Advanced Crypto - Class 5

Julien du Crest

October 2019

Post-Quantum crypto motivations: Beginning with the seminal paper of Shor (94') factoring integers in probabilistic poly-time on a quantum computer, the result was expanded to solving DLOG on any group structure in $O(n^2)$ probabilistic time with a quantum computer, thus making most of todays crypto standard algorithms useless in the quantum world.
This motivates the study of post-quantum assumptions, i.e. problems that are thought to be difficult even in the quantum setting.

Possible candidates:

- Codes (e.g., McEliece) : good for assymetric-encryption.
- Multivariate polynomials : good for signatures.
- Isogenies : promising but still at its premices.
- **Lattices : the Swiss-army knife of Post-Quantum crypto**.

In particular, we would like our crypto system to allow for **fine grained decryption policies**, i.e. allowing for more advanced crypto schemes (e.g Attribute-Based Encryption, Predicate Encryption, Fully Homomorphic Encryption, Functional Encryption).

1 Linear systems and SIS problem

Definition 1. ***SIS(n,m,B,q)***
Given $A \in \mathbb{Z}_q^{n \times m}$ and $b \in \mathbb{Z}_q^n$, finding non-null $e \in [\![-B, B]\!]^m$ s.t

$\boxed{\quad A \quad} \times \boxed{e} = \boxed{b}$ *is hard.*

Remark: Finding **any** e satisfying the above is an easy task using gauss elimination. Restricting it to short vectors makes it hard so the choice of B is crucial.

3 cases are seen in practice :

- Homogeneous regime ($b = 0^n$) is the most common.
- Random regime ($b \xleftarrow{\$} \mathbb{Z}_q^n$) a.k.a. SIS regime.
- Planted regime ($b = Ae$ for previously chosen e) a.k.a. LWE regime.

The is a lot to say about lattices assumptions and many reductions from one to another... to be done another time (or follow cryptanalysis with Damien Stehlé).

1.1 Some reductions

In the following, $A \xrightarrow{red.} B$ means that "A reduces to B" or equivalently that "solving B leads to an algorithm solving A".

Lemma 1. *SIS(n,m,B,q) random* $\xrightarrow{red.}$ *SIS(n,m+1,B,q) homogeneous*

Proof. Given $A \in \mathbb{Z}_q^{n\times m}$,$b \in \mathbb{Z}_q^n$ and $\mathscr{B}$ an algorithm that solves *SIS(n,m+1,B,q) homogenous* with a non-negligible probability.
Let's define $B = [A \mid b] \in \mathbb{Z}_q^{n\times(m+1)}$ and let e denote the result of $\mathscr{B}(B)$.
If $e_m = 1$, the vector $e' = \begin{bmatrix} e_1 \\ e_2 \\ ... \\ e_{m-1} \end{bmatrix}$ is a solution of the *SIS(n,m,B,q) random* instance (A, b).
From this derives an algorithm $\mathscr{A}$ solving *SIS(n,m,B,q) random* with non-negligible probability by making a polynomial number of calls to oracle $\mathscr{B}$ until the property $e_m = 1$ is satisfied.

PS: There remain discussions to be had to ensure that the distribution of e looks uniformly random elementwise to ensure that $\mathbb{P}(e_m = 1) = \frac{1}{B} > neg.$ and thus that a polynomial number of calls to $\mathscr{B}$ will give a non-negligible probability of success. □

Lemma 2. *SIS(n,m,B,q) homogeneous* $\xrightarrow{red.}$ *SIS(n,m,B/2,q) random*

Proof. Given $A \in \mathbb{Z}_q^{n\times m}$,$b \in \mathbb{Z}_q^n$ and $\mathscr{B}$ an algorithm that solves *SIS(n,m,B/2,q) random* with a non-negligible probability.
The algorithm $\mathscr{A}$ that picks $b \in \mathbb{Z}_q^n$ at random, then solve the problem twice and outputs $e_1 - e_2$ solves *SIS(n,m,B,q) homogeneous* with non-negligible probability.

□

Definition 2. *SearchLWE(n,m,q,$\mathcal{X}$):*
Let $A \in \mathbb{Z}_q^{n\times m}, s \in \mathbb{Z}_q^m, e \xleftarrow{\mathcal{X}} \mathbb{Z}_q^n$.

Given $\boxed{A}$ *and* $\boxed{A} \times \boxed{s} + \boxed{e}$, *find* $\boxed{s}$

> Some intuition on LWE :
>
> - If the error is too big (e.g $\mathcal{X} = \mathcal{U}(\mathbb{Z}_q^n)$), it is impossible to recover s.
> - If the error is too small (e.g. $\mathcal{X} = \{0^n\}$), s can be recovered easily with gaussian elimination.
>
> All the interesting cases lie somewhere in between.

Lemma 3. *SearchLWE* $\overset{red.}{\longleftrightarrow}$ *SIS planted (hence the name LWE regime)*

Proof. I will only show that *SearchLWE* $\xrightarrow{red.}$ *SIS planted*
Let $(A, As + e)$ be an LWE sample. Since $m > n$, $\ker_{left}(A)$ has a large dimension, and thus I can construct a matrice $A^{\perp} \in \mathbb{Z}_q^{(m-n)\times m}$ out of random vectors such that $A^{\perp}A = 0^{(m-n)\times n}$.
Let $y = As + e$. Then $A^{\perp}y = A^{\perp}As + A^{\perp}e = A^{\perp}e$.
Using the SIS planted solver on $(A^{\perp}, A^{\perp}y)$ gives e' small such that $A^{\perp}e' = A^{\perp}e$.
Now let's do gaussian elimination on $(A, y - e')$. If $e = e'$ then this will yield a solution of *SeachLWE*.

There remain to prove that $e' = e$... $\square$

Definition 3. *DecisionalLWE(n,m,q,χ):*
Given the same setting as SearchLWE,
Distinguish between $(A, As + e)$ *and* $(A, \mathcal{U}(\mathbb{Z}_q^m))$

Lemma 4. *SearchLWE* $\overset{red.}{\longleftrightarrow}$ *DecisionalLWE*

Proof. *DecisionalLWE* $\xrightarrow{red.}$ *SearchLWE* trivially.
Let's now prove that *SearchLWE* $\xrightarrow{red.}$ *DecisionalLWE*.
This is a method to recover s_1, the first value of s. It then generalizes for every value.

- Guess $s_1 = b \in \mathbb{Z}_q$ at random.
- Writing the instance problem as a collection of inner products
  $I = (a_i, < a_i, s > + e_i)_{i \in \{1,\dots,m\}}$,
  Generate the instance
  $I' = (a_i + (u_i, 0, 0, 0, \dots), y_i + u_i b)_{i \in \{1,\dots,m\}}$,
  for $(u_1, \dots, u_m) \xleftarrow{\$} \mathbb{Z}_q^m$.
- Run the *DecisionalLWE* distinguisher on the new instance.

If $s_1 = b$, then this is a valid instance and the distinguisher for *DecisionalLWE* will answers YES. Else, the $y_i + u_i b$ look uniform, and thus the distinguisher will answer NO.

Now this method can be repeated until the distinguisher answers YES, and a suitable candidate for s_1 is found (remember that this is probabilistic so there is still a chance that this is not the right s_1).
The whole process can then be repeated for the subsequent $s_2, ..., s_n$ giving a suitable candidate for s. □

If we go back to the "Pre-Quantum" crypto, the counterpart for SearchLWE (SLWE) and DecisionalLWE (DLWE) would respectively be DLog and DDH.
One powerful advantage of the LWE assumption is that there is no reduction from DDH to DLog (whereas there is one from DLWE to SLWE as seen just above).

2 First Constructions

2.1 CRH from SIS homogeneous

Let's define the hash function as :

$$\begin{aligned} H_A : \{0, ..., B\}^m &\longrightarrow \mathbb{Z}_q^n \\ e &\longmapsto Ae \end{aligned}$$

Then if a collision (e_1, e_2) is found, this means that $Ae_1 = Ae_2$, hence that $A(e_1 - e_2) = 0$ with $||e_1 - e_2||_\infty \leq 2B$ and this contradicts the SIS assumption.

2.2 Symmetric encryption from DLWE

to be done next week...