2018-07-23

Nankai-Baidu
Joint Laboratory

Parallel and Distributed
Software Technology Lab

- 早期的实现方案

Rivest、Adleman和Dertouzos于1978年提出了同态加密的思想。

随后很多只支持乘法或加法的方案被人们发现：

- 支持乘法的RSA(1978)和ELGamal(1985)；
- 支持加法的Goldwasser-Micali(1982)和Paillier(1999)。

● 早期的实现方案

直到2009年，Gentry在他的博士论文中阐述了同时支持任意次数的加法和乘法的同态加密方案是可以实现的。

理想格（ideal lattice）：

- Ideal：An ideal I of a ring R is a nonempty subset of R with …
- Lattice: …Groups of the third type listed above are called lattices.

A lattice L in the plane R^2 is generated, or spanned by a set S if every element of L can be written as an integer combination of elements of S.

- 早期的实现方案

直到2009年，Gentry在他的博士论文中阐述了同时支持任意次数的加法和乘法的同态加密方案是可以实现的。

Gentry's construction consists of several steps：

- First we construct a somewhat homomorphic scheme
- Next we need to “squash” the decryption procedure
- Finally we can apply a “bootstrapping” transformation to obtain a FHE

- 目前已有的两个实现方案

➢FV方案:　　SEAL

➢BGV方案:　HElib

Nankai-Baidu Joint Laboratory

Parallel and Distributed Software Technology Lab

- FV方案的安全性

FV方案的安全性基于多项式环上容错学习(R-LWE)的计算困难性

公开密钥密码机制　　NP完全问题

Nankai-Baidu Joint Laboratory

Parallel and Distributed Software Technology Lab

- FV方案的安全性

容错学习难题(LWE):

标记: Z_q是一个整数集合，并且$Z_q = \left\{ n \middle| -\frac{q}{2} < n \leq \frac{q}{2} \right\}$.

Z_q^n是一个n维向量。

e_j是从满足离散高斯分布的整数集合中随机抽取的一个整数。

已知: 一个从Z_q^n中按照均匀分布抽取的随机n维向量$\overrightarrow{a_j} \sim Z_q^n$,

用此向量形成一个有噪声e_j 的内积等式$\overrightarrow{y_j} = < \overrightarrow{a_j}, \vec{s} > + \overrightarrow{e_j}$.

给定: 若干$\{\overrightarrow{a_j},\ \overrightarrow{y_j} = < \overrightarrow{a_j}, \vec{s} > + \overrightarrow{e_j}\}$

问题: 求$\overrightarrow{y_j} \approx < \overrightarrow{a_j}, \vec{s} >$的解 $\vec{s}$.

● FV方案的安全性

环上容错学习难题(LWE):

标记: Z_q是一个整数集合，并且$Z_q = \left\{ n \middle| -\frac{q}{2} < n \leq \frac{q}{2} \right\}$.

Z_q^n是一个n维向量。

e_j是从满足离散高斯分布的整数集合中随机抽取的一个整数。

已知: a是从均匀分布中抽取的随机变量，

$a \cdot s$的结果被一些小的随机变量e所干扰，

e通常抽取自一个固定的概率分布（比如高斯分布）.

给定: 若干$(a,\ b \approx a \cdot s) \in R_q \times R_q$

问题: 求s.

- FV方案的安全性

遇到过的问题:

➢设$\mathrm{R} = Z[x]/f(x)$是系数为整数、以$f(x)$为模的多项式环集合

$$f(x) = x^n + 1 \in \mathrm{Z}[x]$$

商环　　生成的多项式度数小于n

➢离散高斯分布　　Gentry

Nankai-Baidu Joint Laboratory

Parallel and Distributed Software Technology Lab

- Gentry's Bootstrapping

Bootstrapping:

➢Idea:

We could refresh a ciphertext if we could completely decrypt it.

We do decrypt the ciphertext, but homomorphically!

- Gentry's Bootstrapping

Bootstrapping:

➢Recrypt:

$$\mathsf{Recrypt}_{\mathcal{E}}(\mathrm{pk}_2, D\mathcal{E}, \langle\overline{\mathrm{sk}_{1j}}\rangle, \psi_1).$$

$$\mathrm{Set}\ \overline{\psi_{1j}} \xleftarrow{\mathrm{R}} \mathsf{Encrypt}_{\mathcal{E}}(\mathrm{pk}_2, \psi_{1j})$$

$$\mathrm{Output}\ \psi_2 \leftarrow \mathsf{Evaluate}_{\mathcal{E}}(\mathrm{pk}_2, D\mathcal{E}, \langle\langle\overline{\mathrm{sk}_{1j}}\rangle, \langle\overline{\psi_{1j}}\rangle\rangle)$$

- Gentry's Bootstrapping

Bootstrapping:

➢Recrypt:

$$c_1 = Encrypt(pk_1, m_1) \qquad m_1 = Decrypt(sk_1, c_1)$$

$$\overline{c_1} = Encrypt(pk_2, c_1)$$

$$\overline{sk_1} = Encrypt(pk_2, sk_1)$$

$$Decrypt_\varepsilon(\overline{sk_1}, \overline{c_1}) = Encrypt(pk_2, m_1)$$

$$c_2 = Encrypt(pk_2, m_1)$$

- Gentry's Bootstrapping

Bootstrapping:

➢Efficiency:

the complexity of bootstrapping is inherently at least the complexity of decryption times the bit length of the individual ciphertexts that are used to encrypt the bits of the secret key.

- BGV方案

➢(Leveled) Fully Homomorphic Encryption without Bootstrapping.
Zvika Brakerski, Craig Gentry, Vinod Vaikuntanathan

➢HElib (linux, make)
Shai Halevi and Victor Shoup

● BGV方案

➢(Leveled) Fully Homomorphic Encryption without Bootstrapping.
Zvika Brakerski, Craig Gentry, Vinod Vaikuntanathan

➢LWE or Ring LWE:

FV

Modulus Switching(developed by B. and V.)

Nankai-Baidu Joint Laboratory

Parallel and Distributed Software Technology Lab