Privacy-Preserving Transaction Escrow

**Motivation**
- Financial transaction records
- Detection of fraud and money laundering
- Medical research databases
- Computer network monitoring
- Law enforcement
- Airline passenger databases
- Credit and debit card databases

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

**Existing Approaches**
- Trust the insiders
- Trust third parties (key escrow)
- Need to protect personal and organizational privacy

**Our Transaction Escrow Scheme**
- Transactions are escrowed in a way that makes information available only for controlled use
- No trusted parties
- Secure against malicious escrow agent
- Secure against guessing and cracking attacks
- Secure against malicious insider agent
- Secure against malicious transaction participants
- Secure audit
- Secure against law enforcement

**Security Properties**
- Subjects of monitoring cannot cheat
- Malicious insiders of escrow agency are powerless
- Subjects of monitoring cannot cheat

**Automatic Selective Revelation**
- Efficient subpoena procedures
- Subjects of monitoring cannot cheat

**Capabilities of Our Scheme**
- Automatic selective revelation
- Escrows that are not subpoenaed and don’t match the revelation condition can’t be opened
- Secure audit
- Secure against malicious insider agent
- Secure audit

**Cryptographic Toolkit**
- Secure audit
- Secure audit
- Secure audit