Security proof for the ABB IBE and ABE for circuits

Nacim Oijid

September - December 2019

1 Security Proof of ABB

Lemma 1 (generalized leftlover hash lemma)**.** *Let $H : \{h : X \to Y\}_{h \in H}$ a universal hash family and let a function $f : X \to Z$. For finite sets X, Y, Z. For a random variable T over X, if $\gamma(T) := \max_t Pr[T = t] = 2^{-H_\infty(T)}$.*

We have $\Delta((h, h(T), f(T)), (h, U(Y), f(T))) \leq \frac{1}{2}\sqrt{\gamma(T)|Y||Z|}$
If $T_1, \ldots, T_k$ are independent random variables over X letting $\gamma = \max_r \gamma(T_r)$,
we have $\Delta((h, h(T_1), f(T_1), \ldots, h(T_k), f(T_k)), (h, U_\gamma^{(1)}, f(T_1), \ldots, U_\gamma^{(k)}, f(T_k))) \leq \frac{h}{2}\sqrt{\gamma(T)|Y||Z|}$

Corollary 1. *Let $m \geq 2n \log q$ and $q \geq 3$ prime. Let $R \leftarrow U(\{-1, 1\}^{m \times k})$ with $k \in poly(n)$. Let $A \sim U(\mathbb{Z}_q^{n \times m})$, $B \sim U(\mathbb{Z}_q^{n \times k})$.*

For any $w \in \mathbb{Z}_q^m$, $(A, AR, R^T w) \overset{s}{\approx} (A, B, R^T w)$

Proof. View $h_A : \{-1, 1\}^m \to \mathbb{Z}_q^n$. $x \to Ax \mod q$ as a universal hash function consider $f(R) = R^T w$ as leaked informations on R and apply the generalized LHL to each column of R. □

Reminder 1. *ABB IBE : $c_0 = u^T s + x + \mu\lfloor q/2 \rfloor \in \mathbb{Z}_q$ $c_1 = \begin{bmatrix} A_0^T \\ A_1^T + G^T \cdot H(ID)^T \end{bmatrix} s + \begin{bmatrix} y \\ R^T \end{bmatrix} \in \mathbb{Z}_q^{m+nk}$*
with

$$\begin{aligned} \mu &\sim U(\mathbb{Z}_q^n) \\ A_0 &\sim U(\mathbb{Z}_q^{n \times m}) \\ A_1 &\sim U(\mathbb{Z}_q^{n \times nk}) \\ x &\sim \chi \\ y &\sim \chi^m \\ R &\sim U(\{-1, 1\}^{n \times nk}) \end{aligned}$$

Secret key : $SK_{id} = e_{ID} \in \mathbb{Z}^{m+nk}$ small such that $[A_0 | A_1 + H(ID) \cdot G] \cdot e_{ID} = u \mod q$

Theorem 1. *The ABB IBE provides set-IND-ID-CPA security under the LWE assumption.*

Proof. Let A an adversary with advantage ε. We build an LWE distinguisher B with advantage $\varepsilon - 2^{-\omega(n)}$
We first consider intermediate experiments Game 0,1,2,3

- <u>Game 0:</u> real SET-IND-ID-CPA experiment
- <u>Game 1:</u> We change the generation of $A_1 \in \mathbb{Z}_q^{n \times nk}$ in MPK. Initially A chooses ID^* the challenge identity. Then, B sets $A_1 : A_0 R^* - H(ID^*)G \in \mathbb{Z}_q^{n \times nk}$ where $R^* \sim U(\{-1, 1\}^{n \times nk}$ is the random matrix used to compute $C^* = (C_0^*, C_1^*)$

  By Corollary 1, $(A_0, A_0 R^*, R^{*T} y) \approx_s (A_0, A_1, R^{*T} y)$ since $A_0 \sim U(\mathbb{Z}_q^{n \times m})$

- <u>Game 2:</u> We change $Keygen(MSK,\cdot)$. For each query $Keyen(MSK, ID)$ with $ID \neq ID^*$ we have

$$A_{id} = [A_0|A_1 + H(ID)G] = [A_0|A_0R^* + (H(ID) - H(ID) \cdot G)$$

  . Here, $(H(ID) - H(ID^*))$ has full rank over $\mathbb{Z}_q$

  So $\Lambda_q^{\perp}((H(ID) - H(ID^*))G) = \Lambda_q^{\perp}(G)$

  So we can use $T_G \in \mathbb{Z}^{nk\times nk}$ and $R^* \in \{-1,1\}^{m\times nk}$ to sample $e_{ID} \in \mathbb{Z}^{m\times nk}$ from $D_{\Lambda_q^n(A_{id}),\sigma}$

  The obtained e_{ID} has the distribution statistically close to that of Game 1 $\implies T_{A_0}$ is no longer used.

- <u>Game 3:</u> Same as ame 2 but we replace (C_0^*, C_1^*) by a random pair in $\mathbb{Z}_q \times \mathbb{Z}_q^{m+nk}$. Then, A has advantage 0, since $Pr(\mu' = \mu) = \frac{1}{2}$

Lemma 2. *Game 2 is indistinguishable from Game3 under LWE assumption*

Let A^{2-3} a distinguisher with advantage ε betweend Game 2 and Game 3. We build a LWE dinstiguisher with advantage ε

Let an LWE instance $(A, V \stackrel{?}{=} A^Ts + e) \in \mathbb{Z}_q^{n\times(m+1)} \times \mathbb{Z}_q^{m+1}$

with $A^T = \begin{bmatrix} A_0^T \\ u^T \end{bmatrix} \in \mathbb{Z}_q^{(m+1)\times n}$ and $V = \begin{bmatrix} v_1 \\ v_0 \end{bmatrix} \stackrel{?}{=} \begin{bmatrix} A_0^T s + y \\ u^T s + x \end{bmatrix}$

Reduction B chooses $R^* \leftarrow U(\{-1,1\}^{m\times nk})$ and $MPK = (A_0, A_1 = A_0R^* - H(ID^*G, u)$

B handles all $keygen(MSK,\cdot)$ queries using T_G and R^* (T_{A_0} is not available)

B constructs $C^* = (C_0^*, C_1^*)$ as $C_0^* = V_0 + \mu\lfloor q/2\rfloor$ with $\mu \leftarrow U(\{0,1\})$, $C_1^* = \begin{bmatrix} v_1 \\ R^{*T}V_1 \end{bmatrix} \in \mathbb{Z}_q^{m+nk}$.

A outputs $\mu' \in \{0,1\}$, If $\mu' = \mu$, B returns 1 (meaning $V = A^Ts + e$). If $\mu' \neq \mu$, B returns 0 (meaning $V \sim U(\mathbb{Z}_q^{m+1})$

$$\text{If} \begin{cases} v_0 = \mu^Ts + x \\ \text{and} \quad v_1 = A_0^T s + y \end{cases} \text{then} \begin{cases} C_0^* = u^Ts + \mu\lfloor q/2\rfloor + x \\ \text{and} \quad C_1^* = \begin{bmatrix} A_0^t s + y \\ R^{*T}A_0^T s + R^{*T} y \end{bmatrix} = \begin{bmatrix} A_0^t s \\ A_1 + G^T \cdot H(ID^*)^T \end{bmatrix} s + \begin{bmatrix} y \\ R^{*T} y \end{bmatrix} \end{cases}$$

Which is a real encryption of μ as in Game 2.

If $\begin{pmatrix} v_1 \\ v_0 \end{pmatrix} \sim U(\mathbb{Z}_q^{m+1})$, then (C_0^*, C_1^*) is statistically uniform, since $(\begin{bmatrix} A_0 \\ V_1^T \end{bmatrix}, \begin{bmatrix} A_0^* \\ V_1^* \end{bmatrix} R)$ is statistically unifomr by the LHL.

$\exists C_1^* = \begin{bmatrix} v_1 \\ R^{*T}v_1 \end{bmatrix} \stackrel{s}{\sim} U(\mathbb{Z}_q^{m+nk})$ even given A_0R^*

$\implies$ A's view is statistically identical to Game 3 □

1.1 Adaptively secure IBE from LWE

View each identity ID as an l-bit string $ID(id_1, \ldots, id_m) \in \{-1,1\}^l$

Encode each $ID \in \{-1,1\}^l$ using $O(l)$ matrices $(A_0, \{A_i\}_{i=1}^l)$ so that $A_{id} = [A_0|G + \sum_{i=1}^{l} id_i \cdot A_i] \in \mathbb{Z}_q^{n\times(m+nk)}$ with $A_0 \sim U(\mathbb{Z}_q^{n\times m})$, $A_1, \ldots, A_l \sim U(\mathbb{Z}_q^{n\times mk})$.

In the proof, set $A_i = A_0 \cdot R_i + h_i \cdot G$ where $R_i \sim U(\{-1,1\}^{m\times nk})$, $h_i \sim U(\mathbb{Z}_q)$

$\implies A_{id} = [A_0|A_0'(\sum_{i=1}^{l} id_ih_i) + (1 + \sum_{i=1}^{l} id_ih_i) \cdot G]$

Define $H(ID) = 1 + \sum_{i=1}^{l} id_i \cdot h_i \mod q$

$\implies$ We need $H(ID^*) = 0$, $H(ID_1), \ldots, H(ID_q) \neq 0$ for all $Keygen(MSK, ID_i)$ queries.

Lemma 3. *Let q a prime such that $0 < Q < q$. For any tuple $(x_0, x_1, ..., x_Q)$ in $(\{-1,1\}^l)^{Q+1}$ of distinct inputs, we have $H(x_0) = 0$, $H(x_1) \neq 0, \ldots, H(x_Q) \neq 0$*

with probability at least $\frac{1}{q}(1 - \frac{Q}{q})$ and at most $\frac{1}{q}$

Proof. Let $(x_0, \ldots, x_q)$ be pairwise distinct over $\{-1,1\}^l$. For each $i \in \{0,1,\ldots,Q\}$, let S_i be the set of $(h_1,\ldots,h_l) \in \mathbb{Z}_q^l$ such that $H(x_i) = 1 + \sum_{i=1}^{l} h_i \cdot x_{i,j} = 0$ we have $|S_i| = q^{l-1}$ Also $|S_0 \cap S_i| \leq q^{l-2}$ for each $i \neq 0$ then $|S| = |S_0| \bigcup_{i=1}^{Q} S_i| \geq |S_0| - \sum_{i=1}^{Q} |S_0 \cap S_i| \geq q^{l-1} - Qq^{l-2}$

Probability is $\frac{|S|}{q^l} \geq \frac{1}{q}(1 - \frac{Q}{q})$ (and smaller than 1/q) □

Remark 1. *Proof uses the encoding of* $ID \in \{-1,1\}^l$*. The reduction can answer all queries for* $ID_1, ..., ID_Q$ *such that* $H(ID_i) \neq 0$ *since* $A_{id} = [A_0 | A_0 \cdot R_{id} + H(ID_i) \cdot G]$ *where* R_{id} *is small and* $H(ID_i) \neq 0$

2 Attribute-Based Encryption for circuits

Until 2012, all ABE were limited to Boolean formulas (equivalently to log-dpeths circuits) using bilinear maps.

In 2013, Gorbmov-Vaihuntanathan-wee gave an ABE for circuits from LWE

In 2014, Boneh et al gave a circuit ABE with short keys (size only depends on circuit depth)

2.1 Idea

Use a connection between ABB and the Gentry-Sahar-Waters FHE

GSW : Let $A \in \mathbb{Z}_q^{n \times m}$ such that secret key is $k \in \mathbb{Z}_q^n$ st $t^T A \mod q$ small

$C_1 = AR_1 + \mu_2 \cdot G \in \mathbb{Z}_q^{n \times nk}$

$C_2 = AR_2 + \mu_2 \cdot G \in \mathbb{Z}_q^{n \times nk}$

with $R_1, R_2 \in \{-1,1\}^{m \times k}$ and $\mu_1, \mu_2 \in \{0,1\}$

Let $G^{-1} : \mathbb{Z}^{n \times \bar{m}} \to \{0,1\}^{nk \times \bar{m}}$ with $k = \lceil \log q \rceil$ a deterministic function such that $G \cdot G^{-1}(M) = M \mod q$ for any $M \in \mathbb{Z}_q^{n \times \bar{m}}$

Recall : $G = I_n \otimes [1, 2, \ldots, 2^{k-1}]$

Then $C_1 \cdot G^{-1}(C_2) = A\big(R_1 \cdot G^{-1}(C2)\big) + \mu_1 \cdot G \cdot G^{-1}(C_2) = A\big(R_1 \cdot G^{-1}(C_2) + R_2\big) + \mu_1\mu_2 \cdot G$

Decrypts to $\mu_1\mu_2$ using secret key $t \in \mathbb{Z}_q^n$

2.2 Fully homomorphic encodings

Let $m = O(n \log q)$ with q prime. Let $G = [I_n \otimes [1, 2, \ldots, 2^{k-1}] | 0^{m-nk}] \in \mathbb{Z}^{n \times m}$ with $k = \lceil \log q \rceil$.

Definition 1. *For any* $A \sim U(\mathbb{Z}_q^{n \times m})$*, an LWE encoding of* $a \in \{0,1\}$ *with refer to a public* $A \in \mathbb{Z}_q^{n \times m}$ *and secret randomness* $s \sim U(\mathbb{Z}_q^n)$ *is a vector* $\Psi_{A,s}(a) = (A + aG)^T s + e \in \mathbb{Z}_q^m$ *with* $e \sim \chi^m$.

Let N use $|\Psi_{A,s}(a)| = ||\Psi_{A,s}(a) - (A + aG)^T||_\infty$

Theorem 2. *Let Matrices* $A, A_1, \ldots, A_l \sim U(\mathbb{Z}_q^{m \times n})$ *Let* $a = a_1, \ldots, a_l \in \{0,1\}^l$ *and LWE encodings* $\Psi_{A_i,s}(a_i) = (A_i + a_i G)^T s + e_i \in \mathbb{Z}_q^m$.

With $e_i \sim \chi^m$ *where* $A_i = AR_i - a_i \cdot G$ *for somme* $R_i \in \mathbb{Z}^{m \times m}$ *with* $||R_i||_\infty \leq r$*. There exist efficient deterministic algorithms (Eval PK, Eval CT, Eval Priv) which, for any Boolean circuit* $C : \{0,1\}^l \to \{0,1\}$ *of depth* d *do the following*

- $EvalPK(C, \{A_i\}_{i=1}^l)$ *outputs* $A_C \in \mathbb{Z}_q^{n \times m}$ *which encodes* C
- $EvalCT(C, \{\Psi_{A_i,s}(a_i)\}_{i=1}^l, a = a_1 \ldots a_l \in \{0,1\}^l)$ *outputs* $\Psi_{A_C,s} \in \mathbb{Z}_q^m$
- $EvalPriv(C, \{A_i = A \cdot R_i - a_i \cdot G\}_{i=1}^l, \{R_i\}_{i=1}^l, \{a_i\}_{i=1}^l)$ *outputs* $R_C \in \mathbb{Z}^{m \times m}$ *of norm* $||R_C||_\infty < O(r^d)$ *such that* $A_C = AR_C - C(a) \cdot G$