Cryptography lecture 20

Denis Rochette

26 November 2019

1 ABE for circuits from LWE

1.1 Fully homomorphic encodings

Theorem (Boneh et al., 2014)**.** *Let $A, A_1, \dots, A_l \sim U(\mathbb{Z}_q^{n\times m})$, $a = a_1 \cdots a_l \in \{0,1\}^l$ and LWE encodings $\psi_i(a_i) = (A_i + a_i \cdot G)^T s + e_i \in \mathbb{Z}_q^m$ with $s \sim U(\mathbb{Z}_q^m)$ and $e_i \sim \chi^m$ s.t. $\|e_i\|_\infty \leq \delta$ for some $\delta > 0$.*
There exist efficient det. algo. (EvalPK, EvalCT, EvalPriv) 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 $A_C \in \mathbb{Z}_q^{n\times m}$*
- *EvalCT($C, \{\psi_i(a_i)\}_{i=1}^l, a = a_1 \cdots a_l$) outputs*
$$\psi_C(C(a)) = (A_C + C(a) \cdot G)^T s + e_c$$
with $e_c \in \mathbb{Z}^m$ s.t. $\|e_c\|_\infty \leq \alpha_C(\lambda)\delta$
- *EvalPriv($C, \{A \cdot R_i - a_i \cdot G\}_{i=1}^l, \{R_i\}_{i=1}^l, a = a_1 \cdots a_l$) outputs $R_C \in \mathbb{Z}^{m\times m}$ of norm $\|R_c\|_\infty \leq O(r^d)$ where $\|R_i\|_\infty \leq r$ and $AR_C - C(a) \cdot G \leftarrow$ EvalPK($c, \{AR_i - a_i \cdot G\}_i$)*

Proof. Let $\psi_1(a_1) = (A_1 + a_1 \cdot G)^T s + e_1$ and $\psi_2(a_2) = (A_2 + a_2 \cdot G)^T s + e_2$ with $a_1, a_2 \in \{0,1\}$ and $e_1, e_2 \in \chi^m$.
EvalCT computes

$$a_1 \cdot \psi_2(a_2) = (a_1 \cdot A_2 + a_1 a_2 \cdot G)^T s + \underbrace{a_1 e_2}_{\text{small}}$$
$$G^{-1}(A_2)^T \cdot \psi_1(a_1) = (A_1 \cdot G^{-1}(A_2) + a_1 \cdot A_2)^T s + \underbrace{G^{-1}(A_2)^T \cdot e_1}_{\text{small}}$$

$$\Rightarrow \psi_\times(a_1 a_2) = a_1 \cdot \psi_2(a_2) - G^{-1}(A_2)^T \cdot \psi_1(a_1)$$
$$\psi_\times(a_1 a_2) = (\underbrace{-A_1 \cdot G^{-1}(A_2)}_{A_\times} + a_1 a_2 \cdot G)^T s + \underbrace{a_1 e_2 - G^{-1}(A_2)^T \cdot e_1}_{e^\times}$$
$$= (A_\times + a_1 a_2 \cdot G)^T s + e^\times$$

$$\begin{aligned}\left\|e^{\times}\right\|_{\infty} &\leq \left\|G^{-1}(A_2)^T \cdot e_1\right\|_{\infty} + a_1 \left\|e_2\right\|_{\infty} \\ &\leq m \left\|e_1\right\|_{\infty} + a_1 \cdot \left\|e_2\right\|_{\infty} \leq (m+1)\delta\end{aligned}$$

EvalCT computes $\psi_{\times}(a_1 a_2) = a_1 \cdot \psi_2(a_2) - G^{-1}(A_2)^T \cdot \psi_1(a_1)$
EvalPK computes $A_{\times} = -A_1 \cdot G^{-1}(A_2)$
EvalPriv computes $R_x = -R_1 \cdot G^{-1}(A_2) + a_1 \cdot R_2 \in [-(m+1), (m+1)]^{m \times m}$,
$A \cdot R_x - a_1 a_2 \cdot G \leftarrow \text{EvalPK}(\times, \{AR_i - a_1 \cdot G\}_{i=1}^2)$

EvalCT can compute an LWE encoding of $a_1 + a_2$ as

$$\begin{aligned}\psi_+(a_1 + a_2) &= \psi_1(a_1) + \psi_2(a_2) \\ &= (A_+ + (a_1 + a_2)G)^T + e^+\end{aligned}$$

with $\left\|e^+\right\|_{\infty} \leq 2\delta$, $A_+ = A_1 + A_2$.

Problem: $a_1 + a_2$ may not be a bit.
$\Rightarrow$ To evaluate a Boolean circuit C over $a = a_1 \cdots a_l \in \{0,1\}^l$, assume $a_0 = 1$ and an LWE encoding $\psi_0(1) = (A_0 + G)^T s + e_0$.
Evaluate C using NAND gates: $\psi_{\text{NAND}}(a_1 \text{NAND} a_2) = \psi_0(1) - \psi_{\times}(a_1 a_2)$.
$\Rightarrow$ we have $\alpha_C(\lambda) = O(m^d)$ s.t. $\left\|e_c\right\|_{\infty} \leq \alpha_C(\lambda)\delta$ □

1.2 The Boneh et al. ABE

Convention: SK_C decrypts any ciphertext CT whose attributes $a \in \{0,1\}^l$ s.t. $C(a) = 0$.

Setup(1^{λ}):

1. Choose $m \in \text{poly}(\lambda)$ and $q = q(n)$ as needed for (EvalPK, EvalCT, EvalPriv) and $m = \Theta(n \log q)$.
   Choose a noise distribution χ s.t. $\left\|e\right\|_{\infty} \leq \delta$ for some $\delta > 0$, for any $e \sim \chi^m$ w.h.p.
   Choose $\sigma = \omega(\sqrt{n \log q \log n})$ a standard deviation.
2. Run $(A, T_A) \leftarrow \text{TrapGen}(1^n, 1^m, \sigma)$ where $A \sim U(\mathbb{Z}_q^{n \times m})$ and $T_A \in \mathbb{Z}^{m \times m}$ is a basis of $\Lambda_q^{\perp}(A)$ with $\left\|\tilde{T_A}\right\| \leq O(\sqrt{n \log q})$.
3. Choose $u \leftarrow U(\mathbb{Z}_q^n)$ and $A_1, \ldots, A_l \leftarrow U(\mathbb{Z}_q^{n \times m})$.
4. Output $MPK = (n, m, \chi, \sigma, A, \{A_i\}_{i=1}^l, u)$ and $MSK = T_A$.

Keygen(MSK, C): given $T_A \in \mathbb{Z}^{m \times m}$ and a circuit $C : \{0,1\}^l \to \{0,1\}$

1. Run $A_C \leftarrow \text{EvalPK}(C, \{A_i\}_{i=1}^l)$ to get $A_C \in Z_q^{n \times m}$
2. Using T_A, sample $v_C \sim D_{\Lambda_q^m([A|A_c]),\sigma}$ to get $v_C \in \mathbb{Z}^{2m}$ Gaussian s.t. $[A|A_C] \cdot v_C = u \mod q$.

3. Return $SK_C = v_C \in \mathbb{Z}^{2m}$ (of norm $\|v_C\| \leq \sigma\sqrt{2m}$ w.h.p).

Encrypt$(MPK, a \in \{0,1\}^l, \mu \in \{0,1\})$:

1. Choose
   $s \leftarrow U(\mathbb{Z}_q^m)$
   $S_1, \ldots, S_l \leftarrow U(\{-1,1\}^{m\times m})$
   $e_0 \leftarrow \chi^m, e_1 \leftarrow \chi$.
2. Compute
   $\psi_0 = A^T s + e_0 \in \mathbb{Z}_q^m$
   $\psi_i = (A_i + a_i G)^T s + S_i^T e_0 \in \mathbb{Z}_q^m, \forall i \in [l]$
   $\psi_u = u^T s + e_1 + \mu\lfloor\frac{q}{2}\rfloor$
3. Output $CT = (a, \psi_0, \ldots, \psi_l, \psi_u) \in \{0,1\}^l \times (\mathbb{Z}_q^m)^l \times \mathbb{Z}_q$.

Decrypt(MPK, SK_C, CT): if $C(a) \neq 0$, return $\perp$, otherwise:

1. Compute $\psi_C = (A_C + C(a)G)^T s + e_C \leftarrow \text{EvalCT}(C, \{\psi_i(a_i)\}_{i=1}^l, a)$, where $A_C \leftarrow \text{EvalPK}(C, \{A_i\}_{i=1}^l)$ and $\|e_C\|_\infty \leq \delta m^d$.
2. View
$$(\psi_0, \psi_C, \psi_u) = \left(A^T s + e_0,\ A_C^T \cdot s + e_c,\ u^T s + e_1 + \mu\lfloor\frac{q}{2}\rfloor\right)$$
   as a dual Regev ciphertext for matrix $[A|A_C] \in \mathbb{Z}_q^{n\times 2m}$.
3. Using $SK_C = v_C \in \mathbb{Z}^{2m}$ s.t. $[A|A_C] \cdot v_C = u \mod q$, compute
$$\mu' = \psi_u - v_C^T \cdot \begin{bmatrix}\psi_0 \\ \psi_C\end{bmatrix}.$$
   If $|\mu' - \lfloor\frac{q}{2}\rfloor| < \frac{q}{4}$, return $\mu = 1$ otherwise $\mu = 0$.

Correctness: Let $\chi \sim D_{\mathbb{Z},\alpha q}$.
For each i,
$$\psi_i = (A_i + a_i G)^T s + \underbrace{e_i}_{S_i^T e_0}$$
for some $e_i \in \mathbb{Z}^m$ s.t. $\|e_i\|_\infty \leq m\alpha q\sqrt{m} = \delta$

$\Rightarrow \psi_C = (A_C + C(a)G)^T s + e_c$ with $\|e_C\|_\infty \leq \alpha q m^{d+1.5}$

$$\begin{aligned}\mu' = \psi_u - v_C^T \begin{bmatrix}\psi_0 \\ \psi_C\end{bmatrix} &= u^T s + e_1 + \mu\left\lfloor\frac{q}{2}\right\rfloor - v_C^T \cdot \left(\begin{bmatrix}A^T \\ A_C^T\end{bmatrix} s + \begin{bmatrix}e_0 \\ e_c\end{bmatrix}\right) \\ &= \mu\left\lfloor\frac{q}{2}\right\rfloor + (e_1 - v_C^T \begin{bmatrix}e_0 \\ e_C\end{bmatrix})\end{aligned}$$

If $v_C \sim D_{\Lambda^u_{[A|A_C]},\sigma}$, we have $\|v_C\| \le \sigma\sqrt{2m}$ w.h.p.
Since $\left\|\begin{bmatrix} e_0 \\ e_C \end{bmatrix}\right\| \le \sqrt{(\alpha q\sqrt{m})^2 + (\alpha q m^{d+2})^2} < \alpha q\sqrt{2}m^{d+2}$
$\Rightarrow \left\|\mu' - \mu\lfloor\frac{q}{2}\rfloor\right\| < 2\sigma\alpha q m^{d+3} < \frac{q}{4}$
$\Rightarrow \alpha < \frac{1}{8\sigma m^{d+4}}$ for correctness.

$$\sigma = \underbrace{\left\|\tilde{T_A}\right\|}_{O(\sqrt{n\log q})} \quad \omega(\sqrt{\log m})$$

e.g. $\sigma = O(n)$
$\Rightarrow \sigma < \frac{1}{8m^{d+4}} \Rightarrow \frac{q}{|\text{noise}|} \Rightarrow \frac{\Omega(m^d)}{\Omega(2^{\text{Poly}(\lambda)})}$
Best algorithm for $GapSVP_\gamma$ takes time $2^{\tilde{\Omega}\left(\frac{m}{\log\gamma}\right)}$
$\Rightarrow$ We need a large $n = \text{Poly}(\lambda)$ for the hardness of LWE.

Theorem. *The scheme provides selective CPA security under the LWE assumption.*

Proof. Consider a sequence of games

Game 0: Real selective CPA experiment.

Game 1: Change the generation of $\{A_i\}_{i=1}^l$ in MPK.
Initially, $\mathcal{A}$ choose $a^* = (a_1^*, \ldots, a_l^*) \in \{0,1\}^l$.
For each $i \in \{1, \ldots, l\}$, challenger chooses $S_i^* \leftarrow U(\{-1,1\}^{m\times n})$ and computes $A_i = AS^* - a_i^* G$.
In the challenge phase, challenger computes

$$\begin{aligned}
\psi_0 &= A^T s + e_0 \\
\psi_i &= (A_i + a_i^* G)^T s + {S_i^*}^T e_0 \\
&= {S_i^*}^T \underbrace{(A^T s + e_0)}_{\psi_0}, \forall i \in \{1, \ldots, l\} \\
\psi_u &= u^T s + e_1 + \mu \left\lfloor \frac{q}{2} \right\rfloor
\end{aligned}$$

By the generalized LHL, for each $i \in \{1, \ldots, l\}$

$$(A, AS_i^*, e_0^T S_i^*) \approx_s (A, U(\mathbb{Z}_q^{n\times m}), e_0^T S_i^*)$$

$\Rightarrow$ Game 0 and Game 1 are statistically indistinguishable.

Game 2: Change the Keygen(MSK, $\cdot$) oracle. When $\mathcal{A}$ queries SK_C for a circuit $C : \{0,1\}^l \to \{0,1\}$ s.t. $C(a^*) \neq 0$, challenger computes

$$\text{EvalPriv}(c, \{A_i = AS_i^* - a_i^* G\}_{i=1}^l, \{S_i^*\}_{i=1}^l, a^*)$$

to get $S_C \in \mathbb{Z}^{m\times n}$ s.t.$\|S_C\|_\infty \leq O(m^d)$ and $A_C = AS_C - C(a^*)G$, where $A_C \leftarrow \text{EvalPK}(C, \{A_i\}_{i=1}^l)$.
We have

$$[A|A_C] = [A|AS_C - C(a^*)G]$$

so that T_G and S_C allow sampling from $D_{\Lambda_q^\perp([A|A_C]),\sigma}$.

Challenger uses T_G and S_C to sample $v_C \in \mathbb{Z}^{2m}$ from the distrib. $D_{\Lambda_q^u([A|A_c]),\sigma}$ s.t. $[A|A_C]\cdot v_C = u \mod q$ and ouput $SK_C = v_C$ whose distribution is statistically close to that of Game 1.

Game 3: Same as Game 2 but we replace $CT^* = (\psi_0^*, \ldots, \psi_l^*, \psi_u^*)$ by random elements over $\mathbb{Z}_q$

In Game 3, $\Pr[\mu' = \mu] = \frac{1}{2}$ since CT^* is statistically independent of μ. Hence, $\text{Adv}(\mathcal{A}) = 0$

Lemma. *Under the LWE assumption, Game 3 is indistinguishable from Game 2.*

Proof. Let a distinguisher $\mathcal{A}$ with adv ϵ between the games. We build an LWE distinguisher with adv ϵ.
Distinguisher $\mathcal{B}$ inputs

$$\left(\bar{A}^T = \left[\frac{A^T}{u^T}\right] \in \mathbb{Z}_q^{(m+1)\times n},\ b = \left[\frac{b_0}{b_1}\right] \stackrel{?}{=} \bar{A}^T s + e \in \mathbb{Z}_q^{m+1}\right)$$

and decides if $b = \left[\frac{b_0}{b_1}\right] = (\left[\frac{A^T}{u^T}\right] s + \left[\frac{e_0}{e_1}\right])$ or $V \sim U(\mathbb{Z}_q^{m+1})$.

$\mathcal{A}$ initially chooses $a^* = (a_1^*, \ldots, a_l^*) \in \{0,1\}^l$.
$\mathcal{B}$ chooses $S_1^*, \ldots, S_l^* \leftarrow U(\{-1,1\}^{m\times n})$ and sets $A_i = AS_i^* - a_i^* G, \forall i$.
$\mathcal{B}$ gives $\mathcal{A}$: $\text{MPK} = (A, \{A_i\}_{i=1}^l, u)$.
At each Keygen(MSK, c) query, we have $C(a^*) \neq 0$.
$\mathcal{B}$ computes $S_C \leftarrow \text{EvalPriv}(C, \{A_i\}_{i=1}^l, \{S_i^*\}_{i=1}^l, a^*)$ to get S_C s.t.

$$AS_C + C(a^*)G \ \leftarrow\ \text{EvalPK}(c, \{A_i\}_{i=1}^l)$$

$\mathcal{B}$ uses S_C and T_G to sample $SK_C = v_C$ Gaussian s.t. $[A|A_C]\cdot v_C = u \mod q$ with distribution $D_{\Lambda_q^u([A|A_C]),\sigma}$.

Challenge: $\mathcal{B}$ chooses $\mu \leftarrow U(\{0,1\})$ and sets

$$\begin{aligned}
\psi_0^* &= b_0 \stackrel{?}{=} A^T s + e_0 \\
\psi_i^* &= S_i^{*T} \cdot b_0 \stackrel{?}{=} S_i^{*T} \cdot (A^T s + e_0) = (A_i + a_i^* G)^T s + S_i^{*T} \cdot e_0 \\
\psi_u^* &= b_1 + \mu \left\lfloor \frac{q}{2} \right\rfloor = u^T s + e_1 + \mu \left\lfloor \frac{q}{2} \right\rfloor
\end{aligned}$$

Output: $\mathcal{A}$ outputs $\mu' \in \{0,1\}$. If $\mu' = \mu, \mathcal{B}$ returns 1 otherwise 0.

If $b = \bar{A}^T s + e$, then $CT^* = (\psi_0^*, \ldots, \psi_l^*, \psi_u^*)$ is distributed as in Game 2.
If $b \sim U(\mathbb{Z}_q^{m+1})$, then CT^* is statistically uniform over $\mathbb{Z}_q$ by the LHL

□