TFHE実装入門

8.Multi Value and PBS many LUT

松岡 航太郎

ここで話すこと

- 実はBootstrappingは一度に複数の関数を評価することが可能
  - それを実現する手法を3系統説明する
- 後半２つのアルゴリズムもノイズが増加する
  - 性能の向上に見合うかどうかには慎重になる必要がある

Gao's method

- Gao18で使われている方法
  - SampleExtractを複数ヶ所で行うと複数の関数が評価できる
  - 2入力ゲートの場合は、すべての２入力ゲートは一度に評価できる

```
HalfAdder(ca,cb,KSK,BK)
  cadd = IdentityKeySwitching(ca + cb,KSK )
  crot = BlindRotate(cadd,BK, ∑^{N-1}_{i=0} 1/8 X^i)
  cand = -SampleExtractIndex(crot, N - 2N·1/8)
  cor = SampleExtractIndex(crot, 2N·1/8)
  cxor = cor - cand - (0,1/8)$
  return cxor,cand
```

Programmable Bootstrapping

- Blind Rotateは(ノイズの許す範囲で)任意の非線形関数を評価できる
  - LUTで非線形関数を表現できる
- HomNANDでは平文は$\pm\frac{1}{8}$にとられた
  - その線形和は$\pm\frac{1}{8}, \pm\frac{3}{8}$にとられる
    - この線形和の結果を丸めたρがLUTへのindex
    - LUTの出力はそれぞれの線形和の結果に対してある程度独立に決められる
      - negacyclicなので、$\frac{1}{8}$と$-\frac{3}{8}, \frac{3}{8}$と$-\frac{1}{8}$のペアの出力はそれぞれ互いに符号だけが違うものに固定される
  - 平文をもっと細かい値に取れば線形和の結果のパターンは多くなる
    - 入力bit数が2より大きいLUTが作れる
    - 入力を整数を暗号化したものとして扱うこともできる
  - 細かくすると誤り確率が上がるのでそことのトレードオフ

Multi Value

- CIM19がよくまとまっている
- 基本的なアイデアはtest vector$TV[X]$を$TV_1[X] \cdot TV_0[X]$みたいに因数分解すること
  - $TV_1[X] \in \mathbb{Z}_N$
  - もし共通因子$TV_0[X]$が存在するならこれを使いまわすことができる
  - $\because X^{-\rho} \cdot (TV_1[X] \cdot TV_0[X]) = TV_1[X] \cdot X^{-\rho} \cdot TV_0[X]$
    - $X^{-\rho} \cdot TV_0[X]$はBlind Rotateなので重いが$TV_1[X]$を掛けるのは平文多項式を掛けるだけ
- $TV_0[X]$の選び方で2種類に分かれる
  - $TV[X]$ごとに異なるものを選ぶ方法(Biasse15)
    - 究極的には$TV_0[X] = 1$でも良いが、ケースバイケースで考える
  - 関数空間を制限する代わりに同じものを選ぶ方法(CIM19)
    - 上のに比べるとノイズの点で不利にはなりうる

PBS many LUT

- Programmable Bootstrapping many Look Up Tables
- $N = 2^{Nbit}$と書くとBlind Rotateの出力は$Nbit + 1$のアドレスでLUTを引いていることになる
- 下位のbitを潰せば複数のLUTを同時に評価できるのではないか？
  - v-bit潰すことにすると2^v個同時に評価できる
  - $\rho = 2^v \cdot \lfloor \frac{2N}{2^v} \cdot b \rceil - \sum_{i=0}^{n-1} 2^v \cdot \lceil \frac{2N}{2^v} \cdot a_i \rceil \cdot s_i \mod 2N$
    - [ρ,ρ+2^v-1]の範囲のindexはそれぞれ違うLUTの値を詰めることができる
    - $f_j i, i \in [0, \frac{2}{2^v} - 1], j \in [0, 2^v - 1]$をそれぞれのLUTの値とするとTest Vectorは下のようになる

$$\sum_{i=0}^{\frac{2}{2^v}-1} \sum_{j=0}^{2^v-1} f_{ji} \cdot X^{i \cdot 2^v \cdot j}$$

参考文献

- Biasse15
- CIM19
- CLOT21
- PBSmanyLUTの実装