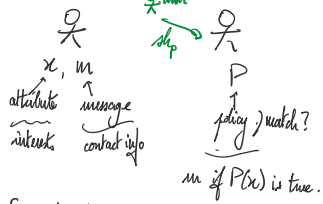


FHE: compute over encrypted data
 FH. signature: "verify computation".

ABE: Access structure.



Security: if $P(x)$ is false \rightarrow m hidden.

Def: ABE.

Setup: mkh / master public key
 msk / master secret key

KeyGen(msk, P): sk_p

Enc(msk, x, m): $ct(x, m)$

Dec($ct(x, m), sk_p$): m .

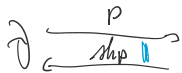
Correctness:

$Dec(ct(x, m), sk_p) = m$
 if $P(x) = true$

Security



$x^*, (m_0, m_1) \rightarrow ct$ $Enc(x^*, m_0) = ct^*$



For all efficient ct , $\left| \Pr[ct(-) = b] - \frac{1}{2} \right| \leq \text{negl}(\lambda)$.

if for all P , $P(x) = false$.

Construction from WE.

FHE (GSW)/FH. sig: $[A_i + x_i \cdot G] \rightarrow [A_i + f(x_i) \cdot G]$

FHE: $A_i = \begin{bmatrix} B \\ s^T B + e \end{bmatrix} \cdot R$
randomize

FH. sig. A_i with trapdoor.

C_1, C_2 : $+ C_1 + C_2$ ($\forall A_x = A_1 + A_2$) ✓

$\times C_1 \cdot G^{-1}(C_2)$ ($\forall A_x = A_1 \cdot G^{-1}(C_2)$)

ABE: "Encrypt m under A_i " // ct
 "Trapdoor for A_i " // sk .

$$C_1 = A_1 + x_1 G \quad | \quad - A_1 \cdot G^{-1}(A_2) \quad x_1 A_2 + x_1 x_2 G$$

$$C_2 = A_2 + x_2 G \quad | \quad \boxed{C_x = -C_1 \cdot G^{-1}(A_2) + x_1 C_2}$$

$-A \cdot G^{-1}(A_1) \rightarrow A$

$$C_x = -C_1 \cdot G^{-1}(A_2) + x_1 \cdot C_2$$

$$= -A_1 G^{-1}(A_2) + x_1 A_2$$

$$C_x = -A_1 G^{-1}(A_2) + x_1 x_2 G$$

- ① Encode the policy checking
- ② How to encode the message. ||
- ③ Security?

$$P(x) = \text{true} \\ = 0$$

"Secret key": Trapdoor for A_p . || $s^T A_p + e \rightarrow s$

$$A_i \rightarrow A_p$$

$$s^T (A_i + x_i G) \xrightarrow{(+noise)} s^T (A_p + P(x)G) \xrightarrow{(+noise)}$$

\hookrightarrow recover s

$$ct(x) : s^T (A_i + x_i G) \quad ||$$

\downarrow (+noise)

$$Dec(ct, \frac{sk_p}{P}) : s^T (A_p + P(x)G) \rightarrow s.$$

How to generate those trapdoors?

Trapdoor delegation.

Trapdoor for A : short matrix R

$$st. A \cdot R = G. \quad s^T G + e$$

$$\left[\begin{matrix} 1 & z & \dots & z^{log_2 q} \\ & & & \vdots \\ & & & 1 \end{matrix} \right]^d$$

Claim 1: Given $s^T G + e$, it is easy to find s .
(Exercise: $q = z^h$)

Claim 2: Can convert $s^T A + e \rightarrow s^T G + e'$

Instead of trapdoor for A_p , \bar{A}

trapdoor for $[\bar{A} || A_p]$. \rightarrow mod.

Claim: Given a trapdoor for \bar{A} , can derive trapdoor for $[\bar{A} || A_p]$. || $R st. [\bar{A} || A_p] R = G$

trapdoor for $[A \| A_p]$. $\exists R$ s.t. $[A \| A_p]R = G$.

[Micciancio's Perfect trapdoor]
 Building \bar{A}
 $\bar{A} = [A \| A_p + G]$
 $\bar{A} \cdot \begin{bmatrix} -R \\ I \end{bmatrix} = G$

cl: Given any u , can find short p s.t. $\bar{A}p = u$.
 $p = \begin{bmatrix} -R \\ I \end{bmatrix} G^{-1}(u)$
 $\bar{A} \cdot p = G \cdot G^{-1}(u) = u$

$$[\bar{A} \| A_p] \begin{bmatrix} R_1 \\ R_2 \end{bmatrix} = \underbrace{\bar{A} \cdot R_1}_{G - A_p R_2} + A_p R_2 = G$$

$R_2 \leftarrow$ short random
 R_1 s.t. $\bar{A} \cdot R_1 = G - A_p R_2$
 sample using trapdoor for \bar{A}

Scheme: Summary l_c : length of attribute x .

Setup: \bar{A} , with trapdoor
 $\{A_i\}_{i \in h}$
 $\text{mpk} = (\bar{A}, A_i)$
 msk : trapdoor for \bar{A}
 $(Pk(x)=0 \Rightarrow \text{authorized})$

① If R is a trapdoor for A
 $s^T A + e$
 $R \rightarrow s$ } correctness

KeyGen(msk, P): Derive A_p
 Derive trapdoor for $[\bar{A} \| A_p]$

② Given trapdoor for \bar{A}
 "can derive trapdoor for $[\bar{A} \| A_p]$ " } correctness
 "looks independent of trapdoor for \bar{A} " } security

Enc(mpk, x, m): $s^T(\bar{A}) + \text{noise}$
 $s^T(A_i + x_i G) + \text{noise}$

Symmetric-key encrypt(s, m):
 (Hard-core bits (NWE symmetric))

An instantiation:

$$\bar{A} = [A \| A_p + G] ; \bar{A} \begin{bmatrix} -R \\ I \end{bmatrix} = G$$

Dec(ct, sk_p):
 Evaluate $\rightarrow s^T(A_p + P(x)G)$ (+more noise)
 use trapdoor to recover s

Delegation: $[\bar{A} \| A_p]$:
 sample R_2 , output $R_1 = \begin{bmatrix} -R \\ I \end{bmatrix} G^{-1}(G - A_p R_2)$
 make \bar{R}_1

use trapdoor to recover s
 recover m .

sample R_2 , output $R_1 = \begin{bmatrix} -R \\ I \end{bmatrix} G^{-1} (G - AR_2)$
 output $\begin{bmatrix} R_1 \\ R_2 \end{bmatrix}$

Security: Way to generate trapdoors for all A_p
 $A_i \rightarrow A_p$ st. $P(x) = 1$ (false).

$$\begin{aligned} \mathcal{S}^T(A_i + x_i G) + \text{noise} &\rightarrow \mathcal{S}^T(A_p + P(x)G) + \text{noise} \\ AR_i &\rightarrow AR_p \quad \parallel \text{if } A_i = AR_i + x_i G \\ [A \parallel AR_p + G] &\leftarrow R \text{ trapdoor.} \\ &\quad \wedge \\ &\quad P(x) = 1 \end{aligned}$$

Summary: Attribute Based Encryption from WE.

- ① "leveled" circuits. (bound on circuit depth) d
 How to remove? Bootstrapping.
- ② ciphertexts $\text{poly}(k, d)$
 secret key $\text{poly}(d)$.
- ③ Weaker form of selective security.
 Remove restriction from similar assumptions.