

Privacy-Preserving Transaction Escrow

Stas Jarecki Pat Lincoln Vitaly Shmatikov
UC Irvine SRI International



Partially supported by ONR grants N00014-01-1-0837 and N00014-03-1-0961

Motivation

- Financial transaction records
 - Detection of fraud and money laundering
- Medical research databases
 - Research queries for interactions
- Computer network monitoring
 - Intrusion detection
- Law enforcement
 - Airline passenger databases (cf. JetBlue debacle)



Need to protect personal and organizational privacy while enabling investigators to do their job

Our Transaction Escrow Scheme

- Transactions are escrowed in a way that makes information available only for controlled use
 - Efficient subpoena procedures (unlike public-key escrow)
 - Assured privacy and anonymity for personal data
 - Investigative pattern matching: escrows are opened only when they match some pattern
- No trusted parties
 - Secure against malicious escrow agent
 - Corrupt transaction participants cannot break privacy and anonymity of transactions between honest parties
- Provable security
 - Reduction to Decisional Diffie-Hellman in Random Oracle Model

Existing Approaches

- Trust the insiders
 - Government agency insiders can search internal databases at whim
 - Visa knows all your transactions
 - HMO knows your entire health history
- Trust third parties (key escrow)
 - Escrow decryption key by sharing it
 - Subpoena is inefficient: all escrows must be decrypted to find subpoenaed records
 - Selective de-escrow is impossible: cannot decrypt only escrows that satisfy certain condition



Aldrich Ames

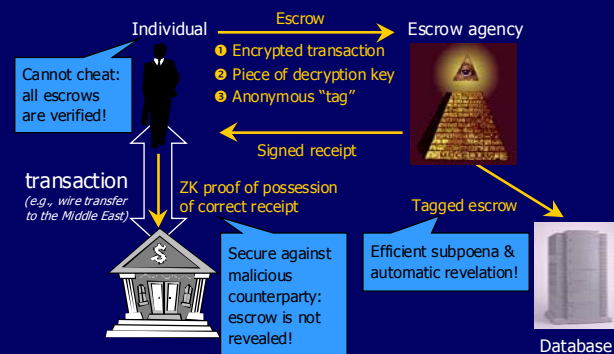


Capabilities of Our Scheme

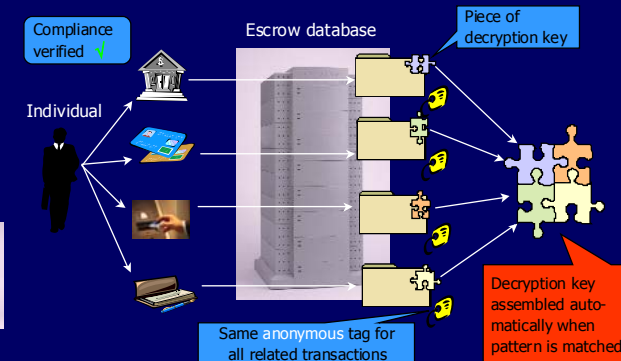
- Automatic selective revelation
 - Reveal all money transfers made by the same person if they total more than \$10,000
 - Reveal records of all passengers who flew to the Middle East more than 5 times in the last year
- Efficient subpoena procedures
 - Easy to find all records of the subpoenaed individual
- Escrows that are not subpoenaed and don't match the revelation condition can't be opened



Verifiable Transaction Escrow



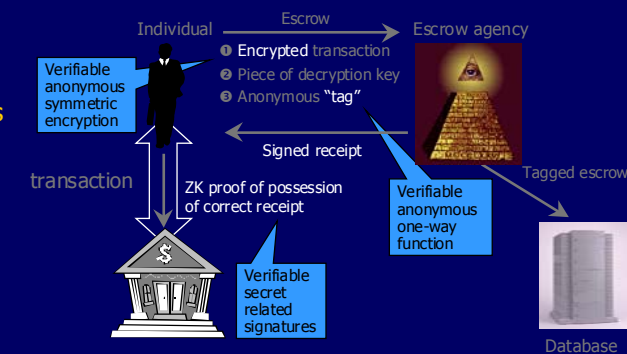
Automatic Selective Revelation



Security Properties

- Subjects of monitoring cannot cheat
 - Correct relationship between plaintext, escrow, tag and key fragments verified in zero knowledge
- Malicious insiders of escrow agency are powerless
 - Cannot gain unauthorized access to the database
 - Cannot frame individuals by inserting bogus records
- Transaction counterparties obtain no information
 - Escrows revealed only to individual and escrow agency
- Anonymous unguessable tags preserve privacy
 - Secure against guessing and cracking attacks
 - Enable efficient subpoena and selective revelation

Cryptographic Toolkit

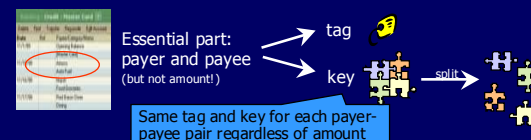


New Cryptographic Primitives

- Verifiable anonymous one-way tagging function
 - Deterministic computation based on user's private key
 - Similar transactions map to the same tag, but recipient cannot invert the tag, nor determine which key was used in computation
 - User proves to verifier in ZK that tag was formed correctly
- Verifiable anonymous symmetric encryption
 - Escrow agent cannot determine which key was used to encrypt
 - User proves to verifier in ZK that escrow was formed correctly
- Related secret signatures (unlinkable receipts)
 - User proves to verifier in ZK that he possesses agent's signature on correctly formed escrow and tag based on a given plaintext
 - Corrupt verifier and malicious escrow agent cannot link their views

Choosing the Key

- User picks a polynomial based on his private key and essential part of transaction plaintext
 - Related transactions have the same essential part
 - Tags and polynomials are based on the same essential part
 - For each tag, user publicly commits to the polynomial
- Polynomial used as key, split into N shares
 - Standard key sharing technique [Feldman '87]



Threshold Revelation

- Each tag uniquely maps to the symmetric key
 - Doesn't compromise privacy since tags are anonymous
 - For each tag, user commits to some key without revealing it
- Escrow encrypted with the key matching its tag
- Each escrow accompanied by 1 share of the key
 - Standard ZK proof that this is the share of the committed key
- Once N escrows with the same tag are collected, decryption key is reconstructed automatically
 - Since escrows with other tags are encrypted with different keys, this does not affect privacy of unrelated transactions

Future Work

- Broader class of patterns for selective revelation
 - Dynamically evolving patterns
 - Patterns not specific to an individual user
- Probabilistic revelation
 - Reveal cumulative transactions with high probability
- Secure audit
- Relaxing PKI assumptions
 - Currently assume a database of unique public keys
 - Investigate schemes without global public keys