2018-07-30

Nankai-Baidu
Joint Laboratory

Parallel and Distributed
Software Technology Lab

- Fully Homomorphic Encryption without Bootstrapping

  Zvika **B**rakerski Craig **G**entry Vinod **V**aikuntanathan

- Efficient Fully Homomorphic Encryption from (Standard) LWE

  Zvika **B**rakerski Vinod **V**aikuntanathan

- Efficient Fully Homomorphic Encryption from (Standard) LWE

  Zvika **B**rakerski Vinod **V**aikuntanathan

- Show that Somewhat HE can be based on LWE, using a new re-linearization technique.
- We introduce a new dimension-modulus reduction technique, which shortens the ciphertexts and reduces the decryption complexity

➢Efficient Fully Homomorphic Encryption from (Standard) LWE

Zvika **B**rakerski Vinod **V**aikuntanathan

- Re-linearization technique:

  does not require hardness assumptions on ideals.

  In contrast, all previous schemes relied on complexity assumptions related to ideals in various rings.

- Re-linearization technique:

  To encrypt a bit $m \in \{0,1\}$

  using secret key $s \in Z_q^n$, a random vector $a \in Z_q^n$, and a noise e.

  $c = (a,\ b = \langle a, s\rangle + 2e + m)$

  $f_{a,b}(x) = b - \langle a, x\rangle \ \ (mod\ q) = \mathrm{b} - \sum_{i=1}^{n} a[i] \cdot x[i]$

  decryption: $f_{a,b}(s)$, and then taking the result modulo 2.

  Homomorphic multiplication:

$$f_{a,b}(x) \cdot f_{a',b'}(x) = \left(\mathrm{b} - \sum a[i] \cdot x[i]\right) \cdot \left(b' - \sum a'[i] \cdot x[i]\right)$$

Nankai-Baidu Joint Laboratory

Parallel and Distributed Software Technology Lab

- Re-linearization technique:

$c = (a,\ b = \langle a, s\rangle + 2e + m)$

$f_{a,b}(x) = b - \langle a, x\rangle \pmod q = \mathrm{b} - \sum_{i=1}^{n} a[i]\cdot x[i]$

decryption: $f_{a,b}(s)$, and then taking the result modulo 2.

$$f_{a,b}(x)\cdot f_{a',b'}(x) = \left(\mathrm{b} - \sum a[i]\cdot x[i]\right)\cdot\left(b' - \sum a'[i]\cdot x[i]\right)$$

$$= h_0 + \sum h_i \cdot x[i] + \sum h_{i,j}\cdot x[i]x[j]$$

$m = s[i], s[i]s[j] \qquad b = \langle a, \boldsymbol{t}\rangle + 2e + m$

$$= h_0 + \sum h_i \cdot (b_i - \langle a_i, t\rangle) + \sum h_{i,j}\cdot (b_{i,j} - \langle a_{i,j}, t\rangle)$$

➢Efficient Fully Homomorphic Encryption from (Standard) LWE

Zvika **B**rakerski Vinod **V**aikuntanathan

- Dimension-modulus reduction technique:

$$(a,\ b = \langle a, \boldsymbol{s} \rangle + 2e + \boldsymbol{m}) \quad >>> \quad (a',\ b' = \langle a', \boldsymbol{t} \rangle + 2e' + \boldsymbol{m})$$

$\boldsymbol{s}$ and $\boldsymbol{t}$ need not have the same dimension n.

$\boldsymbol{t}$ have not only low dimension but also small modulus p

➢Efficient Fully Homomorphic Encryption from (Standard) LWE

Zvika **B**rakerski   Vinod **V**aikuntanathan

- Dimension-modulus reduction technique:

$(a,\ b = \langle a, \boldsymbol{s} \rangle + 2e + \boldsymbol{m}) \quad >>> \quad (a',\ b' = \langle a', \boldsymbol{t} \rangle + 2e' + \boldsymbol{m})$

intuition: $\quad Z_q \quad >>> \quad Z_p$

(by simple scaling, up to a small error.)

$s \to t: \quad b_{i,\tau} = \langle b_{i,\tau}, t \rangle + e + \left\lfloor \frac{\boldsymbol{p}}{\boldsymbol{q}} \cdot 2^{\tau} \cdot s[i] \right\rceil$

➢Efficient Fully Homomorphic Encryption from (Standard) LWE

Zvika **B**rakerski   Vinod **V**aikuntanathan

- Dimension-modulus reduction technique:

$$(a,\ b = \langle a, \boldsymbol{s}\rangle + 2e + \boldsymbol{m}) \quad >>> \quad (a',\ b' = \langle a', \boldsymbol{t}\rangle + 2e' + \boldsymbol{m})$$

$$s \rightarrow t: \quad b_{i,\tau} = \langle b_{i,\tau}, t\rangle + e + \left\lfloor \frac{\boldsymbol{p}}{\boldsymbol{q}} \cdot 2^{\tau} \cdot s[i] \right\rceil$$

we scale $2^{\tau} \cdot s[i]$ into an element in Z_p by multiplying by $\frac{\boldsymbol{p}}{\boldsymbol{q}}$ and rounding.(which incurs an additional error of magnitude at most .5)

Nankai-Baidu Joint Laboratory
Parallel and Distributed Software Technology Lab

➢Efficient Fully Homomorphic Encryption from (Standard) LWE

Zvika **B**rakerski   Vinod **V**aikuntanathan

- Re-linearization: FV RLWE
- Dimension-modulus reduction: BGV

➢Fully Homomorphic Encryption without Bootstrapping

Zvika **B**rakerski   Craig **G**entry   Vinod **V**aikuntanathan

- They use modulus switching in one shot to obtain a small ciphertext
- We will use it iteratively to keep the noise level essentially constant.

$m = \quad [\langle c', s\rangle]_p = [\langle c, s\rangle]_q \ mod\ 2.$

if s is short and p is sufficiently smaller than q,

the noise in the ciphertext actually decreases.

- Fully Homomorphic Encryption without Bootstrapping

  Zvika **B**rakerski   Craig **G**entry   Vinod **V**aikuntanathan

- We will use it iteratively to keep the noise level essentially constant.

  $m = [\langle c', s \rangle]_p = [\langle c, s \rangle]_q \ mod\ 2.$

  a ladder of decreasing moduli

  from $q_L\big((L+1) \cdot \mu\ bits\big)$ down to$q_0(\mu\ bits)$

  FHE.Add FHE.Refresh

  FHE.Mult FHE.Refresh

- 目前已有的两个实现方案

- BGV方案: Helib (Linux)

  Java BGV

Nankai-Baidu Joint Laboratory

Parallel and Distributed Software Technology Lab