SHANGHAI JIAO TONG UNIVERSITY

A Universally Composable Non-Interactive Aggregate Cash System

Yanxue Jia, Shi-Feng Sun, Hong-Sheng Zhou, Dawu Gu

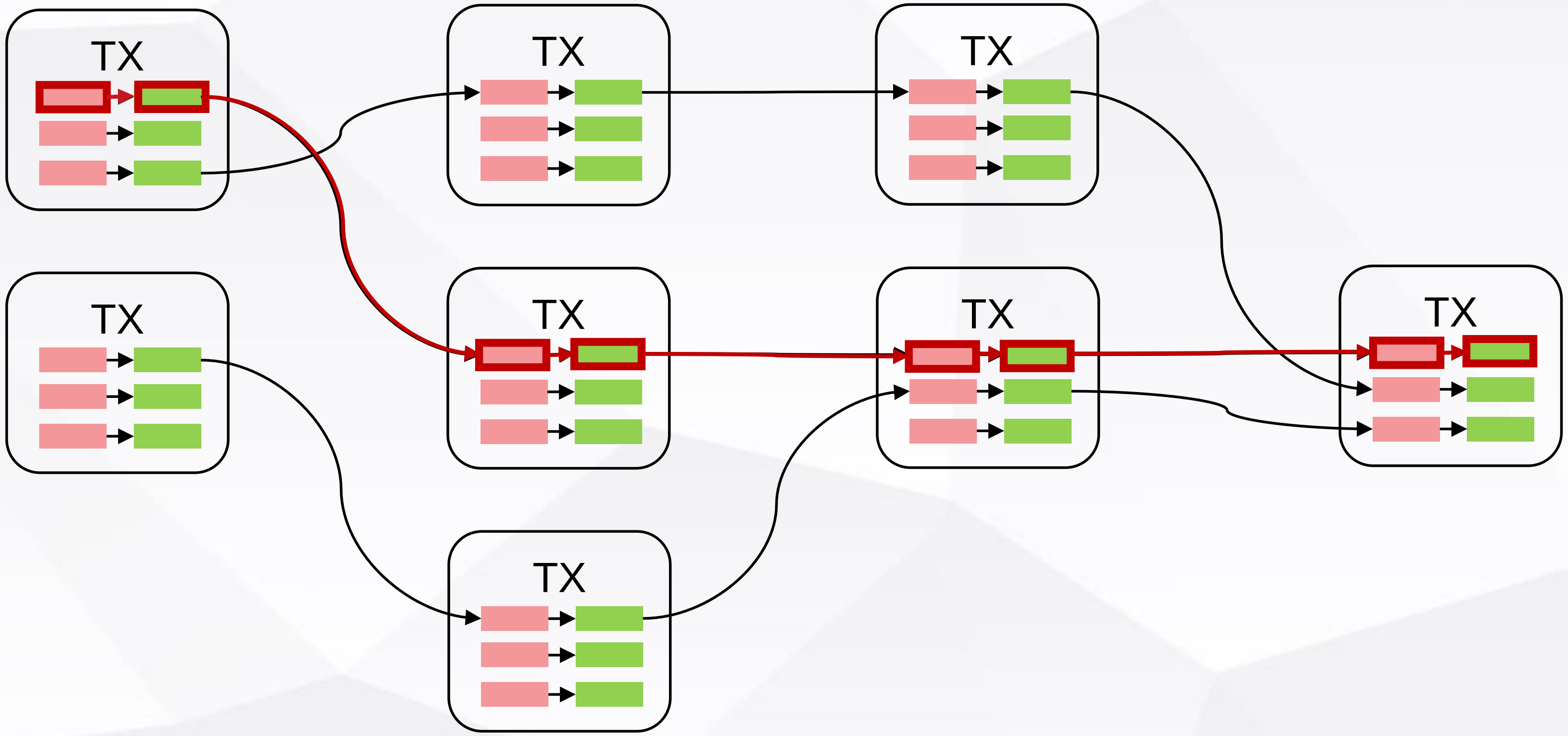
饮 水 思 源 • 爱 国 荣 校

Contents

SJTU

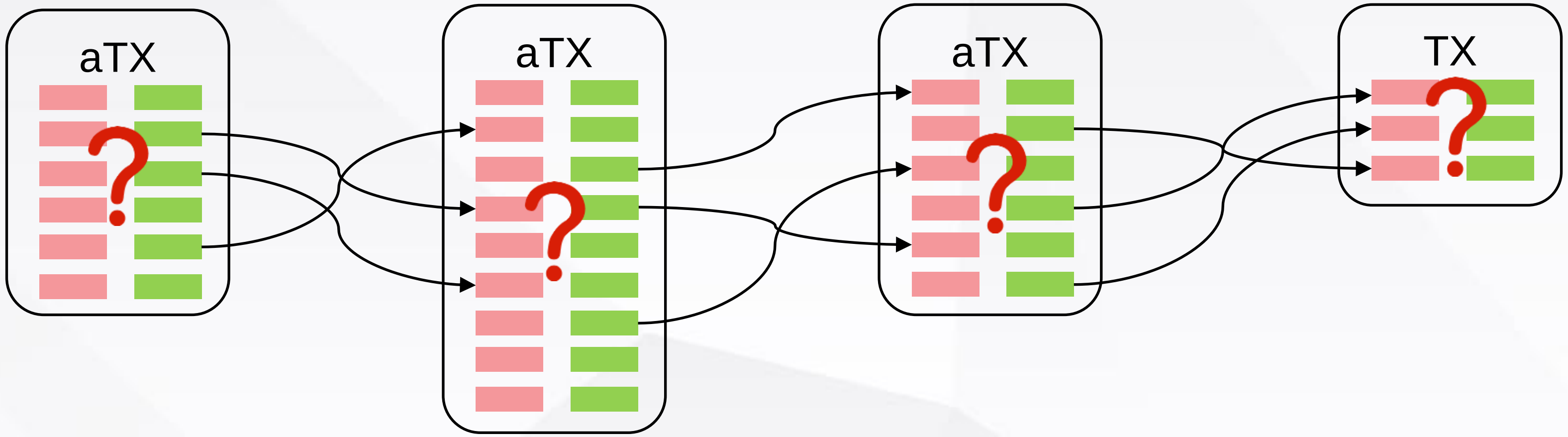
Recall Mimblewimble

Transaction Graph

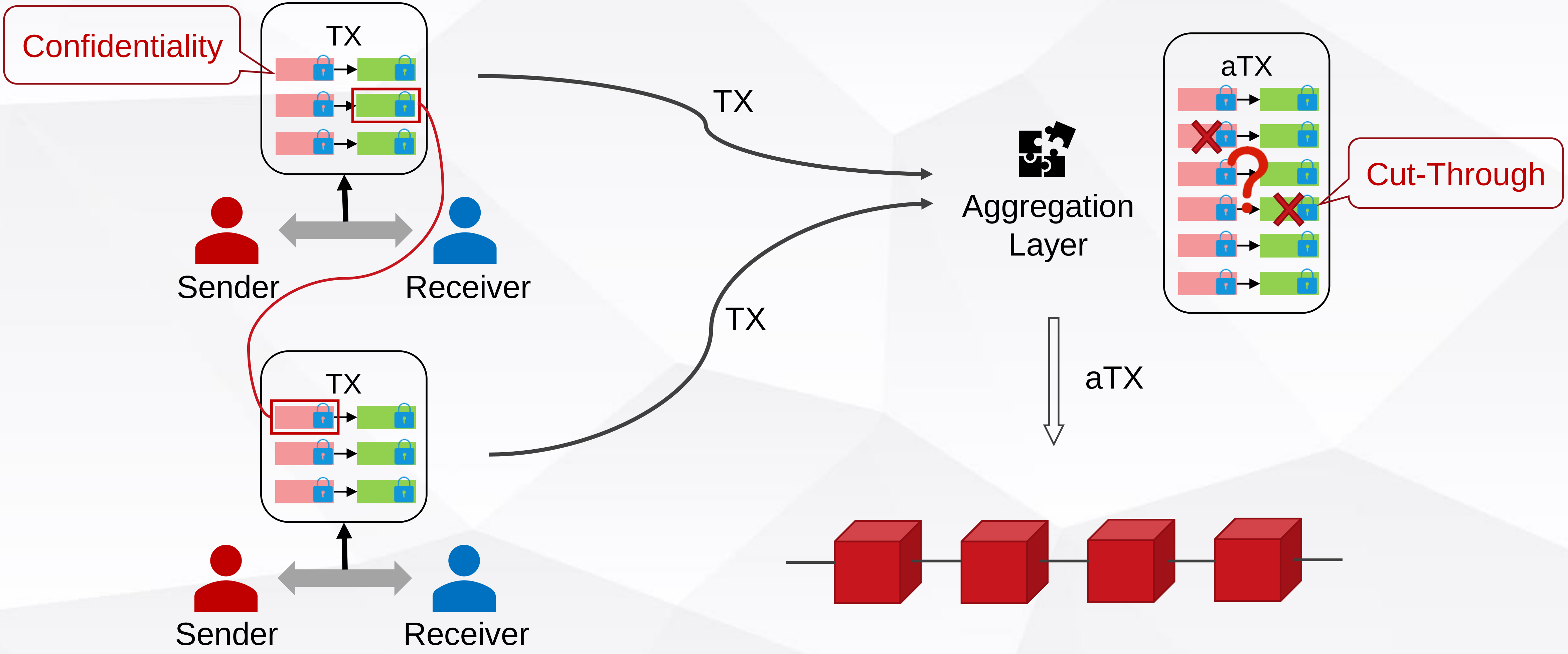


Recall Mimblewimble

CoinJoin

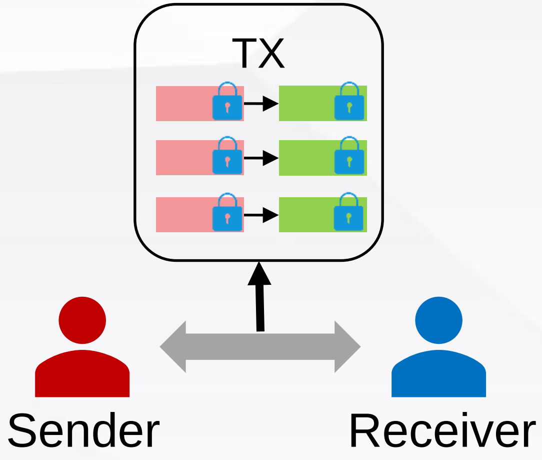


Recall Mimblewimble



Recall Mimblewimble

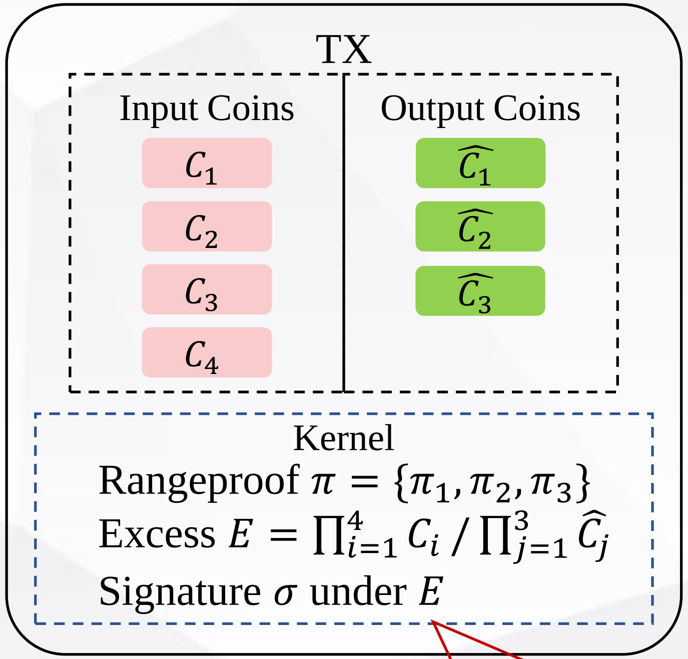
Drawback: Interactive Payment



Sender and Receiver must interact to generate a transaction.

⇩

Sender and Receiver have to be online simultaneously. ☹



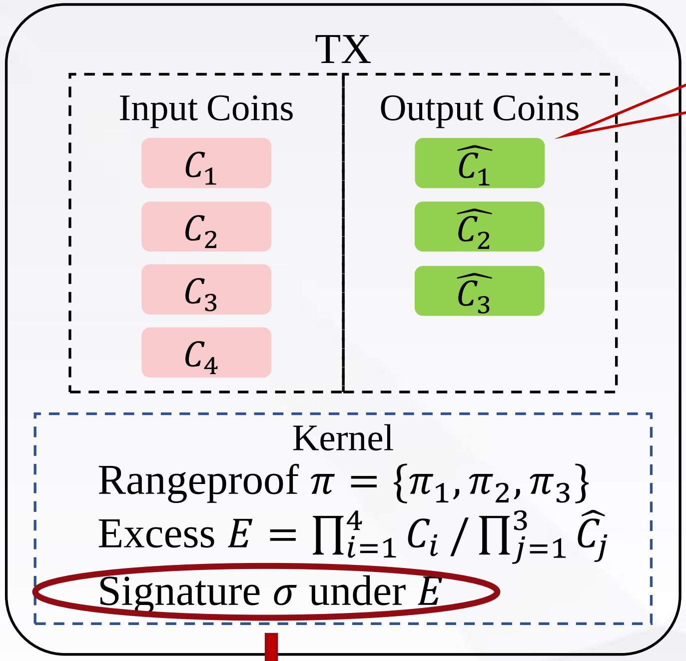
Each party holds a part of the signing key.

Our Contributions

- Design a non-interactive Aggregate Cash System (NiACS) Π_{NiACS} in a hybrid model.
- Formalize an ideal functionality $\mathcal{F}_{NiACS}$ for NiACS.
- Prove that our Π_{NiACS} can securely realize $\mathcal{F}_{NiACS}$ under the Universal Composition (UC) framework.

Our Non-interactive Aggregate Cash System

The essential reason why each party holds a part of the signing key



$C = g^r h^a$, r is the spending key.

⇓

The sender cannot know the spending keys of the output coins.

- The transaction is balanced;
- The sender knows the spending keys of the input coins;

Separate

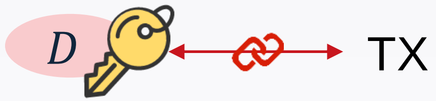
Adding the notion of address to achieve non-interaction

C	D
⇓	⇓
Signature σ_E under E	Signature σ_D under D
⇓	⇓
The transaction is balanced.	The sender knows the spending key of the input coin.

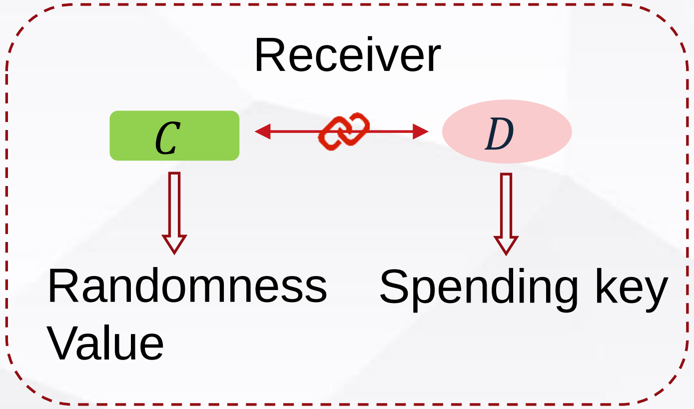
Challenges of Achieving Non-interaction

- How to bind a commitment and an address;

- How to bind the proof of the ownership of input coins with the transaction;

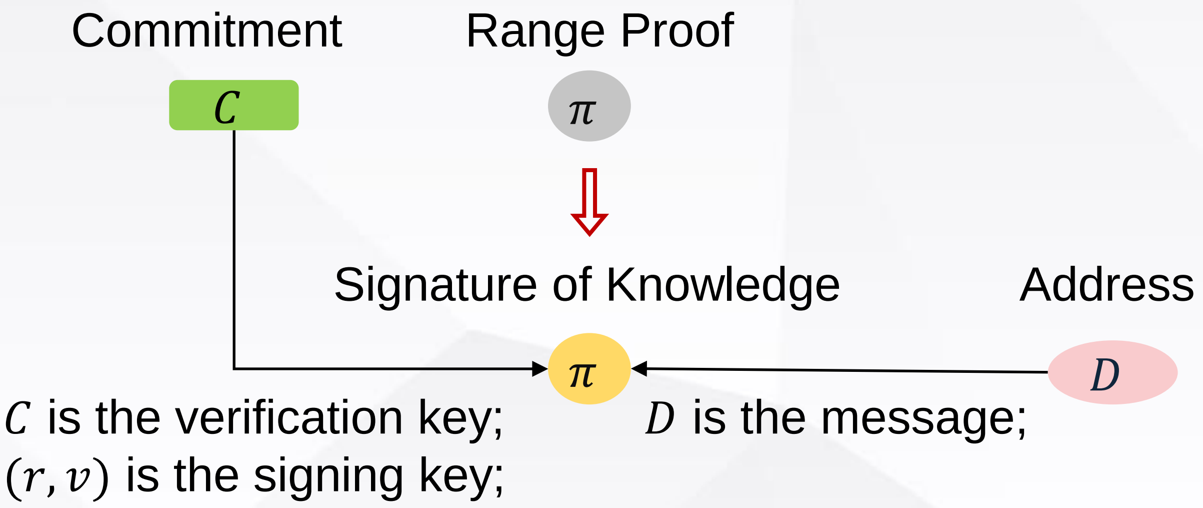


- How to non-interactively transfer the private information of the output coins to the receiver;



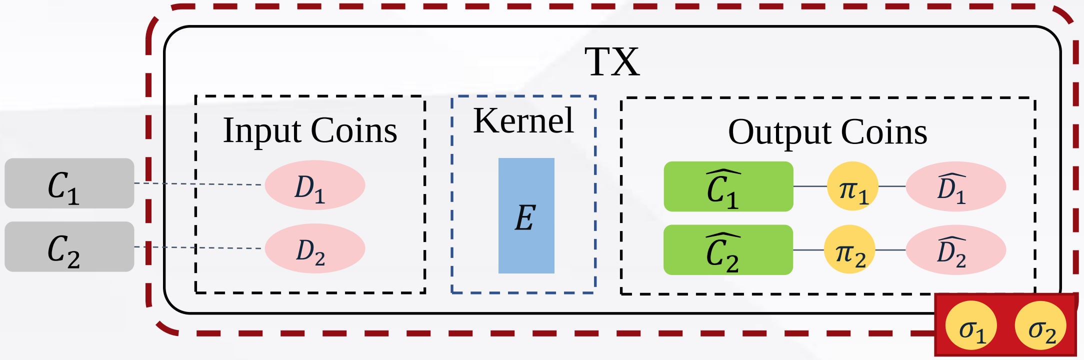
- How to maintain the important feature “cut-through”.

Bind a Commitment and an Address



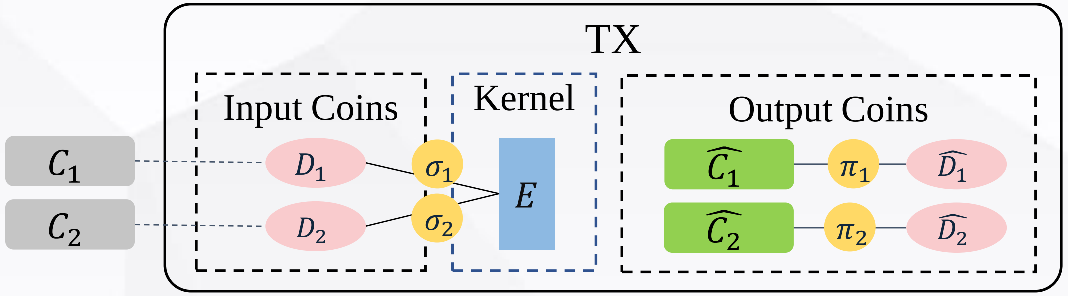
Prove the Ownership of Input Coins

Sign the transaction.



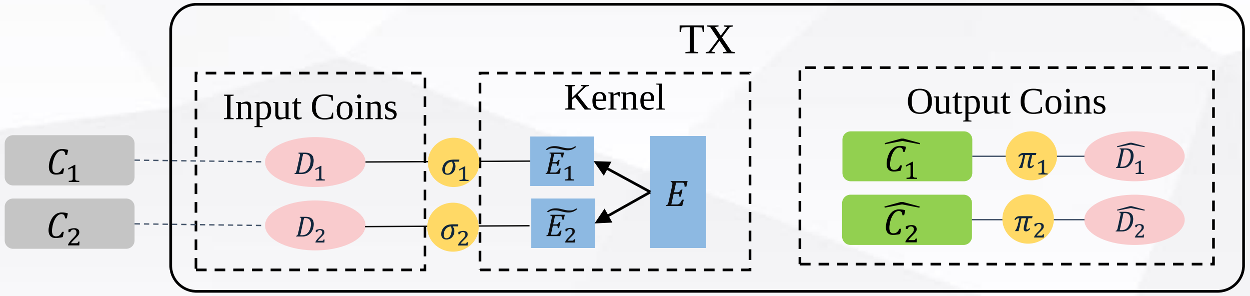
The transaction cannot be aggregated with other transactions.

Sign the excess.



These input coins can be identified as belonging to the same transaction.

Split the excess into multiple parts, then sign each part under an address.



Non-Interactively Transfer the Private Information

Receiver

C ↔ D

C ⇩ Randomness Value

D ⇩ Spending key

New Variant of ElGamal

C ⇩

Ciphertext = $(pk^r, g^{\alpha} h^v)$

sk ⇩ g^r ⇩ $\alpha = H(g^r)$

v

When the message space is small enough

Stealth Address

Permanent Address: (Key, Addr=g^{Key})

Randomly choose r, then $s = H(Addr^r)$

D ⇩ $(g^r, Addr^s)$

Key ⇩ $Addr^r$ ⇩ $s = H(Addr^r)$

Spending key=$Key \cdot s$

Support Cut-Through

$$E_1 = \frac{\widehat{C_1}\widehat{C_2}}{C_1 C_2} \qquad E_2 = \frac{\widehat{C_3}\widehat{C_4}}{C_3 C_4}$$

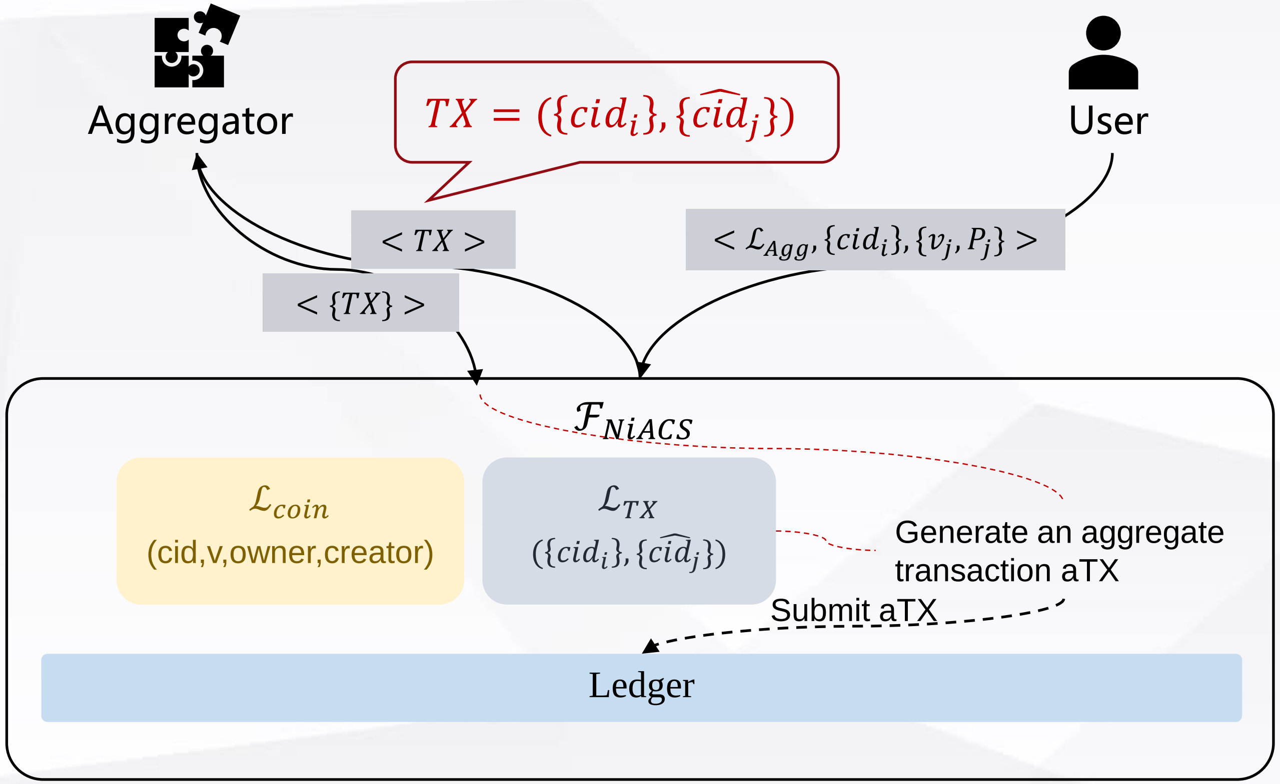
If $\widehat{C_1} = C_3$

$$E_1 \cdot E_2 = \frac{\widehat{C_1}\widehat{C_2}}{C_1 C_2} \cdot \frac{\widehat{C_3}\widehat{C_4}}{C_3 C_4}$$

In our work, the excess is computed in the same way.

Ideal Functionality for NiACS

Can be used to analyze the security in complex execution environments;



Spend the coins with enough value ⟹ Inflation-resistance

Record each coin's owner ⟹ Theft-resistance

Coin id is pseudorandom
- TX ⟹ Transaction Indistinguishability
- aTX ⟹ Unlinkability

Thanks

jiayanxue@sjtu.edu.cn

饮水思源 爱国荣校