完全準同型暗号のパラメータ導出に関する一考察

On Deriving Parameters of Fully Homomorphic Encryption

中山幸郎・システム分科会・情報セキュリティ大学院大学

Fully homomorphic encryption makes it possible to operate encrypted data. Lattice based fully homomorphic encryption have not been enough researched on the parameter settings with no waste that satisfy the correctness of the decryption and security until today. In this work, we propose optimal parameters derivation of fully homomorphic encryption for FV improved BGV, which are considered to be the most practical is fully homomorphic encryption.

完全準同型暗号の問題点・・・鍵サイズ，暗号文サイズ，計算量
解決案・・・無駄を抑えたパラメータ設定

FV暗号スキーム

- SecretKeyGen(1^λ): $s \leftarrow \chi_{key}$
  output 秘密鍵sk=s
- PublicKeyGen(sk): $a \leftarrow R_q$, $e \leftarrow \chi_{err}$
  $b=[-(as+e)]_q$
  output 公開鍵pk=(b,a)
- Enc(pk,m): $u \leftarrow \chi_{key}$, $e_1, e_2 \leftarrow \chi_{err}$
  output $ct=([bu+e_1+\Delta m]_q, [au+e_2]_q)$
- Dec(sk,ct):$c_0=ct[0]$, $c_1=ct[1]$とし,
  compute $\left[\left\lfloor \frac{t[c_0+c_1 s]_q}{q} \right\rceil \right]_t$

t:平文のモジュラス(t>1)
q:暗号文のモジュラス(q>t)
χ_{key}, $\chi_{err} \in R$:多項式環R上のガウス分布
$\|\chi_{key}\| < B_{key}$
$\|\chi_{err}\| < B_{err}$
$\Delta = \lfloor q/t \rfloor$

準同型乗算

- Evkgen(sk,T): $a_i \leftarrow R_q$, $e_i \leftarrow \chi_{err}$
  output $evk=\{([-(a_i s+e_i)+T^i s^2]_q, a_i): i \in [0,\cdots,l]\}$
- Mult(ct_1,ct_2,evk): compute

$$d_0=\left[\left\lfloor \frac{t(ct_1[0]\cdot ct_2[0])}{q} \right\rceil \right]_q$$

$$d_1=\left[\left\lfloor \frac{t(ct_1[0]\cdot ct_2[1]+ct_1[1]\cdot ct_2[0])}{q} \right\rceil \right]_q$$

$$d_2=\left[\left\lfloor \frac{t(ct_1[1]\cdot ct_2[1])}{q} \right\rceil \right]_q$$

Relin(d_0, d_1, d_2,evk):output

$$d_0'=[d_0+\sum_{i=0}^{l} evk[i][0]\cdot d_2^{(i)}]_q$$

$$d_1'=[d_1+\sum_{i=0}^{l} evk[i][1]\cdot d_2^{(i)}]_q$$

パラメータ導出

演算回路の深さL=10としたとき，以下の式を満たすとき暗号文は正しく復号される．

$$(\lfloor \log_T(q) \rfloor +1)T - q/(960(21/2)^9)+1687/240 < 0$$

この不等式から最小のqを求める．

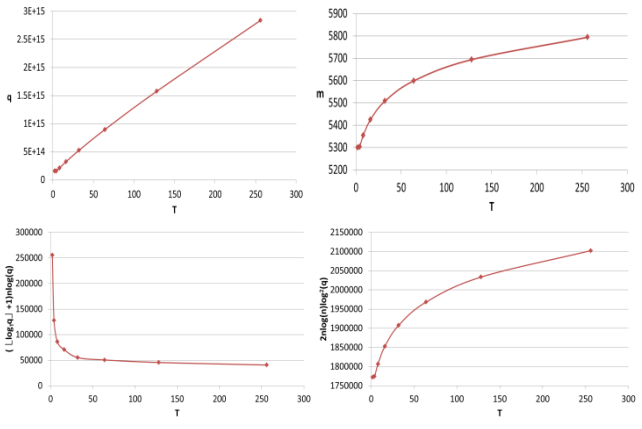
安全性のため，多項式環Rの次元n，格子の次元m，エルミートファクター$\gamma(m)$としたとき，以下の式を満たす必要がある．

$$\gamma(m)^m \cdot q^{n/m} \cdot \sigma_{err} \leq \sqrt{-\log \varepsilon / \pi}$$

この不等式から格子の次元の下限mを求める．

T	暗号文モジュラス(q)	格子の次元(m)	評価鍵サイズ($(\lfloor \log_T q \rfloor+1)n\log(q)$)	暗号化時間($2n\log(n)\log^2(q)$)
2	1538207507896781 (1.53821E+14)	5300	255585	1772020
4	1568840360001201 (1.56884E+14)	5304	127870	1774160
8	2113686113164681 (2.11369E+14)	5354	86024	1806668
16	3213769342935201 (3.21377E+14)	5425	70782	1852861
32	5241806502042551 (5.24181E+14)	5508	55245	1907531
64	8947967866153771 (8.94797E+14)	5599	50505	1968200
128	15759296453479431 (1.57593E+15)	5694	45632	2033448
256	28381305408995121 (2.83813E+15)	5794	40599	2102394

考察



T=32がベスト