Policy-based Chameleon Hash with Black-box Accountability

Yangguang Tian, Nan Li, Yingjiu Li, Pawel Szalachowski, and Jianying Zhou

Singapore University of Technology and Design, Singapore
The University of Newcastle, Australia
University of Oregon, US
Background

• Motivation: correct illicit contents in the “immutable” blockchain, without breaking the link of the hash-chain
  • Ateniese et al. “Redactable blockchain-or-rewriting history in bitcoin and friends”. In EuroS&P 2017

• Significance: data regulation law (e.g., GDPR)
  • The right to erasure (or right to be forgotten)

• Research impact: secure and broad applications
Outline

• State-of-the-art: fine-grained blockchain rewriting
  • Derler et al. “Fine-grained and controlled rewriting in blockchains: Chameleon-hashing gone attribute-based”. In NDSS 2019

• Our proposal
  • fine-grained accountable blockchain rewriting in the permissioned setting, such as Ripple and Hyperledger
Fine-grained Blockchain Rewriting

- Attribute-based access control for blockchain rewriting
  - Each modifier owns a set of attributes (credential)
  - If a modifier’s credential satisfies the access policy associated with a transaction, the modifier can rewrite the transaction
System-level Scenario

Fine-grained Blockchain Rewriting

Block $B_{(i-1)}$  Block $B_i$  Block $B_{(i+1)}$

Append  Rewrite  Judge

Owner  Modifier  Attribute Authority

Note: the modifier’s rewriting privilege is given by an Attribute Authority
Transaction-level Scenario

Block $B_{(i-1)}$

Block $B_i$

Block $B_{(i+1)}$

$A = H(\ h_{(i,1)}\ )$

$B = H(\ T_{(i,2)}\ )$

$C = H(\ h_{(i,3)}\ )$

$D = H(\ T_{(i,4)}\ )$

$A : (h_{(i,1)}, r_{(i,1)}) = \text{Hash}(\ pk, T_{(i,1)}, \text{Policy}_{(i,1)})$

$C : (h_{(i,3)}, r_{(i,3)}) = \text{Hash}(\ pk, T_{(i,3)}, \text{Policy}_{(i,3)})$
Accountable Blockchain Rewriting

• Motivation: thwart transaction modifier from malicious rewriting the blockchain

• Key insights:
  • we introduce traceable attribute-based access control for attribute authority (AA) can resolve any dispute over modified transactions
  • a key generation center (i.e., AA) is needed for attribute-based encryption (ABE)
  • suitable for permissioned blockchains
Accountable Blockchain Rewriting

• Technical Challenge:
  • Multiple modifiers may form an access device (black-box) that includes their rewriting privileges, and distribute or sell it to the public
  • Constant ciphertext size
  • Practical instantiation for blockchain applications

• Solution:
  • Attribute-based encryption with black-box traceability (ABET)
  • ABET is built from DLIN-based ABE and HIBE
    • Each modifier’s decryption key has a unique index $i$
    • Each mutable transaction’s ciphertext has a hidden index $j$ (we call it ciphertext anonymity)
    • The modifier can decrypt the ciphertext if her attribute set satisfies the ciphertext’s policy, and $j <= i$
    • HIBE is used to ensure $j <= i$
Accountable Blockchain Rewriting

Given two transactions (e.g., a transaction and its modified version) and an access black-box, AA does:

1. Find the connection between two transactions
2. Find the accused modifiers from the access black-box (use ABET here)
3. Link a modified transaction to a responsible modifier using AA’s master secret key

Note that the first two steps are public operations, the step 3 is performed by AA only
Performance

• Evaluation
  • ciphertext embedded in transaction is of **constant** size
  • running time of Hash or Adapt is about **one second** for a policy of size 100 (involves 100 attributes)

• Impact to existing blockchains
  • Our solution incurs **no** overhead to Merkle tree generation, and chain validation
  • storage cost
    • 2% - 10% mutable transactions inside a block
    • ABET is the most practical one, compared to existing solutions
Conclusion

• The first policy-based chameleon hash with black-box accountability
  • A modifier is accountable for a modified transaction in a black-box manner

• The practical instantiation
  • The proposed solution can be easily integrated into the existing blockchains
  • The proposed ABET scheme is practical
Thanks for your time

Email: sunshine.tian86@gmail.com