



2018-07-19

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)。

Nankai-Baidu
Joint Laboratory

Parallel and Distributed
Software Technology Lab





- 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 .

Nankai-Baidu
Joint Laboratory

Parallel and Distributed
Software Technology Lab





- 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

Nankai-Baidu
Joint Laboratory



Parallel and Distributed
Software Technology Lab





- 目前已有的实现方案

- FV方案: SEAL

- BGV方案: HELib

- 别的方案

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

公开密钥非对称密码机制 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 $Z_q = \left\{ n \mid -\frac{q}{2} < n \leq \frac{q}{2} \right\}$.

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 $\vec{a}_j \sim Z_q^n$,

用此向量形成一个有噪声 e_j 的内积等式 $\vec{y}_j = \langle \vec{a}_j, \vec{s} \rangle + \vec{e}_j$.

给定: 若干 $\{\vec{a}_j, \vec{y}_j = \langle \vec{a}_j, \vec{s} \rangle + \vec{e}_j\}$

问题: 求 $\vec{y}_j \approx \langle \vec{a}_j, \vec{s} \rangle$ 的解 \vec{s} .

Nankai-Baidu
Joint Laboratory

Parallel and Distributed
Software Technology Lab





- 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 $Z_q = \left\{ n \mid -\frac{q}{2} < n \leq \frac{q}{2} \right\}$.

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 .

Nankai-Baidu
Joint Laboratory



Parallel and Distributed
Software Technology Lab





- FV方案的安全性

遇到过的问题:

➤ 设 $R = Z[x]/f(x)$ 是系数为整数、以 $f(x)$ 为模的多项式环集合
 $f(x) = x^n + 1 \in Z[x]$

商环

生成的多项式度数小于 n

➤ 离散高斯分布

Gentry

➤ 抽象代数、数论等名词的基本定义、概念以及推理过程



- FV方案的安全性

目前遇到的问题:

- FV方案 实现了部分同态加密 (忽略了理论部分)
把部分同态加密变成全同态加密 (参数的设置、推理论证)
- FV论文 没有Bootstrapping的介绍, 只介绍了其中的关键部分
Gentry的论文

Nankai-Baidu
Joint Laboratory

Parallel and Distributed
Software Technology Lab

