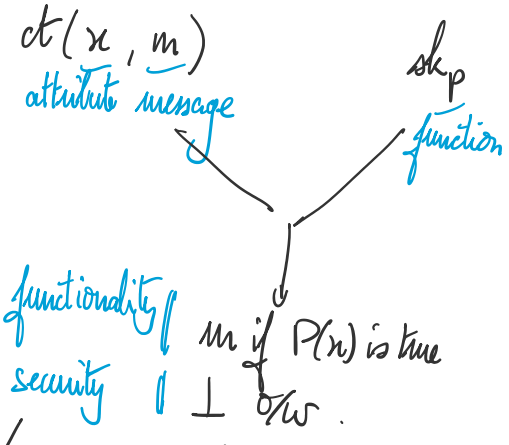
ABE part 2

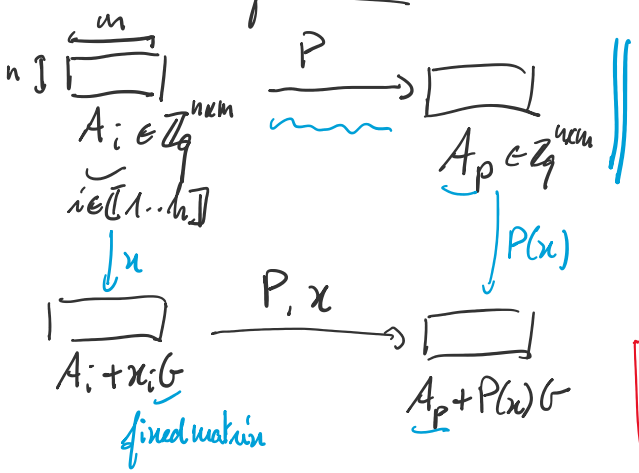
Thursday, October 1, 2020 2:51 PM

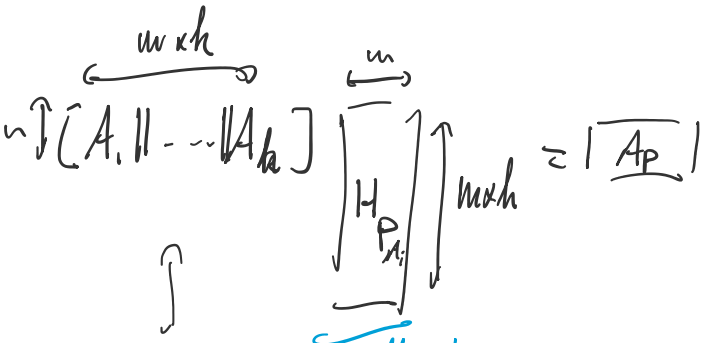
Previously:

Attribute-Based Encryption:



Construction from LWE:





$$[A_1 + x_1 G \| \cdots \| A_{hm} + x_{hm} G] \begin{bmatrix} H_{P,x} \\ A_i \end{bmatrix} = \boxed{} \quad A_P + P(x)G$$

small entries.

Main idea: A_i: "public keys"

A_P: "function public key"

encryption: $s^T(A_i + x_i G) + e_i$: "encoding of x_i"

when decrypting: $s^T(A_P + P(x)G) + e^{++}$

When decrypting: $s^T(A_p + P(x)G) + e^{++}$

* Trapdoors: secret key for policy P: trapdoor for A_p.

① * Functionality: how to produce trapdoors?

② * Security: "trapdoor for A_p shouldn't give info about trapdoor for A_p"

---

① If trapdoor for A (master secret key) $\longrightarrow$ trapdoor for $[A \| \overline{A_p}]$ (new: A_p).

② Want: generate trapdoors for A_p, $P(x) = \text{true}$.

doesn't allow $\longrightarrow$ $P(x) = \text{false}$.

Alternate way of generating trapdoors:

(Trapdoor for A: R small st $AR = G$).

(*) $A = [\bar{B} \| \bar{B}\bar{R} + G]$ $\longrightarrow$ $R = \begin{bmatrix} -\bar{R} \\ I \end{bmatrix}$ $\Big\}$ $AR = G$

small if $\bar{R}$ is small.

For correctness: (results from hom.)

$\overline{A_p} = [A \| A_p]$: if trapdoor for $A \longrightarrow$ trapdoor for $\overline{A_p}$

$\longrightarrow$ trapdoor

(*) if $A_p = A\bar{R} + G$ $\xrightarrow{\bar{R}}$ trapdoor for $\overline{A_p} = [A \| A_p]$

Trapdoor for A:

LWE: $s^T A + e \xrightarrow{\text{hard}} s^T$. ($A$ random)

with trapdoor: $s^T A + e \xrightarrow{\text{trapdoor}} s^T$.

Construction:

Trapdoor := small matrix R st $AR = G$.

[Ajt] If $M_p = M|C + G \longrightarrow$ trapdoor for $A_p = [A \| A_p]$

if $P(x)=1$, $A_p = A\bar{R} + P(x)G$.

$R_{A_p} = \begin{bmatrix} -\bar{R} \\ I \end{bmatrix}$

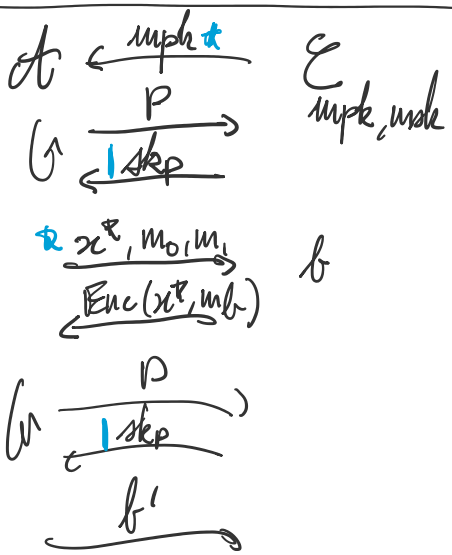
$P(x)=1 \rightarrow$ false.

↳ if know $\bar{R}$ st $A_p = A\bar{R} + G$

↳ trapdoor for $[A \| A_p] = \bar{A}_p$.

(only uses $\bar{R}$, not trapdoor for A)

Proof of security:



Security: for all Poly. time A

$|P[b'=b] - 1/2| \leq 1/n^c$ for all c. (2^{-n})

if $P(x^*) =$ false.

Suppose that x^* is fixed in advance.

We'll set: $A_i = A\bar{R}_i - x_i^* G$. ($\bar{R}_i + x_i^* G$)

original scheme: A_i random — small — uniform by leftover hash lemma.

$[R_1 - x_1^* G \| \cdots \| R_\ell - x_\ell^* G] \begin{bmatrix} \cdots \end{bmatrix}$

$$[B_1 - x_1^* G \,\|\, \cdots \,\|\, B_k - x_k^* G] \left[H_{P, B_i, x^*} \right] = B_p - P(x) G.$$

$$B_i = A \cdot R_i \qquad \begin{bmatrix} \\ B_p \end{bmatrix} = [A] \left([R_i] \cdots [R_k] \right) \left[H_{P, B_i} \right]$$

$$B_p = A \cdot R_p$$

small. $\qquad R_p$

$$A_p = B_p + P(x) G$$
$$= A \cdot R_p + P(x) G$$

Now: relation between A and A_p!

$R_p \longrightarrow$ derive trapdoor for $[A \| A_p]$.

use R_p to derive sk_p:

all the secret key queries satisfy $P(x) = 1$.

if $P(x) = 0 \qquad A_p = A \cdot R_p$.

$$s^T A + e_1 \,,\; s^T A_p + e_2 \;/\!/\; s^T [A \| A_p] + \underline{e}$$

$\sim$

$$\rightarrow s^T A + e \,,\; (s^T A + e) \cdot R_p$$

$s^T A + e$, $s^T (A_i + x_i G) + e_i$ // part of the ciphertext

$s^T A + e$, $s^T(A_i + x_i G) + e_i$ // part of the ciphertext

$\rightarrow s^T(A_p + \underbrace{P(x)}_{0} G) + e''$

$s^T A + e$, $s^T A \cdot \Pi_i + e_i$ //

$\times \Pi_i$

Now : invoke the LWE assumption

unif , unif $\cdot \Pi_i$

Now m is hidden.

A note on hypothesis.

I assumed that x^* is set in advance.

In proof, I set $\underbrace{A_i}_{\text{mpk}} = A\Pi_i - x_i^* G$.

We showed selective security

$\mathcal{A} \xrightarrow{x^*} \| \xleftarrow[\text{mpk}]{} \mathcal{C}$

---

① Not an issue if willing to assume sub-exponential hardness of LWE

① Not an issue if willing to assume sub-exponential hardness of LWE.

② Open: do from polynomial hardness (??)

The ABE we saw:

* is compact: ciphertext, secret keys $\propto O(d)$ where d is a bound on circuit depth of P

* Need some bound d on depth: "levelled" scheme...
  full one?

Extensions (techniques)

* Predicate encryption: attribute is hidden (against unauthorized keys)

* Functional encryption: ct_x, sk_P → $P(x)$

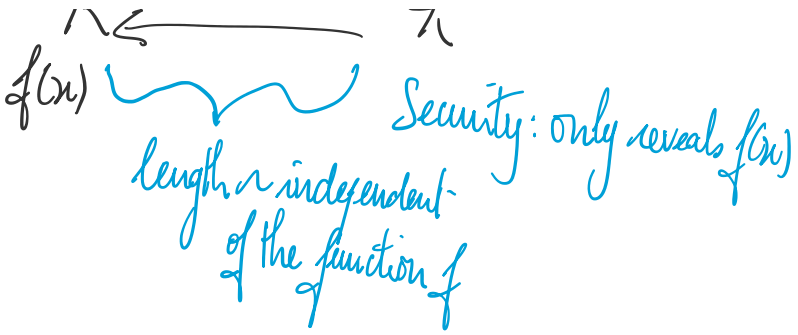
  some versions using ABE (+FHE)
  (weak)

  deep connections with indistinguishability obfuscation

* Laconic Function Evaluation:

  f $\mathcal{O}_K$ —A_f→ $\mathcal{O}_K x$

  $f(x)$


f(x)
Security: only reveals f(x)
length n independent
of the function f