Brando banko raktai

Privatus banko raktas: skaičius x; Vieši duomenys:

- pirminiai skaičiai p, q, $p-1$ dalijasi iš q;
- trys q-osios eilės elementai g, g_1, g_2;
- h-funkcija $H(x_1, x_2, \ldots) \to \mathbb{Z}_q$;
- dydis $h \equiv g^x \pmod{p}$.

Kliento registracija

Klientas pasirenka atsitiktinį skaičių $U \in \mathbb{Z}_q$, skaičiuoja $I \equiv g_1^U \pmod{p}$ ir siunčia bankui.

I yra kliento identifikavimo numeris banke!

Bankas atsiunčia klientui $z \equiv (Ig_2)^x \pmod{p}$.

Skaitmeninės monetos sukūrimas

1 žingsnis. Klientas pareiškia norą gauti monetą. Bankas parenka atsitiktinį skaičių w ir atsiunčia klientui skaičius
$a \equiv g^w \pmod p, b \equiv (Ig_2)^w \pmod p$.

2 žingsnis. Klientas pasirenka atsitiktinius skaičius s, x_1, x_2, u, v ir skaičiuoja

- $A \equiv (Ig_2)^s \pmod p, \quad B \equiv g_1^{x_1} g_2^{x_2} \pmod p$;
- $z' \equiv z^s \pmod p, \quad a' \equiv a^u g^v \pmod p, \quad b' \equiv b^{su} A^v \pmod p$;
- skaičiuoja $c \equiv H(A, B, z', a', b') u^{-1} \pmod q$ ir siunčia bankui.

3 žingsnis. Bankas skaičiuoja $r \equiv cx + w \pmod q$ ir siunčia klientui.

4 žingsnis. Klientas patikrina lyginius

$$g^r \equiv h^c a \pmod p, \quad (Ig_2)^r \equiv z^c b \pmod p$$

Jeigu lyginiai teisingi, praneša bankui, kad priima monetą ir skaičiuoja $r' \equiv ru + v \pmod q$.
Monetą sudaro skaičiai $[A, B, z', a', b', r']$.
Be to reikia išsaugoti s, x_1, x_2 kurių prireiks parduotuvėje!

Mokėjimas skaitmenine moneta

- Pirkėjas perduoda pardavėjui skaitmeninę monetą $[A, B, z', a', b', r']$.
- Pardavėjas suskaičiuoja $H = H(A, B, z', a', b')$ ir tikrina lyginius

$$g^{r'} \equiv h^H a' \pmod{p}, \quad A^{r'} \equiv (z')^H b' \pmod{p}.$$

- Jei lyginiai teisingi, skaičiuoja $d = H(A, B, P, T)$ ir siunčia pirkėjui; čia P – pardavėjo ID, T – laiko žyma.
- Pirkėjas skaičiuoja

$$r_1 \equiv dUs + x_1 \pmod{q}, \quad r_2 \equiv ds + x_2 \pmod{q}$$

ir siunčia pardavėjui.

- Pardavėjas tikrina lyginį $g_1^{r_1} g_2^{r_2} \equiv A^d B \pmod{p}$. Jei lyginys teisingas, monetą priima ir siunčia bankui

$$[A, B, z', a', b', r'], \quad [d, r_1, r_2].$$

Apgaviko atskleidimas

Jeigu klientas du kartus sėkmingai atsiskaitė moneta $[A, B, z', a', b', r']$, tai bankas gaus

$$[A, B, z', a', b', r'] \text{ su dviem patvirtinimais } [d, r_1, r_2], [d', r_1', r_2'].$$

Tada bankas gali surasti $U \equiv (r_1 - r_1')(r_2 - r_2')^{-1} \pmod{q}$ ir atskleisti apgaviką pagal $I \equiv g_1^U \pmod{p}$.