On the Anonymity of Banknotes

Dennis Kügler
Federal Office for Information Security

Privacy Enhancing Technologies 2004, Toronto

2004-05-26

Motivation

- Euro banknotes to embed RFID-chip by 2005?
  - Reading serial numbers without optical contact
  - Makes tracking easier
  - Improves blacklisting
- Our work does **not** depend on such RFID-chips
  - Required “technology” is already available/installed

Attack Scenario

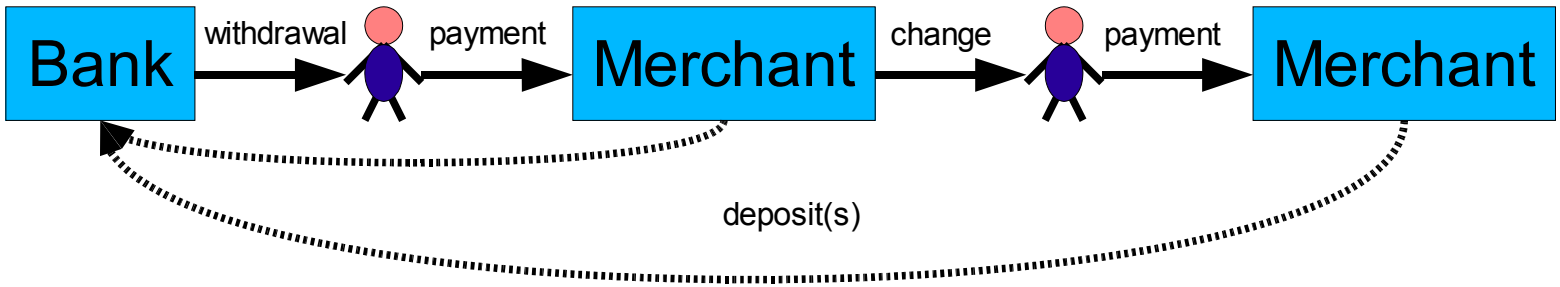
- **Attacker:** Bank as “Local Passive Adversary”
  - Observes withdrawals & deposits
  - Stores serial numbers
    - OCR or RFID
  - Not unrealistic in the real world...
- **Goal:** Deanonymization of some low value payments

Traceability of Banknotes

- Token based payment system
  - Unique serial number
  - Unforgeable: difficult to copy
- Level of Anonymity?
  - Handing on banknotes is unobservable

Intermediary Chains

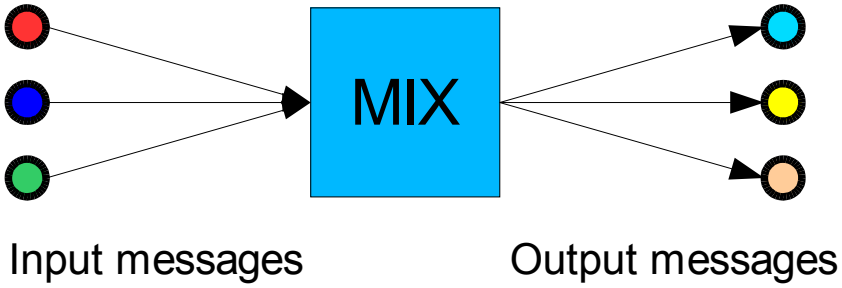
- **Withdrawer Anonymity**
  - Blackmailing
  - Money theft (Bank robbery)
- **Depositor Anonymity**
  - Money laundering



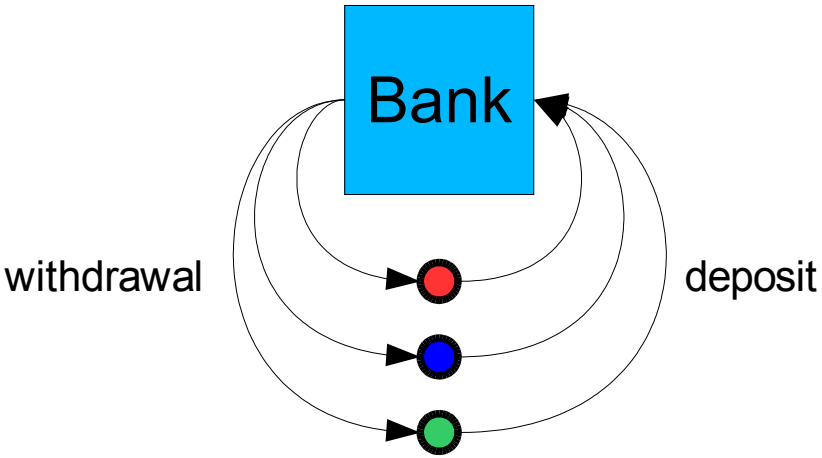
Criminal Investigation

- Restricting Withdrawer Anonymity
  - “Perfect Crime” based on untraceable (electronic) cash
  - Limited traceability (blacklisting) required
  - RFIDs may simplify blacklisting
- Restricting Depositor Anonymity
  - Strong traceability required?

Relation to MIX-Networks



Linkability:
- Intersection Attacks
- Deanonymization over time



Linkablility:
- Sets of Banknotes
- Deanoymization possible?

Linked Banknotes

- Set of linked banknotes
  - Banknotes that a person has withdrawn recently
- Bank sets up a database
  - Store serial numbers at withdrawal
  - Check for sets of linked banknotes at deposit

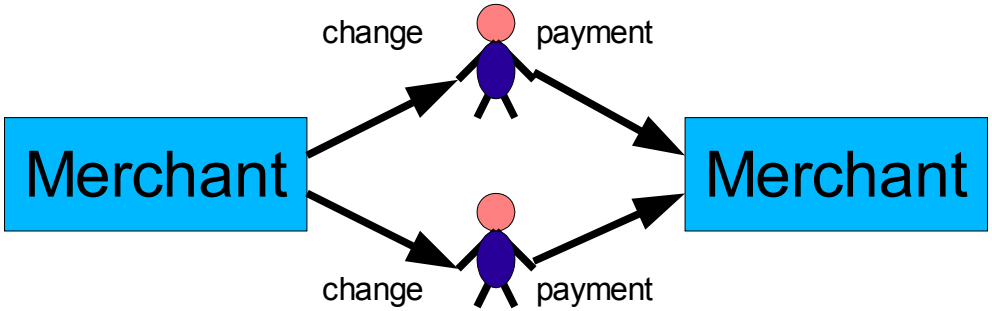
- **Basic Idea:** Use linked sets to find short intermediary chains

Model

- **Merchants**
  - *Cash Desk Model*
  - Last in first out
  - Return small subset as change to customer
  - Keep sets at deposit
- **Customers**
  - *Wallet Model*
  - Random selection
  - Valid for low denominated banknotes

Limitations of the Model

- Customer to Customer transactions (Pocket Money)
- Merchant to Merchant transactions
- Even more complicated cases:



Deanonymization

- The bank receives a set of linked banknotes from Merchant M
  - A: Withdrawer spent those banknotes at M
  - B: Withdrawer spent those banknotes at N, another customer received them as change and spent them at M
- Probability of Event B ???
  - Reject hypothesis (A), if $\mathrm{P}(B) > t$

Wallet Model

X: # linked banknotes used for a payment

Y: # linked banknotes in the customer's wallet

U: total # banknotes used for a payment

V: total # banknotes in the customer's wallet

- Probability to pay with i linked banknotes:

$$P(X=i|Y=j\cap U=n\cap V=t)=\frac{\binom{j}{i}\binom{t-j}{n-i}}{\binom{t}{n}}$$

Cash Desk Model

- **Observation:** Only a small number of (linked) banknotes are returned to the customer as change
  - $\mathrm{E}(Y) = c$ empirically determined
  - Independent of the merchant

- Probability to receive j linked banknotes as change:

$$P(Y = j) = \frac{c^j}{j!} \exp^{-c}$$

Probability of Event B

- s: # of linked banknotes in deposit
- m: max. # of banknotes returned as change
- c: average # of banknotes returned as change

- Probability of event B:

$$P(s \leqslant X \leqslant n \cap Y \leqslant m \mid U = n \cap V = t) = \sum_{i=s}^{n} \sum_{j=i}^{m} \frac{\binom{t-j}{n-i}}{\binom{t}{n}} \frac{c^j}{i!(j-i)!} \exp^{-c}$$

Deanonymization

- **Intuitively:** a deposited linked set of size > 2 is not anonymous
- Example
  - Change: avg. 2, max. 5
  - Deposited set of size 3

total wallet	total payment	P(B)
6	5	0.22
5	5	0.48
5	4	0.27

$$P(V=t|Y=j\cap U=n)=?$$

How to Use Banknotes Correctly

- Avoid using sets of linked banknotes for payments
  - Withdrawal:
    - Single high denominated banknote
    - Use for one (non-anonymous) low value payment
    - Change is anonymous
  - Payments with non-anonymous banknotes:
    - Use as few banknotes as possible
    - Avoid recurring payments at the same (or a related) merchant

Conclusion

- On the negative side:
  - Banknotes are more traceable than one would expect
  - Deanonymization can be circumvented
- On the positive side:
  - Powerful tool for criminal investigation?
  - Difficult to circumvent deanonymization