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.
**DLP:** Given prime \( p = 2q + 1 \) (\( q \) prime),
egenerator \( g \) of \( G_q \) = squares in \( \mathbb{Z}_p^* \)
\( \text{ord} \) value \( y \) in \( G_q \)
to find \( x \in \mathbb{Z}_q \) s.t. \( g^x = y \) (mod \( p \))

**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. \( g_1^{x_1} g_2^{x_2} = y \) (mod \( p \))

**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:** \[
y = g_1^{x_1} g_2^{x_2} = g_1^{x'_1} g_2^{x'_2}
\]
\( \Rightarrow \)
\( g_2 = g_1^{(x_1 - x'_1) / (x'_2 - x_2)} \) (mod \( p \))

\( \Rightarrow \) discrete log of \( g_2 \) mod \( p \) base \( g_1 = \frac{(x_1 - x'_1) / (x'_2 - x_2)}{x_1 - x'_1} \) mod \( p \)
CUP Commitment Scheme (Chaum-van Heijst-Pointche)

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

Commit $(m)$: $r \in \mathbb{Z}_q$

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

Reveal $(C)$: give $m$ & $r$

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

Thm: Computationally binding
(assuming discrete log of $g_2$ box $g$, is unknown)

Note: malleable.
Proof of Knowledge (cf. Schnorr ID scheme)

- Let $p = 2g + 1$, $g$ prime, $g_1, g_2$ generators of $G_2^{*}$
  
  \[ \log_{g_1}(g_2) \] 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 $x_1, x_2$

\begin{align*}
  & \text{Alice} \\
  k_1 \in \mathbb{Z}_p & k_1 \cdot g_2 \\
  k_2 \in \mathbb{Z}_p & k_2 \cdot g_2 \\
  a = g_1^{k_1}g_2^{k_2} & c = \in \mathbb{Z}_p \\
  r_1 = c \cdot x_1 + k_1 & r_2 = c \cdot x_2 + k_2
\end{align*}

\begin{align*}
  c & \rightarrow c' \\
  r_1, r_2 & \rightarrow y^{c} = g_1^{r_1}g_2^{r_2} \pmod{p}
\end{align*}

If Alice can answer these with some $a$ but different $c'$:

\begin{align*}
  & \text{Alice} \\
  r_1' = c' \cdot x_1 + k_1 & r_2' = c' \cdot x_2 + k_2 \\
  c' & \rightarrow c' \\
  r_1', r_2' & \rightarrow y^{c'} = g_1^{r_1'}g_2^{r_2'}
\end{align*}

\[ \begin{align*}
  r_1 - r_1' &= x_1 (c - c') \\
  r_2 - r_2' &= x_2 (c - c')
\end{align*} \]

\[ \therefore \frac{r_1 - r_1'}{r_2 - r_2'} = \frac{x_1}{x_2} \]

\[ \text{we let this to reveal Alice's ID} \]
Brands' scheme: \((\text{CRYPTO '93})\)

"Untraceable Off-line Cash in Wallets with Observers"

\[ p = 2g + 1 \quad p, g \text{ prime public} \]

\[ g_1, g_2, g \quad \text{public generator of } G^* \text{ (prime in DL's unknown)} \]

\[
\begin{align*}
\text{Bank SK} & = x \in \mathbb{Z}_p \\
\text{Let } g^x & = h \\
\text{Bank PK} & = g_1^x, g_2^x, g^x
\end{align*}
\]

\[
\begin{align*}
\text{User secret} & = u_1 \quad (x \in \mathbb{Z}_p \text{ private}) \\
\text{User ID} & = I = g_1^{u_1} \quad (acct \# \text{ at Bank, linked to real name}) \\
Z & = (Ig_2)^x = g_1^{u_1x} g_2^x \quad \text{[needed in withdrawal]}
\end{align*}
\]

\(6.857 \text{  River}^\text{t} \)

\(122.6 \quad 4/29/09\)
Coin has form:

\[(A, B, \text{sign}(A, B))\]

where

\[A = (I g_a)^s = g_1^u g_2^s\]
\[B = g_1^{x_1} g_2^{x_2}\]
\[s \in \mathbb{Z}_q^* \text{ picked privately by user at withdrawal}\]
\[\text{sign}(A, B) = \text{signature by Bob (blind, created at withdrawal)}\]

**Payment:**

\[
\text{d = hash}(A, B, I_B, \text{dhek})
\]
\[r_1 = d(u, s) + x_1\]
\[r_2 = ds + x_2\]

\[g_1^r g_2^r = A^d B\]

If Alice double-spends:

\[r_1' = d'(u, s) + x_1\]
\[r_2' = d'(s) + x_2\]

\[
\frac{r_1 - r_1'}{r_2 - r_2'} = u, \quad \Rightarrow g_1^{u'} = I \Rightarrow \text{user name caught}
\]
Withdrawal:

\[ \text{Sign}(A, B) \triangleq (z, q, b, r) \in G_9 \times G_9 \times G_9 \times Z_q \text{ s.t.} \]

\[ g^r = h^{\mathcal{H}(A, B, z, q, b)} \]

\[ A^r = z^{\mathcal{H}(A, B, z, q, b)} b = z^c b \]

\[ U \]

\[ s \in \mathbb{Z}_q^* \]

\[ A = (I_{g_2})^s, \quad z' = z^s \]

\[ B = g_1^{x_1} g_2^{x_2} \quad (x_1, x_2 \text{ random}) \]

\[ a' = a g^{u v} \quad (u, v \text{ random } \mathbb{Z}_q) \]

\[ b' = b^{s u} a'^v \]

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

\[ c = c' / u \pmod{q} \]

\[ g^r = h^c a \]

\[ (I_{g_2})^r = z^c b \]

\[ r' \leftarrow ru + v \pmod{q} \]

\[ \Rightarrow (A, B) \text{ coin} \]

\[ (z', a', b', r') \text{ is } \text{Sign}(A, B) \]