1 Digital Cash

1.1 Online E-Cash

Vendor and bank are allowed to communicate during a transaction.

Setting:

- User maintains an account with a bank
- The bank decides on a certain denomination that will be used for e-coins
- Bank publishes $e$, a prime number that corresponds to the $1$ e-coin and an RSA modulus $n$ as well as a string $M$ that should be included in all e-coins and a hash function $H$. This public information is known to all vendors.

![Figure 1: Online E-Cash Setup and Protocols](image)

1.2 Withdrawal Protocol (1)

User wants to withdraw an e-coin from his account.

1. User authenticates himself to bank
2. User selects $r$, a random number
3. selects $b \leftarrow_R Z_n$

4. form $v \leftarrow b^e \cdot H(M||r) \mod n$. User submits $v$ to the bank.

5. Bank withdraws $1$ from the user’s account and puts it into the POOL.

6. Bank replies with $\sigma \leftarrow v^{1/e} \mod n$

7. User computes $\text{coin} = \frac{1}{b} \cdot \sigma \mod n$ and outputs $<r,\text{coin}>$ as the $1$ e-coin withdrawn ($\text{coin} = (H(M||r))^{1/e} \mod n$)

In step 4, $b$ is used for blinding. By dividing by $b$ in step 7 the blinding is removed.

1.3 Payment Protocol (2)

User submits $<r,\text{coin}>$ to the vendor. Before the vendor delivers the service:

- vendor checks: $(\text{coin})^e \equiv H(M||r) \mod n$
- if yes, then initiates a check with the bank submitting $<r,\text{coin}>$ through an authenticated channel

1.4 Deposit Protocol (3)

Bank receives $<r,\text{coin}>$.

- verifies validity
- checks whether $<r,\text{coin}>$ exists in the deposited e-coin database
- if no, then return ‘OK’ and moves $1$ from the POOL to the vendor’s account

By this setting it is impossible to link a payment to its corresponding withdrawal!

2 Offline Cash

This case is harder, because there is nothing that can prevent the user from double-spending (at least in the above scheme).

More sophisticated e-cash protocols allow the following:

- every e-coin contains an embedding of the user’s identity
- payment is a challenge-response transaction where the user uses the e-coin
- executing one payment protocol does not reveal anything about the identity of the user
- executing TWO payments reveal the identity

In the withdrawal protocol the bank has to make sure that blinded coins contain an embedding of the user’s identity.