LECTURE 13

ATTRIBUTE-BASED ENCRYPTION

$\text{KeyGen}(1^\lambda) \rightarrow \text{MPK}, \text{MSK}$

$\text{Enc}(m, x, \text{mpk}; r) \rightarrow ct$ where $x \in \{0,1\}^\ell$

$\text{SKGen}(f, \text{msk}; r) \rightarrow sk_f$

where $f : \{0,1\}^\ell \rightarrow \{0,1\}$.

$\text{Dec}(x, f, sk_f, ct) \rightarrow m$ or $\perp$ if $f(x) = 1$

IBE is a special case where

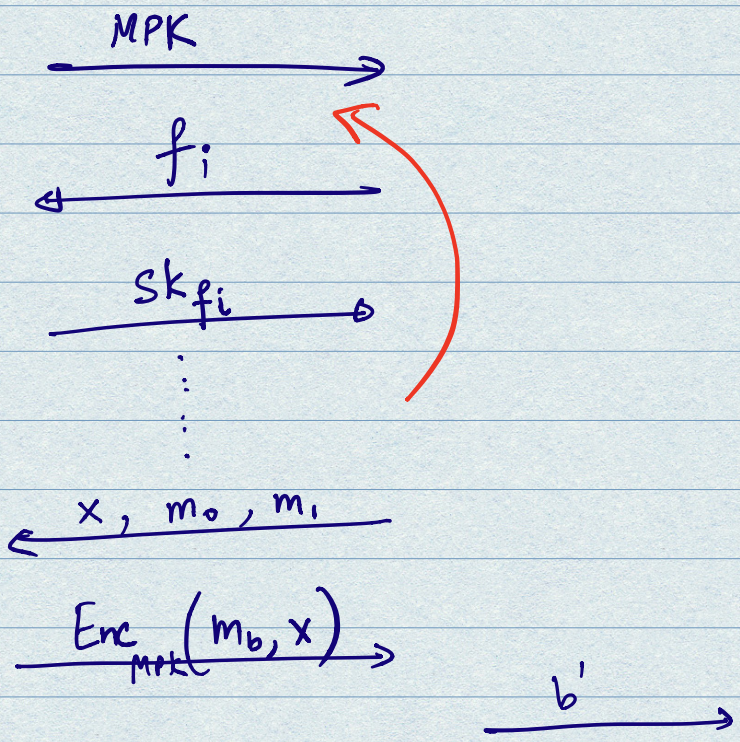
$f \equiv f_{id}$, $f_{id}(v) = 1$ when $v = id$
$= 0$ o/w

and $x = id$

SECURITY

Challenger | Adversary

(MPK, MSK)



Adv wins if $(b' = b)$ AND $(\forall i, f_i(x) = 0)$,

We will say that ABE is secure

$$Pr[Adv \text{ wins}] \leq \frac{1}{2} + negl(\lambda)$$

GSW HOMOMORPHIC ENCRYPTION

TWO FACTS

(1) Invariant : $tA = \mu tG + \text{error}$

$*$

$$t(A_1 + A_2) = (\mu_1 + \mu_2)\, tG + \text{error}$$

$$t(A_1 G^{-1}(A_2)) = \mu_1 \mu_2\, tG + \text{error}$$

$$t(A_f) = f(\mu)\, t\, G + \text{error}$$

$$t(A_f - f(\mu)\, G) = \text{"small" error} \approx 0.$$

(2) TAKE MATRICES

$$A_1 \ldots\ldots A_\ell$$

Take

$$\left[A_1 - \mu_1 G \,\|\, A_2 - \mu_2 G \,\|\, \ldots\ldots \,\|\, A_\ell - \mu_\ell G\right]$$

Then $\exists$ a matrix $H_{f,\vec{\mu}=\mu_1,\ldots,\mu_\ell}$ with "small" entries s.t.

$$\left[A_1 - \mu_1 G \,\|\, A_2 - \mu_2 G \,\|\, \ldots\ldots \,\|\, (A_\ell - \mu_\ell G)\right] H_{f,\vec{\mu}}$$

$$= A_f - f(\vec{\mu}) G$$

f = "+" function

$$\left[A_1 - \mu_1 G \,\|\, A_2 - \mu_2 G\right]\begin{bmatrix} I \\ I \end{bmatrix} = (A_1 + A_2) - (\mu_1 + \mu_2) G$$

f : "$*$" function

$$\left[A_1 - \mu_1 G \,\|\, A_2 - \mu_2 G\right] \begin{bmatrix} G^{-1}(A_2) \\ \mu_1 I \end{bmatrix}$$

$$= A_1 G^{-1}(A_2) - \mu_1 \mu_2 G$$

BGG$^+$ ABE Scheme

$\text{KeyGen}(1^\lambda) \rightarrow \text{MPK} = A, A_1, \ldots, A_\ell, v \in \mathbb{Z}_q^n$

$\text{MSK} = T_A$

$\text{Enc}(m, x, A, A_1, \ldots, A_\ell; r) \rightarrow ct$

$ct_1 \rightarrow s^T \left[A \,\|\, A_1 - x_1 G \,\| \ldots \| A_\ell - x_\ell G\right]$ + noise

$ct_2 \rightarrow s^T v$ + noise + $m\lfloor \frac{q}{2} \rfloor$

Claim: Given f, x, $ct = (ct_1, ct_2)$

$$ct = s^T \left[A \,\|\, A_1 - x_1 G \,\|\, \cdots \cdots \,\|\, A_\ell - x_\ell G \right] + \text{noise}$$

anyone can compute $H_{f,x}$

s.t. $ct \begin{pmatrix} I & 0 \\ 0 & H_{f,x} \end{pmatrix} = s^T \left(A \,\|\, A_f - f(x)\, G \right) + \text{noise}$

[By FACT 2].

Decryption should be possible if (and only if) $f(x) = 1$. , i.e.

$$ct \cdot H_{f,x} = A_f - G$$

$\mathsf{SKGen}(msk, f) \rightarrow sk_f$

$msk = T_A$

sk_f = "short" solution r to

$$\left[A \,\|\, A_f - G \right] \cdot r = v$$

$\mathrm{Dec}(sk_f, ct, f, x) \longrightarrow$

Compute $ct \cdot \begin{bmatrix} I & 0 \\ 0 & H_{f,x} \end{bmatrix} =$

NOTE: This is $s^T \left[A \,\|\, A_f - f(x) G \right] + \text{noise}$

If $f(x) = 1$ then this is

$s^T A' + \text{noise}$ where $A' = [A \| A_f - G]$

sk_f = "short" solution to $A' r = v$.

H.W. Given r, $s^T A' + \text{noise}$, $s^T v + m\lfloor \frac{q}{2} \rfloor + \text{noise}$,

show that it is easy to recover $m\lfloor \frac{q}{2} \rfloor + \text{noise}$

Δ thus recover m.

[Hint: Dual-Regev!]

RECALL: (Sampling Type-1 trapdoor)

If I sample $B = [A \| AR + G]$

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

then $T_B = \begin{bmatrix} I + RG^{-1}(A) & -RT_G \\ -G^{-1}(A) & T_G \end{bmatrix}$

is a trapdoor for B.

where T_G is s.t. $G T_G = 0$.

H.W.: Check this!

NOTE: Only need to know R to find this trapdoor.

For

$B = [A \| AR + \alpha G]$ where $\alpha \neq 0$ and α is "short",

$T_B = \begin{bmatrix} \alpha I + RG^{-1}(A) & -RT_G \\ -G^{-1}(A) & T_G \end{bmatrix}$

is a trapdoor for B