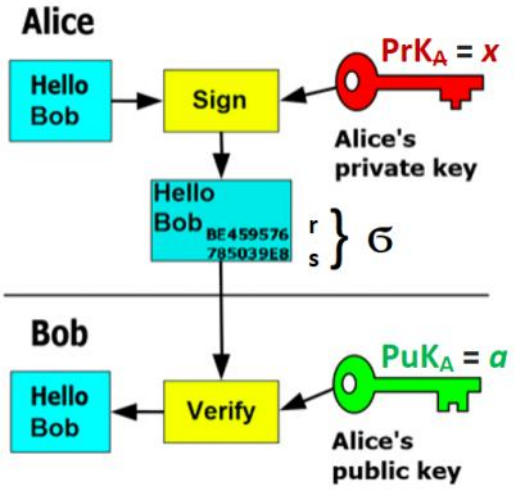
Schnorr Signature



Alice has a message ***M*** in string format to be signed by and sent to **Bob**
M='Hello Bob'
Alice for signature creation uses public parameters **PP=(*p*, *g*)**
Alice's key pair is **PrK_A=*x***, **PuK_A= *a* = g^x mod *p***.

Alice chooses at random ***u***, 1<***u***<***p***-1 and computes first component ***r*** of her signature: $r=g^u \bmod p$. (2.19)
Alice computes H-function value ***h*** and second component ***s*** of her signature: $h=H(M||r)$, (2.20)
$s=u+xh \bmod (p-1)$. (2.21)
Alice's signature on ***h*** is **σ=(*r*, *s*)**.
Alice sends ***M*** and **σ** to **Bob**.

Bob after receiving ***M*** and **σ**, according to (2.20) computes ***h***
$h=H(M||r)$,
Bob verifies if

$$g^s \bmod p = ra^h \bmod p. \quad (2.22)$$

V1 V2

Symbolically this verification function we denote by
$Ver(a,\sigma,h)=V\in\{True, False\}\equiv\{1, 0\}$.

Schnorr Signature Homomorphic property: a single signer

A: Let M_1, M_2 be a messages signed by Schnorr signature

$u_1 \leftarrow rand(\mathcal{Z}_{p-1})$ $\quad$ $u_2 \leftarrow rand(\mathcal{Z}_{p-1})$

$$\mathcal{Z}_{p-1} = \{0, 1, 2, \dots, p-2\} + \bmod(p-1); \cdot \bmod(p-1)$$

$r_1 = g^{u_1} \bmod p$
$h_1 = H(M_1||r_1)$
$s_1 = (u_1 + x\,h_1) \bmod (p-1)$
$Sign(x, u_1, h_1) = \sigma_1 = (r_1, s_1)$

$r_2 = g^{u_2} \bmod p$
$h_2 = H(M_2||r_2)$
$s_2 = (u_2 + x\,h_2) \bmod (p-1)$
$Sign(x, u_2, h_2) = \sigma_2 = (r_2, s_2)$

Let homomorphic function is Hom(x)
Let o is a binary arithmetic operation between 2 numbers x_1 and x_2.

Then mapping Hom( ) is homomorphic with respect to operation $\circ$, if

$$Hom(x_1 \circ x_2) = Hom(x_1) \circ Hom(x_2)$$

Let's define a special multiplication $*$ of signatures σ_1 and σ_2:

$$\sigma_{12} = \sigma_1 * \sigma_2 = (r_1, s_1) * (r_2, s_2) = \big(r_1 \cdot r_2 \bmod p, (s_1 + s_2) \bmod (p-1)\big) = (r_{12}, s_{12}).$$

B: verifies signature σ_{12} according to (2.22)

$$g^{s_{12}} \bmod p = g^{(s_1+s_2) \bmod (p-1)} \bmod p = g^{s_1} \cdot g^{s_2} \bmod p =$$

$$= g^{(u_1 + x \cdot h_1) \bmod (p-1)} \cdot g^{(u_2 + x \cdot h_2) \bmod (p-1)} \bmod p =$$

$$= g^{u_1} \cdot (g^x)^{h_1} \cdot g^{u_2} \cdot (g^x)^{h_2} \bmod p =$$

$$= g^{u_1} \cdot g^{u_2} \cdot (g^x)^{h_1} \cdot (g^x)^{h_2} \bmod p =$$

$$= r_1 \cdot r_2 \cdot a^{h_1} \cdot a^{h_2} \bmod p = r_{12} \cdot a^{(h_1 + h_2) \bmod (p-1)} \bmod p.$$

$$g^{s_{12}} \bmod p = r_{12} \cdot a^{(h_1 + h_2) \bmod (p-1)} \bmod p$$

$$Sign(x, u_1, h_1) * Sign(x, u_2, h_2) = Sign(x, \underbrace{u_1 + u_2}_{\bmod (p-1)}, \underbrace{h_1 + h_2}_{\bmod (p-1)})$$

$$\sigma_{12} = \sigma_1 * \sigma_2 = Sign(x, u_1, h_1) * Sign(x, u_2, h_2) = Sign(x, u_1 + u_2, h_1 + h_2)$$

Since $r_{12} = r_1 \cdot r_2 \bmod$ $= g^{u_1} \cdot g^{u_2} \bmod p = g^{(u_1 + u_2) \bmod (p-1)} \bmod p$.

Schnorr Multi-Signature

Let A_1 and A_2 are two signers having two key pairs signing two messages M_1, M_2: $M_1 \longrightarrow h_1 = H(M_1 \| r_1)$; $M_2 \longrightarrow h_2 = H(M_2 \| r_2)$.

$(PrK_1 = x_1, PuK_1 = a_1 = g^{x_1} \bmod p)$ and $(PrK_2 = x_2, PuK_2 = a_2 = g^{x_2} \bmod p)$

$A_1: Sign(x_1, u_1, h_1) = \sigma_1 = (r_1, s_1) = (g^{u_1} \bmod p, (u_1 + x_1 \cdot h_1) \bmod (p-1))$

$A_2: Sign(x_2, u_2, h_2) = \sigma_2 = (r_2, s_2) = (g^{u_2} \bmod p, (u_2 + x_2 \cdot h_2) \bmod (p-1))$

In the case of signing a general contract with 2 responsible persons A_1, A_2
Let M_1 is an original contract.

Let A_1 is responsible for the technical part.
Let A_2 is responsible for the financial part.

A_1 signs in the following way:

$u_1 \leftarrow rand(\mathbb{Z}_{p-1})$; $r_1 = g^{u_1} \bmod p \rightarrow h_1 = H(M_1 \| r_1)$

$\sigma_1 = (r_1, s_1) = sign(x_1, u_1, h_1)$

A_2 signs in the following way:

$u_2 \leftarrow rand(\mathbb{Z}_{p-1})$; $r_2 = g^{u_2} \bmod p \rightarrow h_2 = H(M_1 \| r_2 \| \sigma_1)$

$\sigma_2 = (r_2, s_2) = Sign(x_2, u_2, h_2)$

Receiver after receiving σ_1, σ_2 wants to create multisignature for both h_1 and h_2.

Receiver multiplies signatures by the special multiplication $*$

$$\sigma_{12} = \sigma_1 * \sigma_2 = (r_1 \cdot r_2 \bmod p, (s_1 + s_2) \bmod (p-1)) = (r_{12}, s_{12}).$$

Receiver sends $\sigma_{12} = (r_{12}, s_{12})$ to the Verifier

Verifier performes verification of $\sigma_{12} = (r_{12}, s_{12})$

$$g^{s_{12}} \bmod p = g^{(s_1 + s_2) \bmod (p-1)} \bmod p = g^{s_1} \cdot g^{s_2} \bmod p =$$

$$= g^{(u_1 + x_1 \cdot h_1) \bmod (p-1)} \cdot g^{(u_2 + x_2 \cdot h_2) \bmod (p-1)} \bmod p =$$

$$= g^{u_1} \cdot (g^{x_1})^{h_1} \cdot g^{u_2} \cdot (g^{x_2})^{h_2} \bmod p =$$

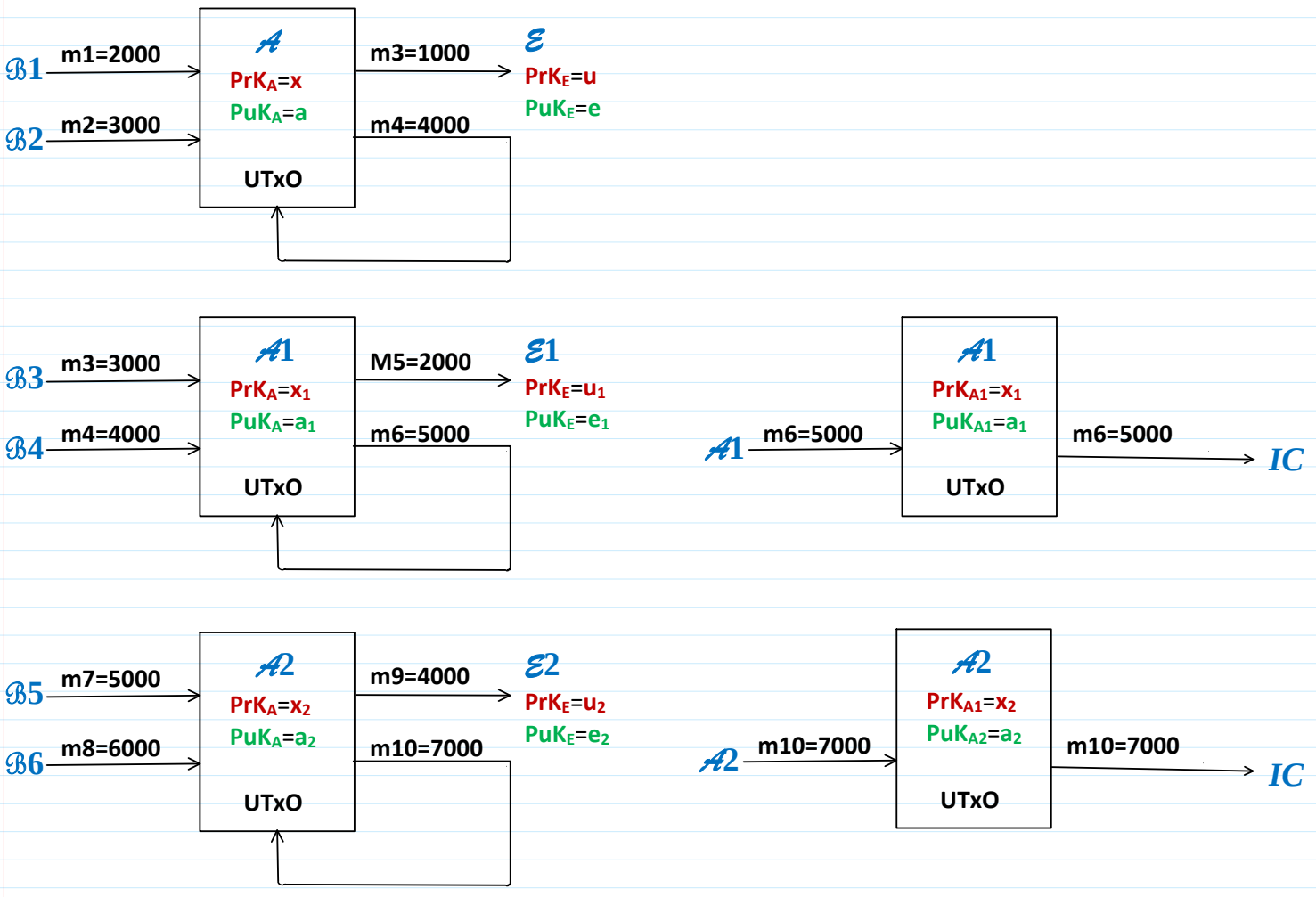
$$= g^{u_1} \cdot r_2 g^{u_2} a_1 (g^{x_1})^{h_1} a_2 (g^{x_2})^{h_2} \bmod p =$$

$h_1 \cdot a^{h_2} \bmod p$.

Verifier accepts the signature δ_{12} on both messages M_1, M_2 corresponding to h_1, h_2 if the following identity holds:

$$g^{s_{12}} \bmod p = r_{12} \cdot a_1^{h_1} \cdot a_2^{h_2} \bmod p.$$

Anonymization-Deanonymization: UTxO paradigm



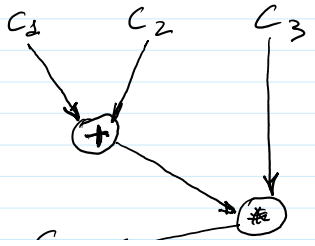
Fully Homomorphic Cryptosystems - Post-Quantum Cryptography (PQC)

Data center case; query about B1 and B2 salary for 12 months

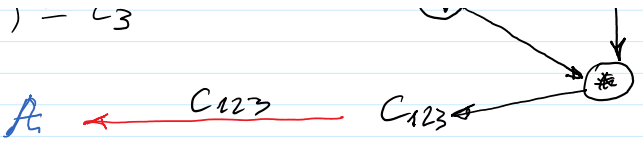
$Enc(a, Sal_{B1}) = c_1$

$Enc(a, Sal_{B2}) = c_2$

$Enc(a, 12m) = c_3$



Enc (u, 12 m) = C_3



Dec (X, C_{123}) = Sal = 12 * (Sal B1 + Sal B2)