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
- ☐ Brand'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

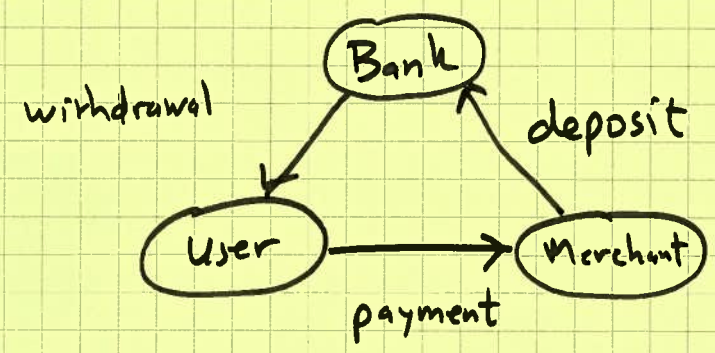
- Have account with bank. Bank has PK_B, SK_B
- Have PK_u & SK_u, cert

Check: [certificate by bank of user's PK_u
sign ("Pay Bob \$100, ser #, date") $\uparrow SK_u$]

- 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?

<u>Properties:</u> (what do we want?)

- Non-forgeable (can't "create money")
- not <u>double-spendable</u>
- on-line <u>vs</u> off-line verification of validity
  (does merchant need to run to bank to verify?)



- 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 amounts / coin sizes
- divisibility / combinability
- efficiency (esp. for small amounts)
- scalabality (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 on-line verification
- bank absorbs risk of fraud... (charges merchant e.g. 5%)

Chaum's Anonymous Cash

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

Blind withdrawal:

user random r $\xrightarrow{m \cdot r^e}$

$\xleftarrow{m^d r}$ $m^d r = (m \cdot r^e)^d$

$\Downarrow$

$m^d = \text{sign}(SK, m)$ bank sig on serial # m

$\boxed{\text{coin} = (m, m^d)}$

could have special format, random serial #

- Need to fix value of coin (per bank PK) since bank doesn't see m. Could have different PK's for different coins values.
- Double-spending is a problem!

Goal: coin withdrawal is 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
- paying once doesn't reveal enough to identify user, but paying twice does (like threshold)

Digression: Zero knowledge proof of identity (Schnorr)

p = large prime

q divides $p-1$, q prime

g generator of order q $\quad G_q = \langle g \rangle$ subgroup of order q generated by g

Alice knows secret $x \in Z_q = \{0, 1, \ldots, q-1\}$

$y = g^x \pmod p$ is Alice's PK

How can Alice (safely) prove she knows x to Bob?

(without revealing anything to Bob)

(zero-knowledge revealed; except that "Alice knows x")

A		B
$k \in_R Z_q$ $a = g^k \pmod p$	$\xrightarrow{\quad a \quad}$	
	$\xleftarrow{\quad c \quad}$	$c \in_R Z_q$
$r = cx + k \pmod q$		
	$\xrightarrow{\quad r \quad}$	Check $\boxed{y^c \cdot a \stackrel{?}{=} g^r \pmod p}$

Thm: [Completeness] If Alice knows x, she can persuade Bob to accept.

Pf:
$$\begin{cases} g^{cx} g^k \stackrel{?}{=} g^r \\ g^{cx+k} = g^r \quad \checkmark \end{cases}$$

Thm: Bob learns nothing about x (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 <u>on his own</u>! with correct distribution!

$c \in_R Z_q$ (assuming

$r \in_R Z_q$ (note r uniform in Z_q since k is)

$a = g^r / y^c$

(a, c, r) has <u>exactly</u> same distribution has it has in protocol.

$\therefore$ Bob learns nothing (except that Alice can play game). $\blacksquare$

[Validity/Soundness]

Thm: Alice can play game
$\Rightarrow$ Alice knows x

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

Pf: Alice can play game $\equiv$ for any a & almost all c
she can produce suitable r

Suppose we fix $a = g^k$

Suppose Alice can succeed for c and for c'

Then
$$r = cx + k$$
$$r' = c'x + k$$
$$r - r' = (c - c') \cdot x$$
$$x = \frac{r - r'}{c - c'} \pmod q$$

$c - c' \neq 0 \bmod q$
q prime
$\therefore (c-c')^{-1}$ exists.

Protocol is a "proof of knowledge"
ZKPOK

$\therefore$ if she can play game for many c's, she "knows" x. (It can be derived easily from two transcripts. ∎

Proof embodies key idea: participating in a protocol twice can reveal secret

Note: Schnorr ID protocol can be turned into signature scheme by taking $c = \text{hash}(a, m)$
↑ message to be signed.