A FEW E-COMMERCE APPLICATIONS

This is based on Chapter 9 of Trappe and Washington
E-COMMERCE: SET

SET = Secure Electronic Transaction
Consider a credit card transaction over the net.
We want:

Authentication
No impersonations. No forgeries.

Integrity
Documents cannot be altered after the fact.

Privacy
The details of the transaction should be private.

Security
Credit card numbers & the like must be protected.

SET - a collection of crypto protocols for credit card transactions (≈ 1997)
SET EXAMPLE

Characters

Cardholder
Merchant
Bank

These guys don’t trust one another

H - a public hash function
PKC - say RSA

Encryption/Decryption Functions

\[ E_C \quad E_M \quad E_B \quad \text{Public} \quad \text{Private} \quad D_C \quad D_M \quad D_B \]

Cardholder

GSO - goods and services order (cardholder’s name, merchant’s name, prices, etc.)
PI - payment instructions (merchant’s name, card number, total price, etc.)
SET EXAMPLE CONTINUED

Q: Who knows what from the transactions?

Cardholder

Computes

\[ GSO_{md} = H(E_M(GSO)) \]
\[ PI_{md} = H(E_B(PI)) \]
\[ PO_{md} = H(PI_{md}||GSO_{md}) \]
\[ DS = D_C(PO_{md}) \]

Sends \( E_M(GSO), DS, PI_{md}, E_B(PI) \) to Merchant

Merchant (on receiving \( E_M(GSO), DS, PI_{md}, E_B(PI) \))

Computes

\[ gso_{md} = H(E_M(GSO)) \]
\[ gso = D_M(E_M(GSO)) \]
\[ b = H(PI_{md}||gso_{md}) \]
\[ c = E_C(DS) \]

Checks

\[ gso_{md} \overset{?}{=} H(E_M(gso)) \] & \[ b \overset{?}{=} c \]

Sends \( GSO_{md}, E_B(PI), DS \) to the Bank
Bank (on receiving $GSO_{md}, E_B(PI), DS$)

Computes

$$p_{imd} = H(E_B(PI)) \quad c = E_C(DS)$$
$$p_i = D_B(E_B(PI)) \quad b = H(p_{imd}|GSO_{md})$$

Checks

$b ?= c$

Sends

$EM$(a payment auth. + signature) to Merchant.

Merchant

Sends

$EC$(receipt + signature) to Cardholder.
Okamoto & Ohta’s Criteria

▶ Cash can be sent securely through computer networks
▶ Cash cannot be copied or reused.
▶ The spender can remain anonymous — neither the merchant nor the bank can id the spender
▶ The transactions can be done off-line — the bank does not have to be involved.
▶ Cash can be transferred to others.
▶ Cash can be divided into smaller amounts.
BRANDS’S DIGITAL CASH SCHEME

Characters

▶ Bank
▶ Spender
▶ Merchant
▶ Central Authority
▶ Eve L. Dewar

Central Authority Chooses:

▶ A prime \( p \ni q = (p - 1)/2 \) is also prime.
▶ \( \alpha \) – a primitive element of \( \mathbb{Z}_p^* \).
▶ \( g = \alpha^2 \pmod{p} \).
  \hspace{1cm} (So: \( g^{e_1} \equiv g^{e_2} \pmod{p} \iff e_1 \equiv e_2 \pmod{q} \))
▶ \( e_1, e_2 \in \mathbb{Z}^*_{p-1} \) – secret exponents.
▶ \( g_1 = g^{e_1} \) and \( g_2 = g^{e_2} \).
▶ \( H: \mathbb{Z}_5 \rightarrow \mathbb{Z}_q \) and \( H_0: \mathbb{Z}_4 \rightarrow \mathbb{Z}_q \). Hash functions

Public: \( p, q, g, g_1, g_2, H, \) and \( H_0 \).

Private: \( e_1 \) and \( e_2 \)
BRANDS’S DIGITAL CASH: THE SETUP CONTINUED

The Bank
Choses $x \overset{\text{ran}}{\in} \mathbb{Z}_q$ – The bank’s private ID
Computes $h = g^x, h_1 = g_1^x, \text{and } h_2 = g_2^x.$ (All $\pmod{p}$)
$h, h_1, h_2$ – the bank’s public ID

The Spender
Choses $u \overset{\text{ran}}{\in} \mathbb{Z}_q$ – The spender’s private ID
Computes $I = g_1^u \pmod{p} \&$ sends $I$ to the bank.

The Bank
Saves $I +$ info on the spender
Computes $z' = (Ig_2)^x \pmod{p}$ and sends $z'$ to the spender.

The Merchant
Chooses an ID number $M$ and sends it to the bank.
CREATING A COIN

Coin \equiv (A, B, z, a, b, r) \in \mathbb{Z}^6

In number theory we trust.

Spender

Asks bank for a coin and sends ID \( I \).

Bank

Chooses: \( w \) \in \mathbb{Z}_q \) and computes:

\[
g_w \equiv g^w \\
\beta \equiv (Ig_2)^w \pmod{p}
\]

Sends \( g_w \) and \( \beta \) to the spender.

Spender

Chooses \((s, x_1, x_2, \alpha_1, \alpha_2)\) \in \mathbb{Z}^5

Computes:

\[
A \equiv (Ig_2)^s \\
B \equiv g_1^{x_1} g_2^{x_2} \\
z \equiv (z')^s \\
a \equiv g_1^{\alpha_1} g_2^{\alpha_2} \\
b \equiv \beta^{s\alpha_1} A^{\alpha_2}
\]

\(A=1\) not allowed.
CREATING A COIN, CONTINUED

Spender – continued

Computes \( c \equiv \alpha_1^{-1} \cdot H(A, B, z, a, b) \pmod{q} \).
Sends \( c \) to the bank.

Bank

Computes \( c_1 \equiv (c \cdot x + w) \pmod{q} \).
Sends \( c_1 \) to the spender.

Spender

Computes \( r \equiv (\alpha_1 c_1 + \alpha_2) \pmod{q} \).

The coin \((A, B, z, a, b, r)\) is complete.

The amount of the coin is removed from the spender’s bank account.
SPENDING THE COIN

Spender
Gives the coin \((A, B, z, a, b, r)\) to the merchant.

Merchant
\[ g^r \equiv ah^H(A,B,z,a,b) \]
Checks:
\[ A^r \equiv z^H(A,B,z,a,b)b \quad (\text{mod } q) \]
Computes \(d = H_0(A, B, M, t)\), where \(t\) = a time stamp.
Sends \(d\) to spender.

Spender
Computes
\[ r_1 \equiv d \cdot u \cdot s + x_1 \]
\[ r_2 \equiv d \cdot s + x_2 \]
(mod q)
Sends \(r_1\) and \(r_2\) to merchant.

Merchant
Checks:
\[ g_1^{r_1} \cdot g_2^{r_2} \equiv A^d \cdot B \quad (\text{mod } p) \]
Accepts the coin iff this holds.
DEPOSITING THE COIN IN THE BANK

Merchant
Sends $(A, B, z, a, b, r)$ and $(r_1, r_2, d)$ to the bank.

Bank
Checks that the coin has not yet be deposited. Fraud control
(If it has, call the cops.)

Checks that
\[
\begin{align*}
g^r &\equiv a \cdot h^H(A, B, z, a, b) \\
A^r &\equiv z^H(A, B, z, a, b) \cdot b \\
g_1^{r_1} \cdot g_2^{r_2} &\equiv A^d \cdot B
\end{align*}
\]
(mod $p$)

Accepts the coin iff these check out.
FRAUD CONTROL: I

The spender tries to spend the same coin with the merchant and the vendor.

Merchant
Sends the coin and \((r_1, r_2, d)\) to the bank.

Vendor
Sends the coin and \((r'_1, r'_2, d')\) to the bank.

Bank
Since
\[
\begin{align*}
    r_1 - r'_1 &\equiv us(d - d') \pmod{q} \\
    r_2 - r'_2 &\equiv s(d - d') \pmod{q}
\end{align*}
\]
we have
\[
\begin{align*}
    u &\equiv (r_1 - r'_1)(r_2 - r'_2)^{-1} \pmod{q} \\
    I &\equiv g_1^u \pmod{q}
\end{align*}
\]
↑ the ID of the spender
FRAUD CONTROL: II

The merchant tries to deposit the same coin twice

Once with \((r_1, r_2, d) \leftarrow \text{legit}\)

Once with \((r'_1, r'_2, d') \leftarrow \text{forged}\)

This is hard to do.
The merchant has to produce \(r'_1, r'_2, \text{ and } d'\) \(\exists\)

\[ g_1^{r'_1} \cdot g_2^{r'_2} \equiv A^{d'} \cdot B \pmod{p}. \]
FRAUD CONTROL: III

Someone tries to make an unauthorized coin

This requires finding numbers \( \exists \)

\[
\begin{align*}
g^r & \equiv a \cdot h^{H(A,B,z,a,b)} \\
A^r & \equiv z^{H(A,B,z,a,b)} \cdot b \\
\end{align*}
\]

(\text{mod } p) \quad \text{Discrete logs and worse!}

---

Eve L. Dewer dot com receives a coin from the spender
and tries to spend the coin with the merchant

**Merchant**

Computes \( d' \) for Eve, which is unlikely to equal \( d \).

Etc. see text
ANONYMITY

The spender
never needs to show the merchant an ID.

The bank
never sees the values of $A, B, z, a, b, r$ until the coin is deposited.

the bank and the merchant
cannot figure out the ID of the spender
unless there is double spending.

See text for fuller details