Basis and Fundamentals of Lattice Cryptography

Rick

2020 年 10 月 23 日

1 Basis and fundamentals of Lattice Cryptography

Fundamental talk, please refer to his survey for more details. Nevertheless, I think the summary presented that summarize the three levels of crypto systems achievable from LWE is valuable. Also the IBE scheme introduced is fairly straightforward and clear.

Anyway, since I have got a morning to do this, I might as well organize my notes here.

2 Part I: Lattice and Hard Problems

In cryptography, we normally consider integer lattices (whereas in the next day Nguyen talked about non-integer lattices) $\mathscr{L} \subseteq Z^m$. Lattice basis is like a linear-space basis, but their integer combinations constitute the whole lattice, rather than all linear combinations. We also usually assume full rank lattice here.

The conjectured hard problems on lattice are usually problems regarding *estimating the geometric property* of lattice, e.g. successive minima in GapSVP_γ; or *finding* the vectors that satisfies the estimated successive minima in SVP_γ or SIVP_γ.

For GapSVP_γ, there are known hardness results according to values of γ. Let us restate the problem: input to GapSVP_γ is a m-dim lattice L and a real number d, the distinguisher is required to distinguish the case between $\lambda_1 \leq d$ and $\lambda_1 > \gamma(m) \cdot d$. Intuitively, when γ becomes larger, the gap between the two cases becomes subsequently larger, which makes the problem easier. For more details regarding the mechanics in lattice cryptoanalysis algorithms, please refer to Phone's talk next day. Anyway, the known result can be drawn in a chart:

Approx.	$2^{\log m^{1-\epsilon}}$	$\sqrt{m}$	$\gtrsim m$	$2^{\sim m}$
Hardness	NP-Hard	coNP	crypto	$\in \mathbf{P}$
Paper	[Ajt98,...]	[GG98,AR05]	[Ajt96,...]	[LLL82,Sch97]

For polynomial approximation factor, the known result [AKS01,MV10] takes 2^m time and space. For SIVP, the status quo is about the same.

3 Part II: SIS/LWE and Basic Applications

Since we are all very familiar with the SIS problem, I will not state more of it here. The parameter choice he mentioned was $q = n^2$ where n is the dimension. SIS directly implies a CRHF $f : \{0,1\}^m \to \mathbb{Z}_q^n$.

SIS corresponds to finding the short vector in the dual code with $A_{n\times m}$ as the generation matrix. Or in lattice term, a dual lattice:

$$L^{\perp}(A) = \{z \in \mathbb{Z}^m : Az = \mathbf{0}\}$$

Ajtai showed in [Ajt96] that solving SIS problem on uniformly random A for $\beta \ll q$ implies solving $\mathsf{GapSVP}_{\sqrt{n}\beta}$ or $\mathsf{SIVP}_{\sqrt{n}\beta}$ on any n-dim lattice (ergo worst case to average case reduction).

Application: Digital signature [GPV08]

- key generation is to sample a random SIS matrix A along with a trapdoor, as in [Ajt99,MP12].
- Signing a message μ is just hashing it and find the CRHF f_A pre-image x such that $A \cdot x = H(\mu)$ (note that x must be short).
- Verification of a signature x, μ is to first check x is short, then checks $H(\mu) = A \cdot x$.

One important security requirement is that the signature x should not reveal any information about the trapdoor (i.e. signing key). Another point is that if two signatures are performed on a same message, then if the random oracle is not randomized (i.e. the map is fixed), we can possibly learn two short x's and then learn the SIS solution, which is the trapdoor. In this manner, H must be randomized.

Chris then proceeded to explain the details about the sampling algorithm he mentioned when producing signatures. Given any short basis T of the SIS sample A ($\max ||t_i|| \leq$ std dev), sample x such that $A \cdot x = u$. The requirement of the distribution of x is that it should not leak any information about A. The algorithm for this function is the *nearest plane* algorithm with *randomized rounding* [GPV08,Klein00]. Here is **my conjectured** rationale of this algorithm, rather than the actual one.

- The distribution we require is one that follows a discrete gaussian on the coset $\mathscr{L}_u^{\perp}(A)$. The probability only relies on the distance (possibly l2) between the origin and the point on lattice.
- From the short basis T we can easily acquire one short basis of coset $\mathscr{L}_u^{\perp}(A)$.
- We can project the distribution on to a hyperplane to get a conditional distribution.
- From the distance of the sub-hyperplane to the origin, we can select a proper one according to the Gaussian distribution.

- We then iterate the process until the acquired hyperplane has dimension zero – a point.

I think I really need to read [GPV08] to understand this process.

Chris then proceeds to introduce the (plain) LWE problem, whose form we are all very familiar with. He restated some hardness results. Let n be the dimension, q be the modulus, $\alpha \cdot q$ be the standard deviation which we require that $\sqrt{n} < \text{std. dev.} \ll q$. Then,

$$\mathsf{GapSVP}_{n/\alpha}, \mathsf{SIVP}_{n/\alpha} \underset{\text{Quantum, [R05]}}{\leq} \mathsf{SLWE} \underset{\text{Quantum, [R05,BFKL93]}}{\leq} \mathsf{DLWE} \leq \mathsf{crypto}$$

Also, [P09,BLPRS13] provide fully classical reductions, but with worse parameters. There is also a direct quantum reduction from worst case lattice problems to DLWE in [PRS17].

There is also a fun table Chris showed about the implications of LWE.

表 1: Application of LWE

Components	Class
PKE/KEM	Regular
OT	Regular
CCA2 PKE w/o RO	Regular
(Constrained) PRF	Regular
IBE w/ RO	Efficient
HIBE w/o RO	Efficient
NIZK for NP w/o RO	Efficient
FHE	Exclusive
ABE for arbitrary policy	Exclusive

He then introduced the dual crypto system that appeared in this survey "a decade of lattice cryptography".

The next part of the talk is about IBE from LWE. This part is quite intuitive from the trapdoor construction in [GPV08]. That being said, I still have yet figured out the exact mechanism of nearest plane with randomized rounding. Anyway, assume there is an algorithm $\mathsf{Sample}(A, u)$ that produces $x : A \cdot x = u$, we can then construct the IBE scheme as A is the master pk, its trapdoor T being the master sk. $pk_{\text{alice}} = H(\text{"alice"})$, sk_{alice} be such that $A \cdot sk_{\text{alice}} = pk_{\text{alice}}$. Then the encryption and decryption proceed just like the dual cryptosystem.

4 Ring for Better Efficiency

We can further use operation over ring to improve the efficiency. The ring we consider here is the polynomial ring $R = \mathbb{Z}[X]/(X^n + 1)$ where n is a power of two, and let $R_q = R/qR$. The multiplication over R_q can be done efficiently using FFT algorithm. (I simply copied the slide for this part, but where do I find the algorithm for this operation?)

And likewise, there are search and decision version of RLWE version, which we call DRLWE and SRLWE. They are just like the non-ring version, except the a_i's where used to be vectors, now are ring elements; e_i's where used to be vectors with short norm, now are small ring elements.

The hardness of ring LWE is established in a series of works. The initial work being [LPR10], the paper showed that:

$$\underset{\text{on ideal lattice}}{\mathsf{approxSVP}} \overset{\leq}{\underset{\text{Quantum}}{}} \mathsf{SRLWE} \overset{\leq}{\underset{\text{Classical}}{}} \underset{\text{on any cyclotomic lattice}}{\mathsf{DRLWE}}$$

It is folklore that approximate SVP problem on ideal lattice is not well-understood as that in integer lattice, causing the hardness assumption of RLWE not so well understood as the non-ring counterpart.

A subsequent work [PRSD17] showed a direct quantum reduction from approximate SVP on ideal lattices to DRLWE.