Recall: SIS-based CRHF/OWF

$$f_A : [-\beta, \beta]^m \to \mathbb{Z}_q^n$$

$$f_A(u) = A \cdot u$$

Recall: gadget matrix $G \in \mathbb{Z}_q^{n \times m}$ s.t.
$\exists$ poly-time $G^{-1} : \mathbb{Z}_q^n \to \{0,1\}^m$

$$G \cdot G^{-1}(v) = v.$$

Everyone can easily invert $f_G$

Goal: trapdoors for $f_A$

Sample $(A, td) \leftarrow Gen(1^n)$

- Given only $A$, $f_A$ is OWF
- Given td, can invert $f_A$.

Solution: Let $\bar{A} \leftarrow \mathbb{Z}_q^{n\times m}$

$R \leftarrow \{0,1\}^{m\times m}$

$$A = [\bar{A} \mid \bar{A}R + G] \in \mathbb{Z}_q^{n\times 2m}$$

$$td = R$$

- If $m \gg n \log q$ then $A$ is stat. close to uniform. So $f_A$ is a OWF by SIS.

— Given $td = R$ can solve SIS:

For $v \in \mathbb{Z}_q^n$

let $u = \begin{bmatrix} -R \cdot G^{-1}(v) \\ G^{-1}(v) \end{bmatrix}$

$$f_A(u) = [\bar{A} \mid \bar{A}R + G] \cdot u =$$

$$- \bar{A}R \cdot G^{-1}(v) + (\bar{A}R + G)G^{-1}(v)$$

$$= G \cdot G^{-1}(v)$$

$$= v$$

- with a little more work
  can even sample a random inverse

$$(A, \ u \leftarrow \chi^m, \ f_A(u))$$

$$\approx (A, \ \tilde{f}^{-1}_{A,td}(v), \ v \leftarrow \mathbb{Z}_q^n)$$

e.g., choose $u_1 \leftarrow [-\beta, \beta]^m$, $f_A(u_1) = v_1$

let $u_0 = f^{-1}_{A,td}(v - v_1)$

let $u = u_0 + u_1$ : $f_A(u) = v$

Analysis when $\beta = n^{\omega(1)}$:

$$(A, u, f_A(u)) \quad : \quad u \leftarrow [-\beta, \beta]^m$$

$$\approx \left(A, u = u_0 + u_1, \; f_A(u) = \underbrace{f_A(u_0)}_{v_0} + \underbrace{f_A(u_1)}_{v_1}\right)$$

$u_1 \leftarrow [-\beta, \beta]^m$

$v_0 \leftarrow \mathbb{Z}_q^n$

$u_0 \leftarrow f_{A,td}^{-1}(v_0)$

$$\equiv (A, u = u_0 + u_1, \quad v \quad )$$

$v \leftarrow \mathbb{Z}_q^n$

$u_1 \leftarrow [-\beta, \beta]^m$

$v_1 = f_A(u_1)$

$v_0 = v - v_1$

$u_0 = f_{A,td}^{-1}(v_0)$

# GPV

## Signatures from SIS in RO

KeyGen($1^n$): $(A, td) \leftarrow Gen(1^n)$

$pk = A, \quad sk = td$

$Sign_{sk}(x)$: $v = RO(x) \in \mathbb{Z}_q^n$

$u = \tilde{f}_{A,td}^{-1}(v)$ // det.

signature: $u$

$verify_{pk}(x, u)$: $v = RO(x)$

check $f_A(u) \stackrel{?}{=} v$

Security: Break sigs $\rightarrow$ Break SIS

Given $v \leftarrow \mathbb{Z}_q^n$ find $u \in [-B, B]^m$

s.t. $f_p(u) = v$.

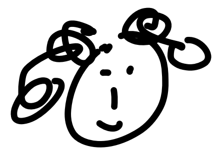
- Run sig adv.
- Choose RO query $x^*$, hope it is forgery
  - program $RO(x^*) = v$
  - $\forall x \neq x^*$ program
    Choose $u_x \leftarrow \chi^m$
    $v_x = f_p(u_x)$

    program $RO(x) = v_x$.
- Answer signature queries with $u_x$.
- Forgery on $x^*$ breaks SIS.

# Homomorphic Signatures

$(pk, sk) \leftarrow Gen(1^n)$

$Sign_{sk}(x) = \sigma$

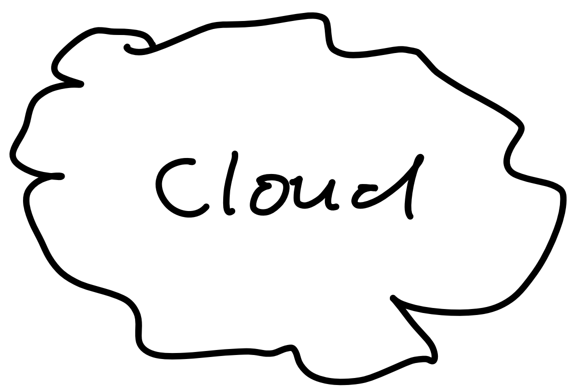

Alice

$\downarrow (x, \sigma)$

$y = f(x)$

$\sigma^* = Eval(f, x, \sigma)$

short




$\downarrow$

$Verify_{pk}(f, y, \sigma^*)$


Bob

Recall: FHE

pk = $A = \begin{bmatrix} \bar{A} \\ s\bar{A} + e \end{bmatrix}$ , sk = $t = [-s, 1$

$t \cdot A \approx 0$

$\mathrm{Enc}_{pk}(x) = C = AR + xG$

$t \cdot C \approx x \cdot t \cdot G$

$\mathrm{Eval}(+, c_1, c_2) = c_1 + c_2$
$\mathrm{Eval}(\times, c_1, c_2) = c_1 \cdot G^{-1}(c_2)$
$\mathrm{Eval}(\mathrm{NAND}, c_1, c_2) = G - c_1 \cdot G^{-1}(c_2)$

$\mathrm{Eval}(f, c_1, \ldots, c_\ell) = c_f$

What if we choose $A \leftarrow \mathbb{Z}_q^{n \times m}$ ?

$Enc_{pk}(x)$:

$C = AR + xG$ is stat close to uniform, indep of $x$.

Think of it as a commitment to $x$.

- $R$ is the "opening"
- commitment is stat hiding / comp. binding

Equivocal given td for $A$:

$R_x = \tilde{f}^{-1}_{A,td}(C - xG)$ opens to $x$.

Can homomorphically compute on openings:

$C_1 = AR_1 + x_1 G$, $C_2 = AR_2 + x_2 G$

$C_+ = A \cdot (R_1 + R_2) + (x_1 + x_2) \cdot G$

$R_+$

$$C_\times = C_1 \cdot G^{-1}(C_2) = (AR_1 + x_1 G)\, G^{-1}(C_2)$$

$$= A \cdot (R_1 \cdot G^{-1}(C_2)) + x_1 (AR_2 + x_2 G)$$

$$= A \cdot (\underbrace{R_1 \cdot G^{-1}(C_2) + x_1 \cdot R_2}_{R_\times}) + x_1 \cdot x_2 G$$

$$C_{NAND} = G - C_\times = G - A(R_\times + x_1 x_2 G)$$

$$A(\underbrace{-R_\times}_{R_{NAND}}) + (1 - x_1 x_2) \cdot G$$

$$\mathrm{Evalopen}(f, \{C_i\}, \{R_i, x_i\}) = R_f$$

$$C_f = AR_f + f(x) \cdot G$$

# FHS Construction

$CRS = C_1, \dots, C_\ell \leftarrow \mathbb{Z}_q^{n \times m}$

$(A, td) \leftarrow Gen(1^n)$

$pk = A$, $sk = td$

$sign_{sk}(x_1, \dots, x_\ell)$:

$R_i := \tilde{f}^{-1}_{A,td}(C_i - x_i G)$

$Eval(f, \{x_i, R_i\}) =$ Use Evalopen: $R_f$ s.t.

$A \cdot R_f = C_f + f(x) \cdot G$

$Verify_{pk}(f, y, R_f)$: Use Eval to get $C_f$

Check $C_f = AR_f + f(x) \cdot G$.

## Security proof:

"program CRS" : $C_i = A R_i + X_i G$

suppose adv creates $f$, $R^*$ s.t.
s.t.

$$\text{Verify}_{pk}(f, y, R^*) = 1 \text{ and}$$

$$f(x) \neq y.$$

Let $R_f$ be sig on $1-y$.

$$A R_f + f(x) \cdot G = A \cdot R^* + (1 - f(x)) G$$

$$\Rightarrow \quad A \underbrace{[R_f - R^*]}_{(1-2f(x))} = G \qquad \text{solve SIS} \boxed{\text{B}}$$

$\underline{\text{Key Property}}$: $\exists$ "short" $H$ s.t.

$$[C_1 - x_1 \cdot G \mid \cdots \mid C_\ell - x_\ell \cdot G] \cdot H = C_f - f(x) \cdot G$$

with $\|H\|_\infty \leq m^d$ $\quad$ $d$ = depth $f$

and $H$ is eff. comp. from $\{C_i, x_i\}$, $f$.

$\Rightarrow$ FHE correctness:

$$t \cdot C_f = \underbrace{t \cdot [\bar{C} - \bar{x} \otimes G] \cdot H}_{\text{small}} + f(x) \cdot t \cdot G$$

$\Rightarrow$ FHS $\quad$ $\text{Eval}_{\text{open}}(f, \{x_i, R_i\})$:

$$R_f = [R_1, \ldots, R_\ell] \cdot H$$

then $\quad A \cdot R_f + f(x) \cdot G =$

$$= A[R_1, \ldots, R_\ell] \cdot H + f(x) \cdot G$$

$$= [C_1 - x_1 G \mid \cdots \mid C_\ell - x_\ell G] \cdot H + f(x) \cdot G$$

$$= C_f - f(x) \cdot G + f(x) \cdot G = C_f$$