完全準同型暗号について

About the Fully Homomorphic Encryption

李泰潤・システム分科会・情報セキュリティ大学院大学

Research has continued on the basis of the encryption that Gentry proposed since 2009. Therefore, in this paper, I investigate about SI-HE which realize homomorphic operation without Modulus Switching recently considered as a high efficient method.

完全準同型暗号

平文を暗号化した暗号文同士,加算や乗算ができる.それを復号すると演算された平文が出力される暗号を準同型暗号という.このような準同型演算が何回でも行える暗号を完全準同型暗号という.

Regevの公開鍵暗号スキーム

・$\mathrm{Enc}_{pk}(m)$:

$$m \in \{0,1\} \quad \boldsymbol{r} \in \{0,1\}^N$$
$$\mathbf{m} \triangleq (m, 0, \dots, 0) \in \{0,1\}^{n+1}$$
$$\boldsymbol{c} := \left[\boldsymbol{P}^{\mathrm{T}} \cdot \boldsymbol{r} + \left\lfloor \frac{q}{2} \right\rfloor \cdot \mathbf{m}\right]_q \in Z_q^{n+1}$$

・$\mathrm{Regev.Dec}_{sk}(\boldsymbol{c})$:

$$m := \left[\left\lfloor \frac{2}{q} \cdot [\langle \boldsymbol{c}, (1, \boldsymbol{s})\rangle]_q \right\rceil\right]_2$$

Key Switching

・$\mathrm{SwitchKeyGen}_{q,\chi}(\boldsymbol{s}, \boldsymbol{t})$:

source key $\boldsymbol{s} \in Z^{n_s}$ target key $\boldsymbol{t} \in Z^{n_t}$

$$\hat{n}_s \triangleq n_s \cdot \lceil \log q \rceil \quad \boldsymbol{A}_{\boldsymbol{s}:\boldsymbol{t}} \xleftarrow{\$} Z_q^{\hat{n}_s \times n_t} \quad \boldsymbol{e} \xleftarrow{\$} \chi^{\hat{n}_s}$$
$$\boldsymbol{b}_{\boldsymbol{s}:\boldsymbol{t}} := \left[\boldsymbol{A}_{\boldsymbol{s}:\boldsymbol{t}} \cdot \boldsymbol{t} + \boldsymbol{e}_{\boldsymbol{s}:\boldsymbol{t}} + \mathrm{POT}_q(\boldsymbol{s})\right]_q \in Z_q^{\hat{n}_s}$$
$$\boldsymbol{P}_{\boldsymbol{s}:\boldsymbol{t}} = [\boldsymbol{b}_{\boldsymbol{s}:\boldsymbol{t}} \| -\boldsymbol{A}_{\boldsymbol{s}:\boldsymbol{t}}] \in Z_q^{\hat{n}_s \times (n_t+1)}$$

・$\mathrm{SwitchKey}_q(\boldsymbol{P}_{\boldsymbol{s}:\boldsymbol{t}}, \boldsymbol{c}_s)$:

$$\boldsymbol{c}_t := \left[\boldsymbol{P}_{\boldsymbol{s}:\boldsymbol{t}}^{\mathrm{T}} \cdot \mathrm{BD}_q(\boldsymbol{c}_s)\right]_q$$

ノイズ評価

$q, n, |\chi| \le B, L \quad |e_1|, |e_1| \le E < \lfloor q/2 \rfloor / 2$

$$\langle \mathbf{c}_1, (1, \mathbf{s}_{i-1})\rangle \equiv \left\lfloor \frac{q}{2} \right\rfloor \cdot m_1 + e_1$$
$$\langle \mathbf{c}_2, (1, \mathbf{s}_{i-1})\rangle \equiv \left\lfloor \frac{q}{2} \right\rfloor \cdot m_2 + e_2$$

$$\langle \mathbf{c}_{\mathrm{add}}, (1, \mathbf{s}_i)\rangle \equiv \left\lfloor \frac{q}{2} \right\rfloor \cdot ([m_1 + m_2]_2) + e_{\mathrm{add}}$$
$$\langle \mathbf{c}_{\mathrm{mult}}, (1, \mathbf{s}_i)\rangle \equiv \left\lfloor \frac{q}{2} \right\rfloor \cdot m_1 m_2 + e_{\mathrm{mult}}$$

$$|e_{\mathrm{add}}|, |e_{\mathrm{mult}}| \le O(n \log q) \cdot \max\{E, (n \log^2 q) \cdot B\}$$

準同型SI-HE

・$\text{SI-HE.Keygen}(1, 1^n)$:

$$\mathbf{s} \leftarrow \text{Regev. PublicKeygen}(\mathbf{s})$$
$$\tilde{\boldsymbol{s}} := \mathrm{BD}((1, \mathbf{s})) \otimes \mathrm{BD}((1, \mathbf{s})) \in \{1,0\}^{((n+1)\lceil \log q \rceil)^2}$$
$$\boldsymbol{P} \leftarrow \mathrm{SwitchKeyGen}(\tilde{\boldsymbol{s}}, \mathbf{s})$$

$$output \quad pk = \boldsymbol{P}, evk = \left\{\boldsymbol{P}_{(i-1):i}\right\}_{i \in [L]}, sk = \mathbf{s}$$

・$\text{SI-HE.Eval}_{evk}(\cdot)$:

- $\text{SI-HE.Add}_{evk}(\boldsymbol{c}_1, \boldsymbol{c}_2)$:

$$\tilde{\boldsymbol{c}}_{\mathrm{add}} := \mathrm{POT}(\boldsymbol{c}_1 + \boldsymbol{c}_2) \otimes \mathrm{POT}((1,0,\cdots,0))$$
$$\boldsymbol{c}_{\mathrm{add}} \leftarrow \mathrm{SwitchKey}(\boldsymbol{P}, \tilde{\boldsymbol{c}}_{\mathrm{add}}) \in Z_q^{n+1}$$

- $\text{SI-HE.Mult}_{evk}(\boldsymbol{c}_1, \boldsymbol{c}_2)$:

$$\tilde{\boldsymbol{c}}_{\mathrm{mult}} := \left\lfloor \frac{2}{q} \cdot (\mathrm{POT}(\boldsymbol{c}_1) \otimes \mathrm{POT}(\boldsymbol{c}_2)) \right\rceil$$
$$\boldsymbol{c}_{\mathrm{mult}} \leftarrow \mathrm{SwitchKey}(\boldsymbol{P}, \tilde{\boldsymbol{c}}_{\mathrm{mult}}) \in Z_q^{n+1}$$

・$\text{SI-HE.Enc}_{pk}(m)$と$\text{SI-HE.Dec}_{sk}(\boldsymbol{c})$はRegevのスキームと同一のため省略

(POT=PowersOfTwo, BD=BitDecomp)

「Without Modulus Switching」とは

暗号文cを復号する際に $\langle \mathbf{c}, (1, \mathbf{s})\rangle = \left\lfloor \frac{2}{q} \right\rfloor \cdot m + e$

ようになるので,準同型演算を行った$\boldsymbol{c}_{add}$と$\boldsymbol{c}_{mult}$の中に$\left\lfloor \frac{q}{2} \right\rfloor$をかけることによって

BGV暗号の復号

$$\left[[\langle c, s\rangle]_q\right]_2 = m \quad \left(-\tfrac{q}{2} < m + 2er < \tfrac{q}{2}\right)$$
$$[\langle c, s\rangle]_q = m + 2er$$

を使わずにノイズを減らすことができる.