$$\Pr[A' \text{ wins}] = \Pr[A \text{ wins} \wedge A' \text{ guesses } j]$$
$$= \Pr[A' \text{ guesses } j] \cdot \Pr[A \text{ wins} \mid A' \text{ guesses } j]$$
$$\geq \frac{1}{q_H} \cdot \frac{1}{\text{poly}} = \frac{1}{\text{poly}}$$

■

The POWER of ROs

1. $H(x) = RO(x)$ is a CRH collision resistant hash function

$$\Pr[H(x) = H(x') : (x,x') \leftarrow\$ A^{RO(\cdot)}(1^\lambda)]$$
$$= \Pr[\exists\, x_i \neq x_j : H(x_i) = H(x_j) \text{ for the queries } x_1, \dots, x_q]$$
$$\leq \binom{q}{2} \cdot 2^{-n} \leq q^2 \cdot 2^{-n} \qquad n: \text{bit size of } x$$
$$= \text{negl}(\lambda) \quad \text{for} \quad n = \omega(\log \lambda), \; q = \text{poly}(\lambda)$$

2. $G^{RO}(x) = RO(x \| 0) \| RO(x \| 1)$ is a PRG

3. $F^{RO}(x) = RO(K \| x)$ is a PRF

4. CCA-2 PKE: OAEP (PKCS #2) from RSA

LECTURE 18 9/12

SIGNATURE SCHEMES

Bilinear groups

$$(G, G_T, g, q, \hat{e}) \leftarrow\$ \text{BilGroupGen}(1^\lambda)$$

(base, target)

i. G, G_T cyclic order q

(ii) $g \in \mathbb{G}$ a generator

(iii) $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is EFF. COMPUTABLE and

bilinear:

biliinearità

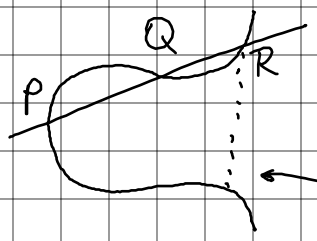
1. $\forall\, g, h \in \mathbb{G},\ \forall\, a, b \in \mathbb{Z}_q$

$$\hat{e}(g^a, h^b) = \hat{e}(g, h)^{ab} \in \mathbb{G}_T$$

2. $\hat{e}(g, g) \neq 1$ non degeneracy

Example: Elliptic curves Groups

$y = x^3 + ax^2 + bx + c \mod p$ $\quad p \in \mathbb{G}$ $\quad Q \in \mathbb{G}$



$P + Q = -R$

$aP = Q$

$a = d\log_P(Q)$

discrete

Obs: DDH does not hold in $\mathbb{G}$

DDH Tuple: $g, g^a, g^b, g^c = g^{ab}$

$$\hat{e}(g, g^c) = \hat{e}(g^a, g^b)$$ ⟸ DDH can be eff. broken if this holds, this is a DDH tuple

Yet, CDH believed to hold

WATERs SIGNATURE

KGen(1^λ): $\text{params} = (\mathbb{G}, \mathbb{G}_T, g, q, \hat{e}) \leftarrow \$\, \text{BilGroupGen}(1^\lambda)$

$a \leftarrow \$\, \mathbb{Z}_q$, $g_1 = g^a$

$g_2, u_0, \dots, u_K \leftarrow \$ G$

$pK = (params, g_1, g_2, u_0, \dots, u_K)$

$sK = g_2^a$

Sign $(sK, m \in \{0,1\}^K)$: $m = m[1], \dots, m[K]$

encoding $\alpha(m) = u_0 \prod_{i=1}^{K} u_i^{m[i]}$

$r \leftarrow \$ \mathbb{Z}_q$

$\sigma = (\underbrace{g_2^a}_{sK} \alpha(m)^r, g^r) = (\sigma_1, \sigma_2)$

Verify $(pK, m, \sigma_1, \sigma_2)$

Check $\hat{e}(g, \sigma_1) = \hat{e}(\sigma_2, \alpha(m)) \cdot \hat{e}(g_1, g_2)$

Why does it work?

Correctness: $\hat{e}(g, \sigma_1) = \hat{e}(g, g_2^a \cdot \alpha(m)^r) =$

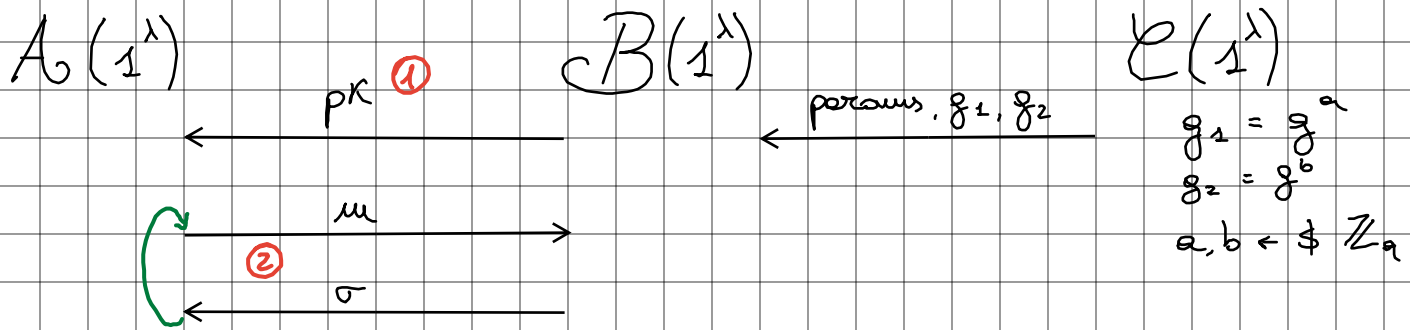
BILINEARITY $= \hat{e}(g, g_2^a) \cdot \hat{e}(g, \alpha(m)^r) =$

$= \hat{e}(g^a, g_2) \cdot \hat{e}(g^r, \alpha(m)) =$

$= \hat{e}(g_1, g_2) \cdot \hat{e}(\sigma_2, \alpha(m))$

THM: WATERS signature is UFCMA assuming CDH

PROOF (Reduction to CDH):



m^*, σ^* ⟶ ③ g_3 ⟶

① The public Key : params = $(G, G_T, g, q, \hat{e})$

g_1, g_2 from $\mathcal{C}(1^\lambda)$

Let $l = 2q_s$ be a parameter

$$u_i = g_2^{x_i} \cdot g^{y_i} \quad \forall\, i \in [0, K]$$

where $y_0, \dots, y_K \leftarrow\$ \mathbb{Z}_q$

$x_1, \dots, x_K \leftarrow\$ \{0, \dots, l\}$

$x_0 \leftarrow\$ \{-Kl, \dots, 0\}$

→ Since y_i's are uniform so are u_i's

Why this strange choice?

Let $\beta(m) = x_0 + \sum_{i=1}^{K} m[i] \cdot x_i$

$\gamma(m) = y_0 + \sum_{i=1}^{K} m[i] \cdot y_i$

Look:

$$\alpha(m) = u_0 \prod u_i^{m[i]}$$

$$= g_2^{x_0} g^{y_0} \prod \left(g_2^{x_i} g^{y_i}\right)^{m[i]}$$

$$= g_2^{x_0 + \sum x_i m[i]} \cdot g^{y_0 + \sum y_i m[i]}$$

$$= g_2^{\beta(m)} \cdot g^{\gamma(m)}$$

② Signature queries m :

If $\beta = \beta(m) = 0 \mod q$

ABORT

Else β^{-1} exists. Let $\gamma = \gamma(m)$

$$\sigma = (\sigma_1, \sigma_2)$$

$$= \left(g_2^{\beta r} \cdot g^{\gamma r} \cdot g_1^{-\gamma\beta^{-1}},\ g^{r} g_1^{-\beta^{-1}} \right)$$

CLAIM: The above signature σ is distributed as a REAL SIGNATURE with coins $\bar{r} = r - a\beta^{-1}$

PROOF (by inspection):

$$\sigma_2 = g^{\bar{r}} = g^{r - a\beta^{-1}} = g^{r} \cdot g^{-a\beta^{-1}} = g^{r} \cdot g_1^{-\beta^{-1}} \quad \checkmark$$

$$\sigma_1 = g_2^{a} \alpha(m)^{\bar{r}} = g_2^{a} \alpha(m)^{r - a\beta^{-1}} = g_2^{a} \cdot \left(g_2^{\beta} \cdot g^{\gamma}\right)^{r - a\beta^{-1}} =$$

$$= g_2^{a}\, g_2^{\beta r - a} \cdot g^{\gamma r - \gamma a \beta^{-1}} =$$

$$= g_2^{\beta r} \cdot g^{\gamma r} \cdot g_1^{-\gamma\beta^{-1}} \quad \checkmark$$

Also if r is UNIFORM, so is $\bar{r}$ ■

③ Solving CDH

Let (m^*, σ^*) be the forgery

If $\beta(m^*) \neq 0 \mod q$

ABORT

Else OUTPUT $g_3 = \sigma_1^* / (\sigma_2^*)^{\gamma(m^*)}$

CLAIM: If $\mathcal{B}$ does not abort, it solves CDH

PROOF: If the forgery is valid,

$$\frac{\hat{e}(g, \sigma_1^*)}{\hat{e}(\sigma_2^*, \alpha(m^*))} = \hat{e}(g_1, g_2) = \hat{e}(g, g)^{ab}$$

$$\Rightarrow \hat{e}(g, g)^{ab} = \frac{\hat{e}(g, \sigma_1^*)}{\hat{e}(\sigma_2^*, \alpha(m^*))}$$

Now, $\alpha(m^*) = g_2^{\beta(m^*)} \cdot g^{\gamma(m^*)} = g_2^{0} \cdot g^{\gamma(m^*)}$

$$\Rightarrow \hat{e}(g, g)^{ab} = \frac{\hat{e}(g, \sigma_1^*)}{\hat{e}(\sigma_2^*, g^{\gamma(m^*)})}$$

$$\Rightarrow g^{ab} = \sigma_1^* / (\sigma_2^*)^{\gamma(m^*)}$$ by BILINEARITY

■