Encrypting with lattices

CR15 / Alain Passelègue

2019-2020

Contents

1 Basics on probability

1.1 Statistical distance

For a distribution $\mathbb{D}$ over a domain X, denote $D(x) = Pr[y = x | y \leftarrow D]$

Definition 1. *(Statistical distance) : Let D_1, D_2 over a domain X the statistical distance between D_1 and D_2 is defined by*

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

We have the following properties for Δ :

- Δ is a distance
- $\forall$ randomized $f : X \leftarrow Y$, we have

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

In particular, for any randomized $f : X \to \{0, 1\}$:

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

- if we have 4 distributions $D_{1,1}$, $D_{1,2}$, $D_{2,1}$, $D_{2,2}$ such that $D_{1,1}$ is independant of $D_{1,2}$ and $D_{2,1}$ is independant of $D_{2,2}$, then

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

1.2 Gaussian distribution

For lattice-based cryptography, in general we use $e \sim D_{0,\alpha q}$ where

$$D_{\mu,\sigma}(x) \sim \exp(-\pi \cdot \frac{|x-\mu|^2}{\sigma^2})$$

Properties :

- sampling from $D_{\mu,\sigma}$ is efficiant (quasi-linear in output size)
- if $\sigma > 1$, $\forall t > 0$:

$$\mathbb{P}_{x \leftarrow D_{\mu,\sigma}} \left[|x-\mu| \geq t \cdot \sigma \right] \leq 4 \cdot \exp(-\pi \cdot t^2)$$

In general for LWE, we use $D_{0,\alpha q}$ with $\alpha \simeq \frac{1}{poly(n)}$ with $n =$ dimension of secret s.

1.3 Leftover Hash Lemma

Definition 2. *(2-universal hash function) Let $h : S \times X \to Y$ be a family of hash functions. We say that h is 2-universal if*

$$\forall x \neq x', \mathbb{P}_{s \xleftarrow{\$} S} \left[h(s,x) = h(s,x') \right] = \frac{1}{|Y|}$$

Lemma 1. *(Leftover Hash Lemma) Let D be a distribution over X such that $max_{x \in supp(D)} D(x) \leq 2^{-H}$ and let $h : S \times X \to Y$ denote a 2-universal hash function, then*

$$\Delta((s, h(s,x)), (s,y)) \leq \sqrt{\frac{|Y|}{2^H}}$$

where $s \leftarrow \mathscr{U}(S)$, $x \to D$ and $y \to \mathscr{U}(Y)$

Remark. *H is called the min-entropy of D, denoted $H_\infty(D)$. 2^{-H} is called the "guessing probability".*

Exemple 1. *We take the function*

$$\begin{array}{rccc} h & : & \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m & \longrightarrow & \mathbb{Z}_q^n \\ & & (A, r) & \longmapsto & {}^t rA \end{array}$$

In this example, $S = \mathbb{Z}_q^{m \times n}$, $X = \mathbb{Z}_q^m$, $Y = \mathbb{Z}_q^n$ and $D = \mathscr{U}(\{0,1\}^n)$.

Lemma 2. *h is 2-universal, i.e. $\forall r \neq r', \mathbb{P}_{A \leftarrow \mathscr{U}(Z_q^{m \times n})}[{}^t rA = {}^t r'A] = \frac{1}{q^n}$.*

Proof.

$$\begin{aligned}
\mathbb{P}_{A\xleftarrow{\$}Z_q^{m\times n}}\left[{}^trA = {}^tr'A\right] &= \mathbb{P}_{A\xleftarrow{\$}Z_q^{m\times n}}\left[{}^t(r-r')\cdot A \equiv 0^n\ [q]\right] \\
&= \left(P_{a\xleftarrow{\$}Z_q^{m\times n}}\left[{}^t(r-r')\cdot a \equiv 0\ [q]\right]\right)^n \\
&= \left(P_{a\xleftarrow{\$}Z_q^{m}}\left[{}^t(r-r')_j\cdot a_j = -\left(\sum_{i\neq j}(r-r')_i\cdot a_i\ [q]\right)\right]\right)^n \\
&\qquad\qquad \textit{where } r_j \neq r'_j \\
&= \left(\frac{1}{q}\right)^n
\end{aligned}$$

□

$D : \mathscr{U}(\{0,1\}^n)$, H from LHL statement is $\big(H_\infty(D) = m\big)$,
we have $\Delta((A, h(A,r)),(A,y)) \leq \sqrt{\frac{q^n}{2^m}}$
If $m \geq 3n\cdot\log_2 q$, we have $\Delta \leq \frac{1}{q_n}$

2 Public-key encryption from LWE

The first PKE scheme from LWE is by Regev and is usually called "primal Regev encryption". The scheme we do today is usually called "dual Regev encryption" and is based on **GPV08** [Gentry, Peiket, Vaikuntanathan]. Main raison : advanced encryption schemes look libe Dual Regev.

2.1 Construction

- $\mathrm{Gen}(1^\lambda)$:

  $r \xleftarrow{\$} \{0,1\}^m,\ A \xleftarrow{\$} \mathbb{Z}_q^{m\times n},\ {}^tu = {}^tr\cdot A$ // h(A, x) from previous example
  $(sk, pk) = (r, (A, {}^tu))$

- $\mathrm{Enc}(pk, M \in \{0,1\})$:

  $s \xleftarrow{\$} \mathbb{Z}_q^n,\ e \leftarrow (D_0, \alpha q)^m,\ e' \leftarrow (D_0, \alpha q)$
  return $ct = (ct_1, ct_2)$ where
  $$\frac{ct_1}{ct_2} = \begin{pmatrix} A \\ {}^tu \end{pmatrix}\cdot s + \begin{pmatrix} e \\ e' \end{pmatrix} + \begin{pmatrix} 0 \\ \lfloor q/2 \rfloor \cdot M \end{pmatrix}$$

- $\mathrm{Dec}(sk, ct)$: compute $ct_2 - {}^t r \cdot ct_1$

$$\begin{aligned} & \left({}^t u \cdot s + e' + \lfloor q/2 \rfloor\right) - {}^t r \cdot (A \cdot s + e) \\ = \ & \left({}^t u \cdot s + e' + \lfloor q/2 \rfloor\right) - \left({}^t u \cdot s + {}^t r \cdot e\right) \\ = \ & \lfloor q/2 \rfloor \cdot M + {}^t r \cdot e + e' \end{aligned}$$

return 0 if $\left|ct_2 - {}^t r \cdot ct_1\right| \leq q/4$ and 1 otherwise

2.2 Correctness

$$ct_2 - {}^t r \cdot ct_1 = \lfloor q/2 \rfloor \cdot M + {}^t r \cdot e + e'$$

Is $\left|e' + {}^t r \cdot e\right|$ small ?

$$\begin{aligned} \left|e' + {}^t r \cdot e\right| &\leq \left|e'\right| + \|e\| \\ &\leq \alpha q \cdot \sqrt{m} + m \cdot \alpha q \cdot \sqrt{m} \qquad \text{with probability } 1 - e^{-\pi(m)} \\ &\leq 2 \cdot \alpha q \cdot m^{3/2} \end{aligned}$$

Remark. *Over $D_{0,\alpha q}$, if $\alpha q > 1$ we have $\mathbb{P}_{e \leftarrow D_{0,\alpha q}}\left[|e| \geq t \cdot \alpha q\right] \leq 4 \cdot \exp\left(-\pi t^2\right)$ $(t = \sqrt{m})$.*

$$2 \cdot \alpha q \cdot m^{3/2} < q/4 \Leftrightarrow \alpha < \frac{1}{8m^{3/2}} \Rightarrow \text{with such } \alpha, \text{ we loose } \left|e' + {}^t r \cdot e\right| \leq \frac{q}{4}$$

Remark. *Correctness is probabilistic, several tricks exist to overcome this.*

2.3 Security (IND-CPA)

$\mathscr{A}$ knows pk and need to distinguish $\mathrm{Enc}(pk, 0)$ from $\mathrm{Enc}(pk, 1)$.

$$pk = (A, {}^t u = {}^t r A),\ sk = r,\ ct^* = \begin{pmatrix} A \\ {}^t u \end{pmatrix} \cdot s + \begin{pmatrix} e \\ e' \end{pmatrix} + \begin{pmatrix} 0 \\ \lfloor q/2 \rfloor \cdot M \end{pmatrix}$$

Game 0 $(M = 0)$
Hyb_1 : same as Game 0 except that u is now uniform over $\mathbb{Z}_q^n$.

$$\Delta\left(Game_0, Hyb_1\right) \leq \frac{1}{q^n}$$

This is exactly LHL with $h : (A, r) \to \left({}^t r \cdot A\right)$.
If $m \geq 3n \cdot \log_2 q$, we have $\Delta \leq \frac{1}{q^n}$ and so

$$\mathrm{Adv}^{\mathscr{A}}\left(Game_0 - Hyb_1\right) \leq \Delta \leq \frac{1}{q^n}$$

This means that

$$ct * \begin{pmatrix} A \\ b \end{pmatrix} \cdot s + \begin{pmatrix} e \\ e' \end{pmatrix} + \begin{pmatrix} 0 \\ \lfloor q/2 \rfloor \cdot M \end{pmatrix} \text{ with } b \xleftarrow{\$} \mathbb{Z}_q^n$$

Hyb_2 : replace $\begin{pmatrix} A \\ b \end{pmatrix} \cdot s + \begin{pmatrix} e \\ e' \end{pmatrix}$ by uniform vector.

Game 1 ($M = 1$)

Lemma 3. *$Hyb_1 = Hyb_2$ under LWE.*

Proof. B gets a LWE instance.

$$\left(\begin{pmatrix} A \\ b \end{pmatrix}, \begin{pmatrix} A \\ b \end{pmatrix} \cdot s + \begin{pmatrix} e \\ e' \end{pmatrix} \right) \text{ or } \left(\begin{pmatrix} A \\ b \end{pmatrix}, u \right) \text{ with } \begin{pmatrix} A \\ b \end{pmatrix} \xleftarrow{\$} \mathbb{Z}_q^{(m+1)\times n}$$

B sets $pk = (A, b)$ and $ct^* = Z + \begin{pmatrix} 0 \\ \lfloor q/2 \rfloor \cdot M \end{pmatrix}$ and $\begin{pmatrix} e \\ e' \end{pmatrix} \leftarrow (D_0, \alpha q)^{n+1}$ and $u \xleftarrow{\$} \mathbb{Z}_q^{n+1}$ □

Conclusion : $\mathrm{Adv}^{\text{IND-CPA}}(A) \leq 2 \cdot \frac{1}{q^n} + 2 \cdot \mathrm{Adv}^{\text{LWE}}(b)$

2.4 Multibit variant (l-bit variant)

$$pk = \left(A, {}^t u_1 = {}^t r_1 \cdot A, \ldots, {}^t u_l = {}^t r_l \cdot A\right), \; sk = (r_1, \ldots, r_l), \; ct^* = \begin{pmatrix} A \\ {}^t u_1 \\ \vdots \\ {}^t u_l \end{pmatrix} \cdot s + \begin{pmatrix} e \\ e_1 \\ \vdots \\ e_l \end{pmatrix} + \begin{pmatrix} 0 \\ \lfloor q/2 \rfloor \cdot M_1 \\ \vdots \\ \lfloor q/2 \rfloor \cdot M_l \end{pmatrix}$$

Play with m so that $\sqrt{\frac{q^n}{ln}} \leq q^{-n}$