Advanced Cryptographic Primitives

Damien Stehlé and Benoît Libert
lecture notes taken by Julien Le Maire

M2IF

Chapter 1

Encryption and IBE from LWE

1.1 Probabilistic interlude

Let D_1 and D_2 be two distributions on a countable domain X.
The *statistical distance* (or l_1 distance or total variation distance) between D_1 and D_2 is:

$$\Delta(D_1, D_2) := \frac{1}{2} \sum_{x \in X} |D_1(x) - D_2(x)|$$

Properties:

- It's a distance (it is positive, symmetric and satistifies the triangular inequality)
- For all (randomized) function f, we have:

$$\Delta(f(D_1), f(D_2)) \leq \Delta(D_1, D_2)$$

  As a consequence, for any randomized algorithm $\mathcal{A} : X \to \{0, 1\}$,
  if we define:

$$\mathrm{Adv}_{\mathcal{A}}(D_1, D_2) := \left| \Pr_{x \leftarrow D_1}[\mathcal{A}(x) = 1] - \Pr_{x \leftarrow D_2}[\mathcal{A}(x) = 1] \right|$$

  Then we have:

$$\mathrm{Adv}_{\mathcal{A}}(D_1, D_2) \leq \Delta(D_1, D_2)$$

- For any distributions $D_{1,1}, D_{1,2}, D_{2,1}, D_{2,2}$ with $D_{1,1}$ independent from $D_{1,2}$ and $D_{2,1}$ independent from $D_{2,2}$, we have:

$$\Delta((D_{1,1}, D_{1,2}), (D_{2,1}, D_{2,2})) \leq \Delta(D_{1,1}, D_{2,1}) + \Delta(D_{1,2}, D_{2,2})$$

- For any event $E \subseteq X$:

$$D_1(E) \geq D_2(E) - \Delta(D_1, D_2) \quad \text{where } D(E) := \Pr_{x \leftarrow D}[x \in E]$$

Leftover Hash Lemma (LHL):
Let $h : S \times X \to Y$ (where S, X, Y are finite sets).

The mapping h is said to be a *2-universal* familly of hash functions if:

$$\forall x \neq x' \in X, \Pr_{s \leftarrow U_S} \left[h(s,x) = h(s,x') \right] = \frac{1}{|Y|}$$

Let D be a distribution over X such that $\max_{x \in X} D(x) \leq 2^{-H}$ for some constant H called the *min entropy* (2^{-H} is called the *guessing probability*). Then, given $s \in S$, the value of $h(s, D)$ is close to uniform:

$$\Delta[(s, h(s,x)), (s,y)] \leq \sqrt{\frac{\mathrm{Card}(Y)}{2^H}} \quad \text{where } (s,x,y) \leftarrow (U(S), D, U(Y))$$

Example: $h(A, r) := r^\top A$
Let q be a prime number, $A \leftarrow U(\mathbb{Z}_q^{m \times n})$ and $D := U(\{0,1\}^m)$ the distribution of r.
Given $r \neq r'$, we have:

$$\begin{aligned}
\Pr_A \left[h(A,r) = h(A,r') \right] &= \Pr_A \left[r^\top A \equiv r'^\top A \ \ [q] \right] \\
&= \Pr_A \left[(r - r')^\top A \equiv (0)_{1..n} \ \ [q] \right] \\
&= \left(\Pr_a \left[(r - r')^\top a \equiv 0 \ \ [q] \right] \right)^n \\
&= \left(\Pr_a \left[(r - r')^\top a_{i_0} \equiv _ \ \ [q] \right] \right)^n \text{ where } i_0 \text{ is such that } r_{i_0} \neq r'_{i_0} \\
&= \left(\frac{1}{q} \right)^n
\end{aligned}$$

Thus, h is *2-universal*, and we can apply the leftover hash lemma (with $\max_r D(r) = 2^{-m}$):

$$\Delta((A, r^\top A), (A, u)) \leq \sqrt{\frac{q^n}{2^m}} \quad \text{where } (r, A, u) \leftarrow (U(\{0,1\}^m), U(\mathbb{Z}_q^{mn}), U(\mathbb{Z}_q^n))$$

Knowing A, the vector $r^\top A$ can be considered uniform when Δ is small, so when $m \gg n \log_2 q$.
For example, if $m = 3n \log_2 q$, then $\Delta \leq q^{-n}$.

1.2 Encrypting from LWE

Encryption Scheme: This is the *dual-Regev* encryption, a scheme easier to extend to schemes with more advanced functionalities than the version introduced by Regev with LWE. It was first introduced in [1].

KeyGen:

- sk: $r \leftarrow U(\{0,1\}^m)$
- PK: $u \in \mathbb{Z}_q^n$ such that $u^\top \equiv r^\top A \ \ [q]$
  Remark: $A \leftarrow U(\mathbb{Z}_q^{nm})$ is a matrix shared by everyone using the scheme.

Enc$(PK, M \in \{0,1\})$*:*

- $s \leftarrow U(\mathbb{Z}_q^n)$
- $e \leftarrow (D_{\mathbb{Z},\alpha q})^m$
- $e' \leftarrow D_{\mathbb{Z},\alpha q}$
- Return (c_1, c_2) with:

$$\begin{pmatrix} c_1 \\ \hline c_2 \end{pmatrix} = \begin{pmatrix} A \\ \hline u^\top \end{pmatrix} \times \begin{pmatrix} s \end{pmatrix} + \begin{pmatrix} e \\ \hline e' \end{pmatrix} + \begin{pmatrix} 0 \\ \hline \lfloor \frac{q}{2} \rfloor M \end{pmatrix}$$

Dec$(sk = r, (c_1, c_2))$*:*

- compute $c_2 - r^\top c_1 \ \ [q]$
- if this is $> \frac{q}{4}$ return $M = 1$, otherwise return $M = 0$

Correctness: We have the following:

$$\begin{aligned} c_2 - r^\top \times c_1 &= (u^\top \times s + e' + \lfloor \frac{q}{2} \rfloor M) - r^\top \times (A \times s + e) \\ &= r^\top \times A \times s + e' + \lfloor \frac{q}{2} \rfloor M - r^\top \times A \times s - r^\top \times e \\ &= \lfloor \frac{q}{2} \rfloor M + (e' - r^\top \times e) \ \ [q] \end{aligned}$$

Thus, the decryption error is:

$$\begin{aligned} \left| e' - r^\top e \right| &\leq \left| e' \right| + \|e\| \\ &\leq \alpha q \sqrt{m} + \sqrt{m}(\sqrt{m}.\alpha q \sqrt{m}) \quad \text{with proba } \geq 1 - 2^{-\Omega(m)} \\ &\leq 2\alpha q m^{\frac{3}{2}} \end{aligned}$$

If $\alpha \leq \frac{1}{16m^{\frac{3}{2}}}$ then this is $\leq \frac{q}{8}$. And:

$$M = 0 \Rightarrow \left| c_2 - r^\top \times c_1 \right| \leq \frac{q}{4}$$

$$M = 1 \Rightarrow \left| c_2 - r^\top \times c_1 \right| > \frac{q}{4}$$

Remarks:

- The correctness is only probabilistic. This can be avoided by cutting the tail of $D_{\mathbb{Z},\alpha q}$, or by choosing the parameters to have a unrealistic probability of failure.
- $2\alpha q m^{\frac{3}{2}}$ is very far from a tight bound.
- Design strategy: compute a bound on the magnitude of error in the decryption, then set α such that the correctness is garanteed. Then set all other parameters such that $\text{LWE}_{n,\alpha q}$ is hard.

Security: proving an IND-CPA security

Goal: The adversary $\mathcal{A}$ is given pk, and an encryption of either 0 or 1. The adversary $\mathcal{A}$ has to distinguish $(A, u, \mathrm{Enc}(0))$ and $(A, u, \mathrm{Enc}(1))$

Game 0 Real IND-CPA game

Game 1 Same game, except that we sample u uniformly

$$\Delta((A, r^\top A), (A, u)) \leq q^{-n} \quad \text{if } m \geq 3n \log q$$

$$|\mathrm{Adv}_{\mathcal{A}}(\text{Game } 0) - \mathrm{Adv}_{\mathcal{A}}(\text{Game } 1)| \leq 2q^{-n}$$

Game 2 Same as 1, but we remplace $As + e$ and $u^\top s + e'$ by something uniform mod q in *Enc*. If $\mathcal{A}$ sees a difference between Game 1 and Game 2, it can break $\mathrm{LWE}_{n,\alpha q}$: we can construct $\mathcal{B}$ such that:

$$\mathrm{Adv}_{\mathcal{A}}(\text{Game } 2) \geq \mathrm{Adv}_{\mathcal{A}}(\text{Game } 1) - \mathrm{Adv}_{\mathcal{B}}(\text{Breaking LWE})$$

Setting parameters: To have a scheme 2^λ secure, choose the parameters as follow:

$$n = \Theta(\lambda) \qquad \alpha = \frac{1}{16m^{\frac{3}{2}}}$$
$$\alpha q = 2m^{\frac{1}{2}} \qquad m \geq 3n \log_2 q$$

With thoses parameters, the cost of the scheme is:

PK length: $O(\lambda \log \lambda)$ time to encrypt one bit: $mn \log_2^2 q = \tilde{O}(\lambda^2)$
sk length: $O(\lambda \log \lambda)$ decryption cost: $\tilde{O}(\lambda)$
ciphertext size: $\tilde{O}(\lambda)$

Encrypting several bits at once:
We can modify the scheme to use several distincts u's to encrypt several bits:

$$\begin{pmatrix} c_1 \\ \hline c_2 \\ c_3 \\ \cdots \\ c_{t+1} \end{pmatrix} = \begin{pmatrix} A \\ \hline u_1^\top \\ u_2^\top \\ \cdots \\ u_t^\top \end{pmatrix} \times \begin{pmatrix} s \end{pmatrix} + \begin{pmatrix} e \\ \hline e_1 \\ e_2 \\ \cdots \\ e_t \end{pmatrix} + \begin{pmatrix} 0 \\ \hline \lfloor \frac{q}{2} \rfloor M_1 \\ \lfloor \frac{q}{2} \rfloor M_2 \\ \cdots \\ \lfloor \frac{q}{2} \rfloor M_t \end{pmatrix}$$

Choosing t is a tradeof between the size of the keys and the number of bits encrypted at once: The size of the keys is multiplied by t, and the ciphertext now encrypt t bits using $\lambda + t$ bits.

1.3 IBE from LWE in the Random Oracle Model

Lemma 1: [2] [3] [4]
There exists a probabilistic polynomial time algorithm `GenBasis` that takes n, m, q with $m \geq \Omega(n \log n)$ as inputs, and returns $(T, A) \in (\mathbb{Z}_q^{m \times n}, \mathbb{Z}_q^{m \times n})$ such that :

- $\Delta(A, U(\mathbb{Z}_q^{mn})) \leq 2^{-n}$
- $\max\|t_i\| = O(n \log n)$ where t_i is the i-th row of T
- the $(t_i)_{1 \leq i \leq n}$ form a basis of $\Lambda^{\perp}(A) = \left\{x \in \mathbb{Z}^m, x^{\top} A \equiv 0 \ \ [q]\right\}$

Remark 1: This can be used to solve LWE, as distinguishing $(A, A \times s + e)$ and (A, u) become easy just by multiplying by T:

- $T \times (A \times s + e) = T \times e$ is small with high probability.
- $T \times u$ is uniform as T is non-singular.

Remark 2: Given just A, it is hard to find such a T.

Lemma 2: [1] [5]
Let L be a n-dimentional lattice in $\mathbb{Z}^n$. Let $(b_i)_{1 \leq i \leq n}$ be a basis of L, and let $s \geq \Omega\left(\max\|b_i\|\sqrt{\log n}\right)$. There exists a probabilistic polynomial time algorithm *GPVSample* that samples from a distribution $D_{L,s,c}$ such that:

$$D_{L,s,c}(b) \sim \exp\left(-\pi \frac{\|b - c\|^2}{s^2}\right)$$

For such an s: $\max_{b \in L} D_{L,s,c}(b) \leq 2^{-n}$ and $\Pr_{b \in D_{L,s,c}}(\|b - c\| \geq s\sqrt{n}) \leq 2^{-n}$

Properties:

- $\Pr_{x \leftarrow D_{L,s,c}}\left[\|x - c\| \geq \sqrt{n}s\right] \leq 2^{-n}$
- $\max_{x \in L} D(x) \leq 2^{-n}$ assuming $s \geq \max\|b_i\|\Omega\left(\sqrt{\log n}\right)$

Bibliography

[1] Craig Gentry and Chris Peikert and Vinod Vaikuntanathan. *Trapdoors for Hard Lattices, and New Cryptographic Constructions* in STOC 2008.

[2] Miklós Ajtai. *Generating hard instances of the short basis problem* in ICAL '99 Proceedings of the 26th International Colloquium on Automata, Languages and Programming

[3] Joël Alwen and Chris Peikert. *Generating Shorter Bases for Hard Random Lattices* in Theory of Computing Systems, April 2011, Volume 48, Issue 3, pp 535-553

[4] Daniele Micciancio and Chris Peikert. *Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller* in Cryptology ePrint Archive, Report 2011/501, 2011

[5] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev and Damien Stehlé. *Classical hardness of learning with errors* in the proceedings of STOC 2013