Admin: PS #5 due Wed.

Next Wed, 5/6 will be a guest lecture by Paul Ducklin of Sophos.

Outline: "Electronic Cash"
-Atoms vs Bits
-checks
-properties/requirements
-credit cards
-chaum's anonymous coins (blind sigs)
-schnorr zk proof of identity
-Bond's electronic coins
"Electronic Money"

- What properties should it have?
- " " can it have?

Atoms vs. Bits

What does "possessing value" (money) mean?
Pretty clear if we are talking about gold atoms...
Not so clear if we are talking about bits, since
bits can be copied
(well, maybe not qubits, but that's another story...)
double-spending becomes possible.

- bit-based cash systems are typically account-based
  account keeper (bank) keeps track of who has how much.

Bank is TTP.
Electronic Checks

- Have account with bank. Bank has PK_B, SK_B
- Have PK_u, SK_u, cert

\[
\text{Check} = \begin{cases} \\
\text{Certificate by bank of user's PK_u} & \\
\text{Sign} \left( \text{"Pay Bob $100, ser #, date"} \right) \\
\text{SK_u} & \\
\end{cases}
\]

- Bank only allows check to be deposited once (ser #)
- Usual problem of overdrawn account
- Cashier's check - bank counter-signs
- Not anonymous - bank knows where you spent your money
  - Merchant knows who purchased & bank (of course)
  - Customer knows merchant (of course)
- Can we make this more like cash?
Properties: (What do we want?)

- Non-forgable (can’t “create money”)
- not double-spendable
- on-line vs off-line verification of validity
  (does merchant need to run to bank to verify?)

![Diagram]

- Persistence/reliability: disk crash?
  (if you backup disk, does your # reappear
  when you restore?)
- exclusive ownership?
- transferability (can make payments): can A pay B then B pay C?
  (transitivity?)
- variable amount/coin sizes
- divisibility/combinability
- efficiency (esp. for small amounts)
- scalability (does bank need large database or computational resources)
  - what about multiple banks?
Credit Cards

- Use weak form of credential (knowledge of CC #) (sent via SSL) and online verification
- Bank absolves risk of fraud... (changes merchant e.g. 5%)

Chaum's Anonymous Cash

Bank uses RSA: \( PK = (n, e) \) \( SK = d \)

Blind withdrawal:

- User
- Random \( r \)
- \( r^e \)
- \( m \cdot r \)
- \( m \cdot r = (m \cdot e)^d \)

- \( nd = sign(SK, m) \) bank sign on serial # \( m \)

- Could have special format, random seed #

- Need to fix value of coin (per bank PK) since bank doesn't see \( m \), could have different PKs for different coins values.

- Double-spending is a problem!
Goal: coin withdrawal 1) anonymous
spending coin is anonymous
but if user double-spends, his identity is revealed!

Idea:
- bank gives blind sig on coin
- user knows secret about coin
- payment protocol involves revealing some info about secret
  but pays twice does (like threshold)

Digression: Zero knowledge proof of identity (Schnorr)

\[ p = \text{large prime} \]
\[ q \text{ divides } p-1, q \text{ prime} \]
\[ g \text{ generator of order } q, \quad G_q = \langle g \rangle \text{ subgroup of order } q \]
Alize knows secret \( x \in \mathbb{Z}_q = \{0, 1, \ldots, q-1\} \)
\[ y = g^x \mod p \] is Alize's PK

How can Alize (safely) prove she knows \( x \) to Bob?
(without revealing anything to Bob)
(zero-knowledge revealed except that "Alice knows \( x \)"
)
\( A \xrightarrow{k \in \mathbb{Z}_q} a = g^k \mod p \xrightarrow{c} r = cx+k \mod q \)

If Alice knows \( k \), she can convince Bob to accept.

**Thm**: Completeness. If Alice knows \( k \), she can convince Bob to accept.

**Pf**:
1. \( g^c g^r = g^{c+m} \)
2. \( g^{cx+k} = g^r \)

\( r = cx+k \mod q \) checks.

---

**Thm**: Zero-knowledge (for honest verifier).

**Pf**:
Bob learns transcript \((a, c, r)\). Nothing more.

Transcript is a random variable (random \( k \), random \( c \)).

Bob gets sample of this R.V.

Bob can generate such samples on his own! with correct distribution.

- \( c \in \mathbb{Z}_q \) (assuming)
- \( r \in \mathbb{Z}_q \) (note \( r \) uniform in \( \mathbb{Z}_q \) since \( k \) is)
- \( a = g^c / y^c \)

\((a, c, r)\) has exactly same distribution as it has in protocol.

\( \therefore \) Bob learns nothing (except that Alice can play game).
[Validity/Soundness]

Thm: Alice can play game  \implies Alice knows x

(\equiv Alice doesn't know x  \implies Alice can't play game)

PF: Alice can play game \equiv for any \lambda \in \text{almstalc}

she can produce suitable r

Suppose we fix a = g^k

Suppose Alice can succeed for c and for c'

Then \[ r = cx + k \]
\[ r' = c'x + k \]

\[ r - r' = (c - c') \cdot x \]

\[ x = \frac{r - r'}{c - c'} \pmod{g} \]

\[ c - c' \neq 0 \pmod{g} \]
\[ g \text{ prime} \]
\[ c - c' \exists \text{ exists} \]

\[ \therefore \text{if she can play game for many c's, she} \]

"knows" x. (It can be derived easily from two transcripts.)

\[ \text{Proof embodies key idea: participating in a protocol twice} \]
\[ \text{can reveal secret} \]

Note: Schnorr ID protocol can be turned into

Signature scheme by taking e = \text{hash}(a, m)

\[ \text{r message to be signed} \]