1　デジタルキャッシュ　デモ

1.1　望ましいデジタルキャッシュの性質

1. ネットワークを通じてキャッシュは安全に送信することができる。
2. キャッシュはコピーかつ再使用できない。
3. キャッシュの送り手は匿名であれる。キャッシュが支払われたとき、受け手と銀行は送り手を特定できない。
4. トランザクションはオフラインで行える、つまりトランザクション間に銀行と通信する必要がない。
5. キャッシュを他人に渡すことができる。
6. キャッシュをより小さな単位に分割することができる。

1.2　デモの概要

- 上記の性質の内 1 から 4 を満たす、Chaum スキームを使用したデジタルキャッシュデモ

2　理論的な説明

2.1　初期化

$q = (p-1)/2$ が素数であることを満たすように素数 p を選ぶ。g を $\mathbb{Z}_p^*$ 上において、原始根の二乗とする。
２つの乱数 $k_1, k_2 \in Z_q$ を選び、g_1, g_2 を以下のように定義する。

$$g_1 \equiv g^{k_1} \mod p$$
$$g_2 \equiv g^{k_2} \mod p$$

H を、引数として５つの整数を取り、戻り値として $\mathbb{Z}_q$ 上の整数を返すハッシュ関数とする。
H_0 を、引数として４つの整数を取り、戻り値として $\mathbb{Z}_q$ 上の整数を返すハッシュ関数とする。
最後に g, g_1, g_2, H, H_0 を公開する。

2.2　銀行

銀行は自身の ID として乱数 x を選び、秘密にする。
次に以下の値を計算する。

$$h \equiv g^x \mod p$$
$$h_1 \equiv g_1^x \mod p$$
$$h_2 \equiv g_2^x \mod p$$

最後に h, h_1, h_2 を公開する。

2.3 送り手

送り手は自身の ID として乱数 u を選び、秘密にする。
次に以下の値を計算する。

$$I \equiv g_1^u \mod p$$

次にこの I を銀行に送る。銀行は送り手を識別できるような情報 (例えば、名前、住所、IP アドレスなど) と共に I を保存する。
ここで送り手は u を銀行に送らないことに注意。銀行は I を受け取った後、以下の値を計算しその結果を送り手に送り返す。

$$z' \equiv (Ig_2)^x \mod p$$

2.4 受け手

送り手と同様な手順を踏む。M を送り手の手順において I と同様に計算した自然数とする。

2.5 コインの引き出し

コインを 6 つの数からなるタプル (A, B, z, a, b, r) として定義する。
送り手が銀行からコインを引き出したい場合以下の手順を踏む。

1. 銀行は乱数 w(コインごとに異なる) を選び、以下の値を計算をする。

$$\begin{aligned} g_w &\equiv g^w \mod p \\ \beta &\equiv (Ig_2)^w \mod p \end{aligned}$$

   g_w と β を送り手に送る。
2. 送り手は 5 つの乱数からなるタプル $(s, x_1, x_2, \alpha_1, \alpha_2)$ を選び、以下の計算をする。

$$\begin{aligned} A &\equiv (Ig_2)^s \mod p \\ B &\equiv g_1^{x_1} g_2^{x_2} \mod p \\ z &\equiv z'^s \mod p \\ a &\equiv g_w^{\alpha_1} g^{\alpha_2} \mod p \\ b &\equiv \beta^{s\alpha_1} A^{\alpha_2} \mod p \end{aligned}$$

   $A = 1$ を満たすコインは禁止とする。
3. 送り手は以下の値を計算をする。

$$c \equiv \alpha_1^{-1} H(A, B, z, a, b) \mod q$$

4. 銀行は $c_1 \equiv cx + w \mod q$ を計算し、c_1 を送り手に送る。
5. 送り手は以下の値を計算をする。

$$r \equiv \alpha_1 c_1 + \alpha_2 \mod q$$

   (A, B, z, a, b, r) を送り手が銀行から引き出したコインとする。

2.6 コインを使用する

送り手がコイン (A, B, z, a, b, r) を受け手に使用したい場合以下の手順を踏む。

1. 受け手は以下の等式が成り立つことを確認する。

$$g^r \equiv ah^{H(A,B,z,a,b)} \mod p$$
$$A^r \equiv z^{H(A,B,z,a,b)}b \mod p$$

   上記の等式が成り立つ場合、コインは正当である。
2. 受け手はさらに $d = H_0(A, B, M, t)$ を計算し送り手に送り返す、ここで t はトランザクションの日時を表す自然数する (タイムスタンプ)。
3. 送り手は以下の値を計算をする。

$$r_1 \equiv dus + x_1 \mod q$$
$$r_2 \equiv ds + x_2 \mod q$$

   送り手は r_1, r_2 を受け手に送る。
4. 受け手は以下の等式が成り立つことを確認する。

$$g_1^{r_1} g_2^{r_2} \equiv A^d B \mod p$$

   この等式が成り立つ場合、受け手はコインを受け取る。成り立たない場合は、コインを受け取らない。

2.7 銀行にコインを預金する

受け手が銀行に受け取ったコインを預金したい場合以下の手順を踏む。
受け手はまず銀行にコイン (A, B, z, a, b, r) とタプル (r_1, r_2, d) を送る。

1. 銀行は、コイン (A, B, z, a, b, r) がすでに預金されたことがあるか否かを確認する。されている場合、次のサブセクションである'ID 特定' に移る。
2. 銀行はさらに以下の等式を確認する。

$$g^r \equiv ah^{H(A,B,z,a,b)} \mod p$$
$$A^r \equiv z^{H(A,B,z,a,b)}b \mod p$$
$$g_1^{r_1} g_2^{r_2} \equiv A^d B \mod p$$

   上記の等式が成り立つ場合、コインは正当であることが保証され、銀行はコインを受け手の口座に追加する。

2.8 ID 特定

送り手がコインを 2 度使用し、一方を受け手 1 にもう一方を受け手 2 に送ったとする。
受け手 1 がコインと共に銀行へ送ったタプルを (r_1, r_2, d) とする。

受け手 2 がコインと共に銀行へ送ったタプルを (r_1', r_2', d') とする。
銀行は以下の値を計算をする。

$$r_1 - r_1' \equiv us(d - d') \mod q$$
$$r_2 - r_2' \equiv s(d - d') \mod q$$

$(r_2 - r_2') \mod q$ が可逆の場合、これらの値から $u \equiv (r_1 - r_1')(r_2 - r_2')^{-1} \mod q$ が求まる。
さらに $I \equiv g_1^u \mod p$ を計算することによって送り手を特定することができる。
ここで注意してほしいのが、$(r_2 - r_2') \mod q$ が可逆ではない場合、送り手を特定できないこと。しかし q が十分に大きい場合、特定できない確率は限りなく小さくなる。

参考文献

[1] *Introduction to Cryptography with Coding Theory,2nd Edition*