented cryptocurrencies are created, like Monero and ZCash

Developments in the world of cryptocurrency
There are now more than 2,000 tradable cryptocurrencies

2020
Can we achieve privacy and accountability simultaneously in the decentralize setting?
Requirements of HKU Coin
HKU Coin: Design Goal

• A blockchain-based decentralized cryptocurrency to provide privacy and accountability simultaneously
  • Account-Based Model
  • Sender Anonymity
  • Receiver Anonymity
  • Transaction Confidentiality
  • Decentralization
  • Accountability
Simplified System Model

Confidential Tx

Validity check

miners

Audit

$ f(\{tx_i\}) = 1 ?$
Security Requirements

• Public Verifiability - validity of txs are publicly verifiable
• Authenticity – only the sender can generate txs
• Soundness – no one can generate an illegal tx that passes verification
• Confidentiality – no one can learn the transfer amount
• Anonymity* - no one can learn the identity of the sender and receiver
• Accountability – auditor can conduct audit, users cannot provide incorrect information about all txs it has participated

*we consider a strong form of anonymity which requires that actions from the same user are unlinkable
Design Philosophy of HKU Coin
Building Blocks of our Construction

- Verifiability
- Authenticity
- Soundness
- Confidentiality
- Anonymity
- Accountability

- Additively Homomorphic Encryption
- Ring Signatures
- Zero-Knowledge Proofs
Confidentiality

• All account balances are encrypted by an additively Homomorphic Encryption (HE) so that only the owner can review the details.

\[
\begin{align*}
M_1 &\rightarrow \text{ENC}(M_1) \\
M_2 &\rightarrow \text{ENC}(M_2) \\
\text{ENC}(M_1) + \text{ENC}(M_2) &\rightarrow \text{ENC}(M_1 + M_2)
\end{align*}
\]

<table>
<thead>
<tr>
<th>Account Balance</th>
<th>ENC(M1)</th>
<th>ENC(M2)</th>
<th>ENC(M1 + M2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>16</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Account Balance in Blockchain:

<table>
<thead>
<tr>
<th>Account Balance</th>
<th>ENC(M1)</th>
<th>ENC(M2)</th>
<th>ENC(M1 + M2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Enc(18)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>Enc(22)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>Enc(32)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>Enc(18)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>Enc(16)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Twisted El Gamal Encryption

Joint work with Yu Chen, Xuecheng Ma and Cong Tang
Twisted El Gamal Encryption

- Public Parameter: $g$
- Public / Secret key: $(pk, sk) = (g^x, x)$
- Encryption: $(c_1, c_2) = (g^m pk^r, g^r)$
- Decryption: $g^m := c_1 c_2^{-x}$, solve* DL of $g^m$

- Public Parameter: $g, h$
- Public / Secret key: $(pk, sk) = (g^x, x)$
- Encryption: $(c_1, c_2) = (h^m g^r, pk^r)$
- Decryption: $h^m := c_1 c_2^{\frac{-1}{x}}$, solve* DL of $h^m$

* Assume $m$ is small

The same format as a Pedersen Commitment. Can use ZKP directly

ElGamal Encryption  \[\rightleftharpoons\] Twisted ElGamal Encryption

As secure and efficient as the original ElGamal Encryption
Twisted ElGamal

Comparison with State-of-the-Art PHE (Paillier Encryption)

<table>
<thead>
<tr>
<th>Scheme</th>
<th>KeyGen</th>
<th>Encryption</th>
<th>Decryption</th>
<th>Addition</th>
<th>Key Size</th>
<th>Ciphertext Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paillier</td>
<td>1644.53ms</td>
<td>32.211ms</td>
<td>31.367ms</td>
<td>0.0128ms</td>
<td>374 bytes</td>
<td>768 bytes</td>
</tr>
<tr>
<td>Twisted ElGamal</td>
<td>0.0151ms</td>
<td>0.114ms</td>
<td>1ms</td>
<td>0.0031ms</td>
<td>33 bytes</td>
<td>66 bytes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scheme</th>
<th>One-time Setup Cost</th>
<th>Public Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paillier</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Twisted ElGamal</td>
<td>56s</td>
<td>66 bytes</td>
</tr>
</tbody>
</table>

Assume 32-bit message space
DualRing

Joint work with Tsz Hon Yuen, Muhammed F. Esgin, Joseph K. Liu and Zhimin Ding

Slides adapted from Joseph K. Liu’s presentation
Ring Signatures

I know one of you leaked the information. But which of you was it?

We have a secret.
Signed,
A member of the crypto team
Conclusions

• We present the design of HKU coin, an account-based, efficient privacy-preserving decentralized cryptocurrencies with accountability
• Simple & Modular
• Transparent Setup
Future Work

• Allow users to generate audit report by himself/herself
• More complex audit policy
• Ensure rightful use of data by auditors
• Post-Quantum Security
Timeline

PHASE I

Design of HKU Coin

Jun 2020

PHASE II

Enhance Scalability & Auditor Responsibility

Jul 2021

PHASE III

Post-quantum Security

Jul 2022

Proof-of-Concept Implementation

Jul 2023
References


Questions and comments are welcome!

Project Team Members
Dr. Allen Au
Ms. Karina Ko
Mr. Franky Lau
Ms. Mengling Liu
Dr. Xingye Lu