6.857 Rivest

L22.1 4/29/09

Admin: Guest lecturer (Paul Ducklin / Sophos) on Wed 5/6

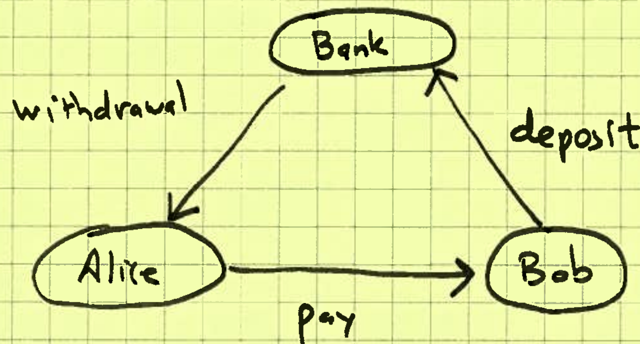
Project presentations Mon 5/11 & Wed 5/13. Approx 16 min each.

Outline:

- ☐ Brands' ecash scheme
- ☐ Electronic voting (Scantegrity) (slideshow)

Brands e-cash scheme

- spending coin once preserves anonymity
- spending coin twice reveals identity of double spender



Withdrawal: blind signature scheme on coin (Bank doesn't see coin)
but Bank knows Alice's ID embedded in coin

Payment: Interactive challenge/response protocol
If Alice does this protocol twice for same coin, enough information is revealed about her identity to identify her.

Deposit: Bank needs to check if same coin is being deposited twice & if so, identify double-spender.

6.857 Rivest

L22.3 4/29/09

DLP: Given • prime $p = 2q+1$ (q prime)

• generator g of G_q = squares in Z_p^* $|G_q| = q$

• value y in G_q

to find $x \in Z_q$ s.t. $g^x = y \pmod p$

DLP Assumption: DLP is hard.

Rep: Given prime $p = 2q+1$

generators g_1, g_2 of G_q

value $y \in G_q$

to find x_1, x_2 s.t. $g_1^{x_1} g_2^{x_2} = y \pmod p$

$\boxed{\text{multiple generators}}$

Rep Assumption: Rep is hard.

Thm: If discrete log of g_2, base g_1 is unknown (DLP) then it is hard to come up with two reps for y

Pf: $y = g_1^{x_1} g_2^{x_2} = g_1^{x_1'} g_2^{x_2'}$

$\Rightarrow g_2 = g_1^{(x_1 - x_1')/(x_2' - x_2)} \pmod p$

$\Rightarrow$ discrete log of g_2 mod p base g_1 = $(x_1 - x_1')/(x_2' - x_2) \bmod q$

∎

CVP Commitment Scheme (Chaum - van Heijst - Pfitzmann)

- Let $p = 2q+1$ be prime, q prime, g_1, g_2 generators of G_q
- Let $m \in Z_q$ (message to commit to)

Commit(m): $r \in_R Z_q$

$c = g_1^m g_2^r \pmod{p}$ commitment

Reveal(c): give m & r

Thm: Unconditionally private (c is random elt of G_q).

Thm: Computationally binding
(assuming discrete log of g_2 base g_1 is unknown)

Note: malleable.

Proof of knowledge (cf. Schnorr ID scheme)

- Let $p = 2q+1$, q prime, g_1, g_2 generators of G_q
  $\log_{g_1}(g_2)$ unknown

- Suppose Alice knows x_1, x_2 s.t. $y = g_1^{x_1} g_2^{x_2} \pmod p$

She can prove she knows x_1, x_2

Alice — **Bob**

$k_1 \in_R Z_q$, $k_2 \in_R Z_q$ $\xrightarrow{a = g_1^{k_1} g_2^{k_2}}$

$\xleftarrow{c}$ $c \in_R Z_q$

$r_1 = cx_1 + k_1$, $r_2 = cx_2 + k_2$ $\xrightarrow{r_1, r_2}$ $y^c a \stackrel{?}{=} g_1^{r_1} g_2^{r_2} \pmod p$

If Alice can answer twice with <u>same</u> a but different c':

$\xrightarrow{a}$

$\xleftarrow{c'}$

$r_1' = c'x_1 + k_1$, $r_2' = c'x_2 + k_2$ $\xrightarrow{r_1', r_2'}$ $y^{c'} a = g_1^{r_1'} g_2^{r_2'}$

$$\therefore \quad r_1 - r_1' = x_1(c - c')$$
$$r_2 - r_2' = x_2(c - c')$$

$$\therefore \quad \frac{r_1 - r_1'}{r_2 - r_2'} = \frac{x_1}{x_2}$$ } want this to reveal Alice's ID

Brands' scheme: (CRYPTO '93 "Untraceable Off-line Cash in Wallets with Observers")

$p = 2q + 1$ $\quad p, q$ prime public

g_1, g_2, g $\quad$ public generators of G_q (pairwise DL's unknown)

Bank SK $= x \in Z_q$

Let $g^x = h$

Bank PK $= g_1^x, g_2^x, g^x$

User secret $= u_1$ $\quad (\in_R Z_q$ privately$)$

User ID $= I = g_1^{u_1}$ $\quad$ (acct # at Bank, linked to real name)

$$Z = (I g_2)^x = g_1^{u_1 x} g_2^x$$

[needed in withdrawal
computed by Bank or user.]

<u>Coin</u> has form

$$(A,\ B,\ \mathrm{sign}(A,B))$$

<u>where</u> $A = (I g_2)^s = g_1^{u_1 s} g_2^s$

$B = g_1^{x_1} g_2^{x_2}$

$s \in Z_q^*$ picked privately by user at withdrawal

$\mathrm{sign}(A,B)$ = signature by Bank (blind, created at withdrawal)

<u>Payment:</u>

$$\xrightarrow{(A,B,\mathrm{sign}(A,B))}$$

$d = \mathrm{hash}(A, B, I_B, \text{date})$

$$\xleftarrow{d}$$

$r_1 = d(u_1 s) + x_1$
$r_2 = ds + x_2$

$$\xrightarrow{r_1,\ r_2}$$

verify $\mathrm{sign}(A,B)$
$g_1^{r_1} g_2^{r_2} \stackrel{?}{=} A^d B$

<u>If Alice double-spends:</u> $r_1' = d'(u_1 s) + x_1$
$r_2' = d'(s) + x_2$

$$\Longrightarrow \frac{r_1 - r_1'}{r_2 - r_2'} = u_1 \Rightarrow g_1^{u_1} = I \Rightarrow \text{user name}$$

!

caught

Withdrawal:

$$\mathrm{Sign}(A,B) \stackrel{\Delta}{=} (z,a,b,r) \in G_q \times G_q \times G_q \times Z_q \text{ s.t.}$$

$$\left.\begin{array}{l} g^r = h^{\mathcal{H}(A,B,z,a,b)} a = h^c a \\ A^r = z^{\mathcal{H}(A,B,z,a,b)} b = z^c b \end{array}\right\} \;\&\; c = \mathcal{H}(A,B,z,a,b)$$

$\mathcal{U}$ $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\mathcal{B}$

$$\left\{\begin{array}{l} w \in_R Z_q \\ a = g^w \\ b = (I g_2)^w \end{array}\right.$$

$\xleftarrow{\quad a,\, b \quad}$

$s \in Z_q^*$

$A \leftarrow (I g_2)^s$, $z' = z^s$

$B \leftarrow g_1^{x_1} g_2^{x_2}$ (x_1, x_2 random)

$a' = a^u g^v$ (u, v random $\in Z_q$)

$b' = b^{su} A^v$

$c' = \mathcal{H}(A, B, z', a', b')$

$c = c'/u \pmod q$

$\xrightarrow{\quad c \quad}$

$r = cx + w$

$\xleftarrow{\quad r \quad}$

$g^r = h^c a$

$(I g_2)^r = z^c b$

$r' \leftarrow ru + v \bmod q$

$\Rightarrow$ (A,B) coin

(z', a', b', r') is $\mathrm{Sign}(A,B)$