Lec 10 Advanced Encryption

- Identity-Based Encryption (IBE)
- Fully Homomorphic Encryption (FHE)

Pairing: $G, G_T, e: G \times G \to G_T$ $\quad G \cong G_T \cong \mathbb{Z}_q$

let $g \in G$ be a generator $\quad g_T = e(g, g)$

$e(g^a, g^b) \to g_T^{ab} = e(g,g)^{ab}$

↑ efficiently computable

Assumptions

① Bilinear Diffie-Hellman (BDH)

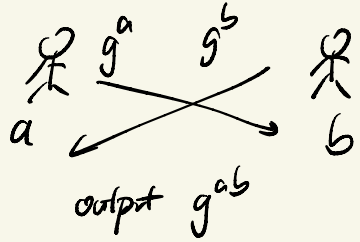
Given $g^a\ g^b\ g^c$, compute g_T^{abc}

② Decisional Bilinear DH (DBDH)

$(G, G_T, e, g, q, g^a, g^b, g^c, g_T^{abc}) \approx_c (G, G_T, e, g, q, g^a, g^b, g^c, g_T^d)$

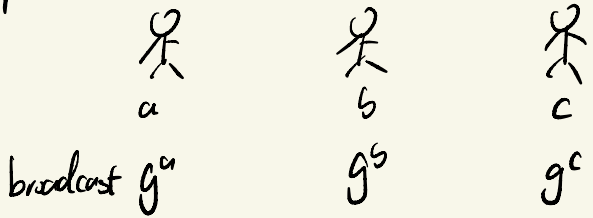
group $\mathbb{G}$. assume DH is hard on $\mathbb{G}$

1-round key exchange



Pairing $e: \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. assume BDH/DBDH

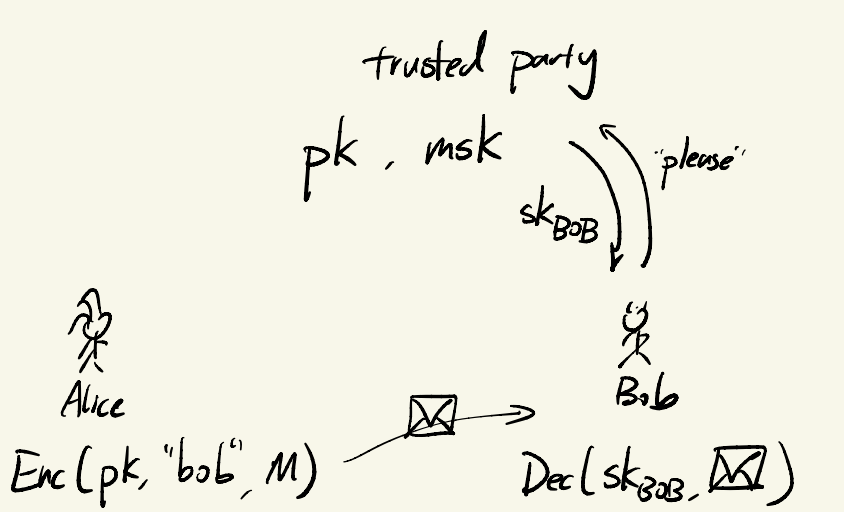
3-party 1-round key exchange



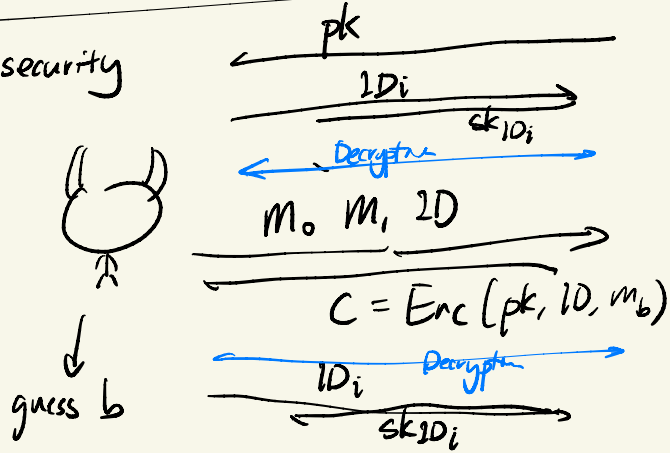
output key $= g_T^{abc} = e(g^a, g^b)^c$

Identity-based encryption

- $Gen(1^\lambda) \to (pk, msk)$
- $Enc(pk, ID, M) \to c$
- $Ext(msk, ID) \to sk_{ID}$
- $Dec(sk_{ID}, c) \to M$



CPA/CCA - security



Pairing-based IBE

$e(g,g)$

$H_2 : G_T \to \{0,1\}^\lambda$

Gen (1^λ) pk: G, G_T, g, g_T, e, g^s, $H : \{0,1\}^* \to G$

msk: s

Ext (msk, ID): $h_{ID} = H(ID)$

let $sk_{ID} = h_{ID}^s$

Enc (pk, ID, m) $= \left(g^r, H_2(e(h_{ID}, g^s)^r) \oplus m \right)$

Dec (sk_{ID}, c) $= \square = e(h_{ID}^s, g^r)$, $m = c \oplus H_2(\square)$

$g_T^{t_{ID}}$

A sees g^s g^r h_{ID}

$\square = g_T^{s \cdot r \cdot t}$

CPA + "one-wayness" $\Rightarrow$ CCA [Fujisaki-Okamoto '99]

$$Enc'(pk, M) = Enc(pk, [\sigma, H_3(\sigma, M)), H_4(\sigma) \oplus M$$

Attribute-Based Encryption (ABE)

$Gen(1^\lambda) \to pk, msk$

$Enc(pk, attr, M) \to c$

$Ext(msk, f) \to sk_f$ $f \in$ some function class

$Dec(sk_f, c) \to m$ if $f(attr) \to 1$

Fully Homomorphic Encryption (FHE)

$Gen \to k$

$Enc(k, m) \to c$

$Eval(f, c_1 c_2 \cdots c_n) \to c$

$Dec(k, c) \to m$

Correctness:

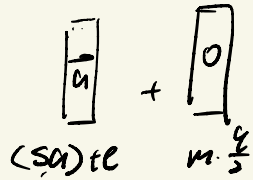
$c_i = Enc(k, m_i)$

$c \leftarrow Eval(f, c_1 \cdots c_n)$ ← f can be any poly-size circuit

$Dec(k, c) = f(m_1, \ldots m_n)$

Add-Homomorphic Encryption (Pset)

$sk = s$

$Enc(m) = c =$ 

$Dec(c)$: $(-s, 1)\begin{bmatrix} a \\ c \end{bmatrix} = e + m \cdot \frac{q}{2}$

$Dec(c_1 + c_2)$: $e_1 + e_2 + (m_1 + m_2) \cdot \frac{q}{2}$

Attempt:

$t = [\, s \;\; [-1] \,]$ (s: $n+1$, $[-1]$: 1)

$sk = s$ (n)

$$Enc(sk, m) = C = \begin{bmatrix} A \\ sA + e \end{bmatrix} + m\mathbf{1}$$

(A: $n \times (n+1)$, $sA + e$: $1 \times (n+1)$, $\mathbf{1}$: $1 \times (n+1)$)

$$Dec(sk, C) \qquad t \cdot C = -e + m \cdot t$$

"$Eval(C_1, C_2)$" Addition

$$t \cdot (C_1 + C_2) = -e_1 - e_2 + (m_1 + m_2)\, t$$

Multiplication

$$\begin{aligned} t \cdot C_1 C_2 &= (-e_1 + m_1 \cdot t)\, C_2 \\ &= -e_1 C_2 + m_1 (-e_2 + m_2 t) \\ &= -e_1 C_2 + m_1 e_2 + m_1 m_2 t \end{aligned}$$

$-e_1 C_2 + m_1 e_2$: too large

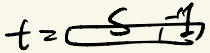
gadget

$$z = \lfloor 1\ 2\ 4\ 8\ \cdots\ 2^{\lfloor \log q \rfloor} \rfloor (z_0\ z_1 \cdots z_{\lfloor \log q \rfloor})^T \quad z \in \{0,1\}$$

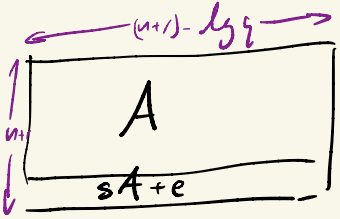
gadget matrix

$$G = \begin{bmatrix} 1\ 2\ 4\ 8\ \cdots & & & \\ & 1\ 2\ 4\ 8\ \cdots & & \\ & & 1\ 2\ 4\ 8\ \cdots & \\ & & & 1\ 2\ 4\ 8\ \cdots \end{bmatrix}$$

any matrix $M = G \cdot \underbrace{G^{-1}(M)}_{\text{0-1 matrix}}$

$t =$ 

Gen: $sk =$ 

Enc: $C :$ 

$+ m G$

Dec: $t \cdot C = -e + m \cdot t G$

Eval: Addition $C_1, C_2 \mapsto C_1 + C_2$

Multiplication: $C_1, C_2 \mapsto C_1 \cdot G^{-1}(C_2)$

$$t \cdot C_1 \cdot G^{-1}(C_2) = (-e_1 + m_1 \cdot t \cdot G)\, G^{-1}(C_2)$$
$$= -e_1 G^{-1}(C_2) + m_1 \cdot t \cdot \cancel{G \cdot G^{-1}}(C_2)$$
$$= -e_1 G^{-1}(C_2) - m_1 e_2 + m_1 m_2 \cdot t G$$

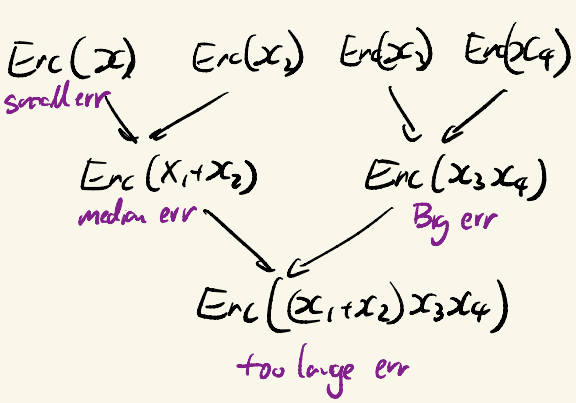
$$C_1 \cdot G^{-1}(C_2)$$
$$= \boxed{\begin{matrix} A \\ sA+e \end{matrix}} \cdot G^{-1}(C_2) + m_1 G G^{-1}(C_2)$$
$$= \boxed{\begin{matrix} B \\ sB+e \end{matrix}} + m_1 \boxed{\begin{matrix} A' \\ sA'+e \end{matrix}} + m_1 m_2 G$$
$$= \boxed{\begin{matrix} C \\ sC+e \end{matrix}} + m_1 m_2 G$$

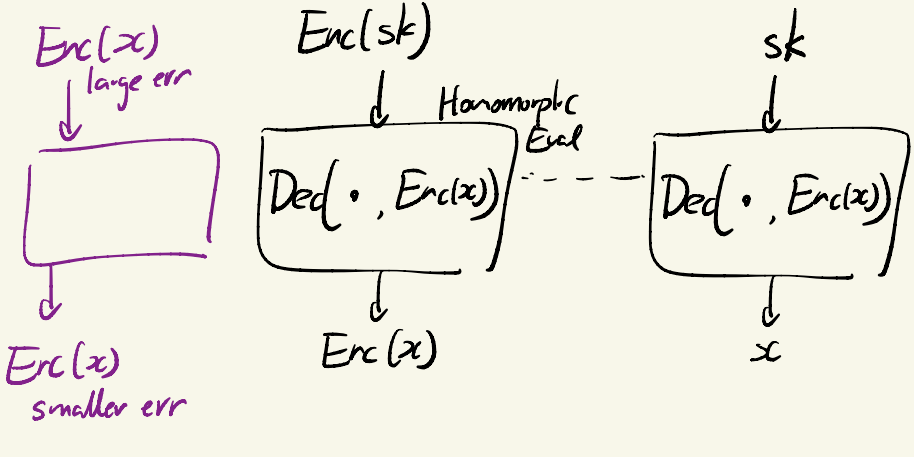
Somewhat Homomorphic Encryption —Bootstrap→ FHE

allows homomorphic evaluation of f if $\text{depth}(f) \leq ???$

- Bootstrap: circular security
- Bootstrap: Decryption has low-depth circuit

Circular security $\hat{=}$ fine to reveal $\text{Enc}_{sk}(sk)$





① FHE w/o circular security iO + OWF ⇒ FHE

sub-exp LWE + blabla ⇒ iO

② FHE based on cheaper assumptions

③ optimization:

e.g. SIMD: (multiple, data; single, instruction)

FHE

$Enc(x) \to Enc(f(x))$

SIMD ver

$Enc(x_1\ x_2\ x_3 \cdots)$

$\hookrightarrow Enc(f(x_1)\ f(x_2) \cdots)$

$C : \begin{bmatrix} A \\ sA+e \end{bmatrix}$ ($n+1$ rows, $(n+1)\cdot \lg q$ columns) $+ \begin{bmatrix} m_1 m_2 \cdots m_{n\lg q} \end{bmatrix} G$

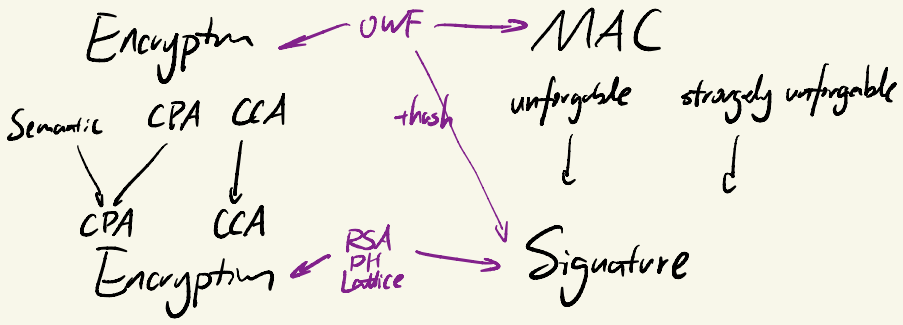
e.g. rate-1 FHE

$$\text{rate} = \frac{\text{ciphertext length}}{\text{msg length}}$$

Lec "11" Digital Signature

Secret-Key

Public-Key

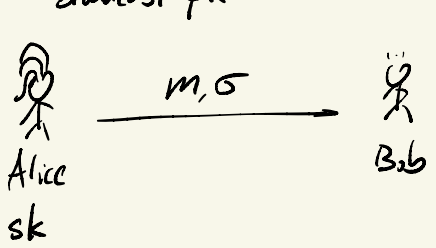


Signature = (Gen, Sign, Verify)

Gen(1^λ) → sk, pk

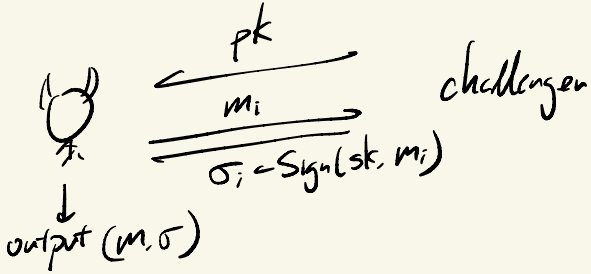
Sign(sk, m) → σ (signature)

Verify(pk, m, σ)



secure

Signature Scheme is existentially unforgeable




wins iff $m \notin \{m_i\}$
and $Verify(pk, m, \sigma) = 1$

Lamport's Signature (based on hash function)

① $\mathcal{M}=\{0,1\}$ $\quad sk=(r_0\ r_1)$ $\quad pk=(H(r_0),\ H(r_1))$ Secure

② $\mathcal{M}=\{0,1\}^n$ $\quad sk=\begin{pmatrix} r_{1,0} & r_{1,1} \\ r_{2,0} & r_{2,1} \\ \vdots & \\ r_{n,0} & r_{n,1} \end{pmatrix}$ $\quad pk=\begin{pmatrix} H(r_{1,0}) & H(r_{1,1}) \\ \vdots & \vdots \\ H(r_{n,0}) & H(r_{n,1}) \end{pmatrix}$ $\quad Sign_2(m) = (r_{1,m_1}, r_{2,m_2}, \ldots, r_{n,m_n})$

Secure (one-query)

③ $\mathcal{M}=\{0,1\}^*$ $\quad$ ② + CRHF $\quad Sign_3(m) = Sign_2(H(m))$

Secure (one-query)

hash-and-sign

④ $\mathcal{M}=\{0,1\}^*$

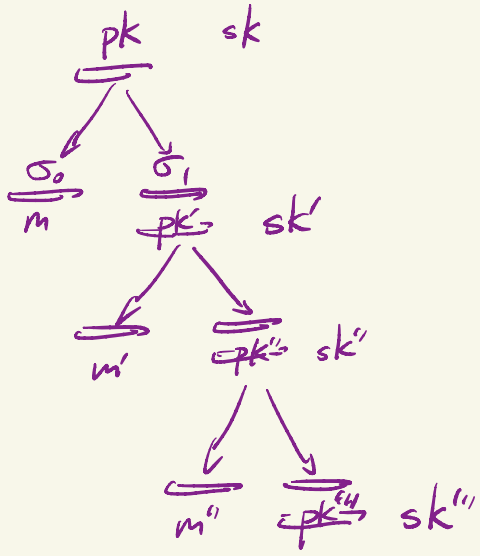
Secure (2-query)

Solutions → ③ but model H as a random oracle

stateful

$$sk=\begin{matrix} 0 \\ \begin{pmatrix} r_{1,0} & r_{1,1} \\ r_{2,0} & r_{2,1} \\ \vdots & \\ r_{n,0} & r_{n,1} \end{pmatrix} \end{matrix} \quad \begin{matrix} 1 \\ \begin{pmatrix} r_{1,0} & r_{1,1} \\ r_{2,0} & r_{2,1} \\ \vdots & \\ r_{n,0} & r_{n,1} \end{pmatrix} \end{matrix}$$

"Chain" — pk
stateful signature — sk



Sign(m)

sk', pk'

$\sigma_0 = \text{Sign}(sk, m, 0)$

$\sigma_1 = \text{Sign}(sk, pk', 1)$

output σ_0

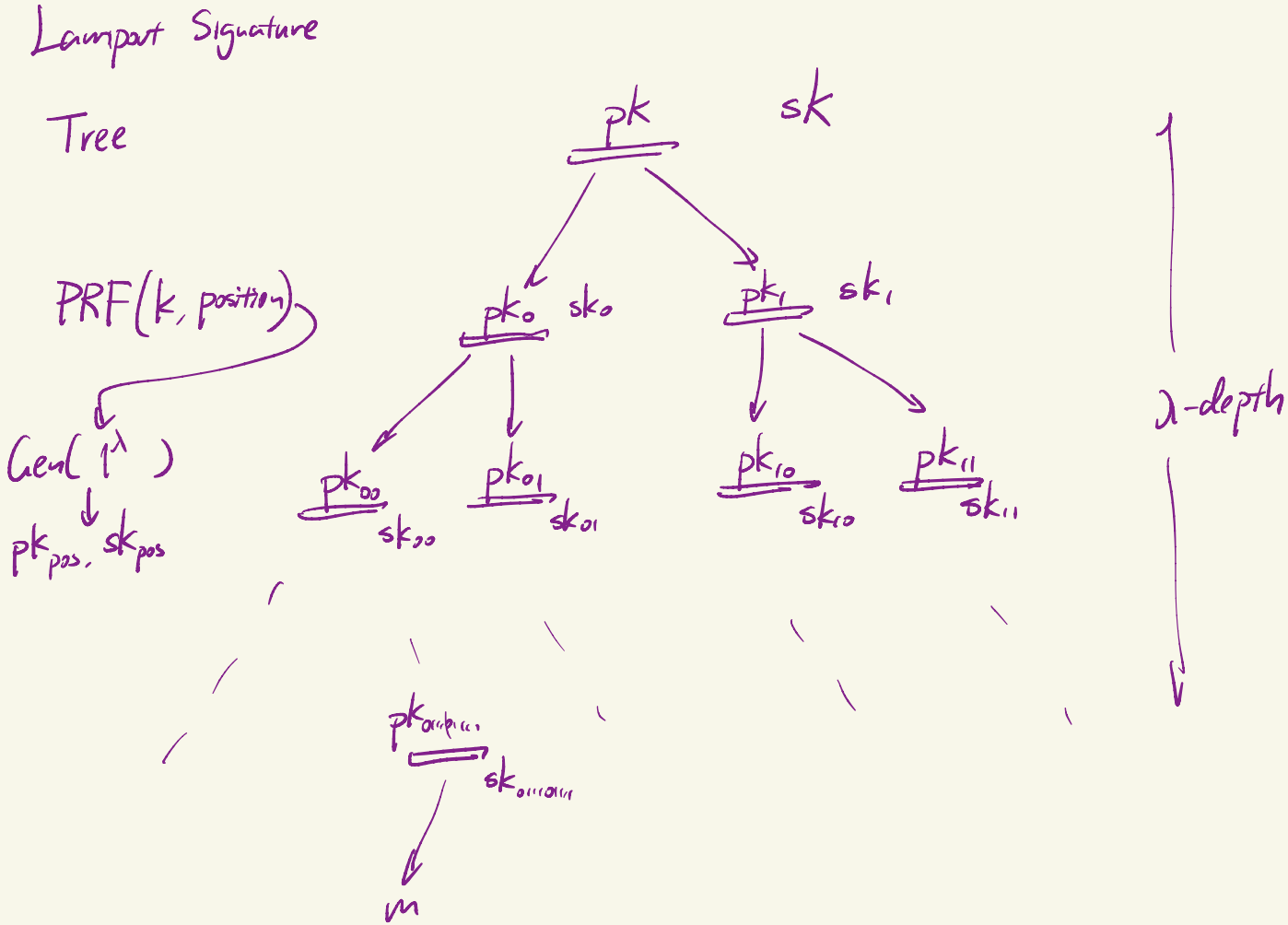
Sign(m')

sk'', pk''

$\sigma_0' = \text{Sign}(sk', m', 0)$

$\sigma_1' = \text{Sign}(sk', pk'', 1)$

output $(pk', \sigma_1, \sigma_0')$


Lamport Signature
Tree
pk
sk
PRF(k, position)
pk_0 sk_0
pk_1 sk_1
Gen(1^λ)
pk_{pos}, sk_{pos}
pk_{00} sk_{00}
pk_{01} sk_{01}
pk_{10} sk_{10}
pk_{11} sk_{11}
λ-depth
m