An implementation of FHE with small ciphertext and key size through a modification of Gentry

Alan R. Hahn

Technische Universität Kaiserslautern

Jan 2020

Small Principal Ideal Problem (SPIP)

Given a principal ideal $\mathfrak{a}$ *in two element representation, compute a "small" generator of the ideal.*

Small Principal Ideal Problem (SPIP)

Given a principal ideal $\mathfrak{a}$ in two element representation, compute a "small" generator of the ideal.

- $N^{O(N)} \cdot \sqrt{\min(A, R)} \cdot |\Delta|^{O(1)}$
- $\exp(O(N \log N) \cdot \sqrt{\log(\Delta) \cdot \operatorname{loglog}(\Delta)})$

Definitions and Notation

For $g(x) = \sum_{i=0}^{t} g_i x^i \in \mathbb{Q}[x]$, *define*

$$||g(x)||_2 = \sqrt{\sum_{i=0}^{t} g_i^2} \quad \textit{and} \quad ||g(x)||_\infty = \max_{i=0,\dots,t} |g_i|.$$

Definitions and Notation

For $g(x) = \sum_{i=0}^{t} g_i x^i \in \mathbb{Q}[x]$, *define*

$$||g(x)||_2 = \sqrt{\sum_{i=0}^{t} g_i^2} \quad \textit{and} \quad ||g(x)||_\infty = \max_{i=0,\ldots,t} |g_i|.$$

For $r > 0$, *define*

$$B_{2,N}(r) = \left\{ \sum_{i=0}^{N-1} a_i x^i : \sum_{i=0}^{N-1} a_i^2 \leq r^2 \right\},$$

$$B_{\infty,N}(r) = \left\{ \sum_{i=0}^{N-1} a_i x^i : -r \leq a_i \leq r \right\},$$

$$B_{\infty,N}^{+}(r) = \left\{ \sum_{i=0}^{N-1} a_i x^i : 0 \leq a_i \leq r \right\}.$$

Definitions and Notation

For $g(x) = \sum_{i=0}^{t} g_i x^i \in \mathbb{Q}[x]$, *define*

$$||g(x)||_2 = \sqrt{\sum_{i=0}^{t} g_i^2} \quad \textit{and} \quad ||g(x)||_\infty = \max_{i=0,\dots,t} |g_i|.$$

For $r > 0$, *define*

$$B_{2,N}(r) = \left\{ \sum_{i=0}^{N-1} a_i x^i : \sum_{i=0}^{N-1} a_i^2 \le r^2 \right\},$$

$$B_{\infty,N}(r) = \left\{ \sum_{i=0}^{N-1} a_i x^i : -r \le a_i \le r \right\},$$

$$B_{\infty,N}^{+}(r) = \left\{ \sum_{i=0}^{N-1} a_i x^i : 0 \le a_i \le r \right\}.$$

Note $B_{2,N}(r) \subset B_{\infty,N}(r) \subset B_{2,N}(\sqrt{N} \cdot r)$.

Definitions and Notation (Continued)

Denote by $a \leftarrow b$ the assignment of the value of b to the value of a.
Denote by $a \leftarrow_R A$, for a set A, the selection of a from A using a uniform distribution.
For $m \in \mathbb{Z}_{Odd}$, reductions modulo m result in a value in the range $[-(m-1)/2, (m-1)/2]$.

Definitions and Notation (Continued)

Denote by $a \leftarrow b$ the assignment of the value of b to the value of a.
Denote by $a \leftarrow_R A$, for a set A, the selection of a from A using a uniform distribution.
For $m \in \mathbb{Z}_{Odd}$, reductions modulo m result in a value in the range $[-(m-1)/2, (m-1)/2]$.

Facts about Ideals in Number Fields

Let $K = \mathbb{Q}(\theta)$, with $F(\theta) = 0$ for some monic irreducible $F \in \mathbb{Z}[x]$ of degree N.
Consider $\mathbb{Z}[\theta] \subset \mathcal{O}_K$; the scheme works with ideals of $\mathbb{Z}[\theta]$ coprime to $[\mathcal{O}_K : \mathbb{Z}[\theta]]$.
Such ideals can be generated by two elements.

Facts about Ideals in Number Fields (Continued)

Let $K = \mathbb{Q}(\theta)$, with $F(\theta) = 0$ for some monic irreducible $F \in \mathbb{Z}[x]$ of degree N.
Consider $\mathbb{Z}[\theta] \subset \mathcal{O}_K$; the scheme works with ideals of $\mathbb{Z}[\theta]$ coprime to $[\mathcal{O}_K : \mathbb{Z}[\theta]]$.
Such ideals can be generated by two elements.
Indeed, for a rational prime p,

$$F(x) = \prod_{i=1}^{t} F_i(x)^{e_i} \pmod{p},$$

so that for ideals lying above a rational prime p, p not dividing $[\mathcal{O}_K : \mathbb{Z}[\theta]]$, the prime ideals dividing $p\mathbb{Z}[\theta]$ are given by

$$\mathfrak{p}_i = \langle p, F_i(\theta) \rangle.$$

For $F_i(x)$ of degree 1, reduction modulo $\mathfrak{p}_i$ produces a homomorphism

$$\iota_{\mathfrak{p}_i} : \mathbb{Z}[\theta] \to \mathbb{F}_p,$$

and $\mathfrak{p}_i = \langle p, \theta - \alpha \rangle$, where α is a root of $F(x)$ modulo p.
Given $\chi = \sum_{i=0}^{N-1} c_i \theta^i$, $\iota_{\mathfrak{p}_i}$ then corresponds to evaluation of $\chi(\theta)$ in α modulo p.

Somewhat Homomorphic Scheme : Parameters N, η, μ

- **KeyGen**() :
  - Set plaintext space $\mathcal{P} = \{0, 1\}$
  - Choose monic, irreducible $F(x) \in \mathbb{Z}[x]$ of degree N
  - Repeat until p prime:
    - $S(x) \leftarrow_R B_{\infty,N}(\eta/2)$
    - $G(x) \leftarrow 1 + 2 \cdot S(x)$
    - $p \leftarrow resultant(G(x), F(x))$
  - $D(x) \leftarrow gcd(G(x), F(x))$ over $\mathbb{F}_p[x]$
  - Denote by $\alpha \in \mathbb{F}_p$ the unique root of $D(x)$
  - Apply XGCD-algorithm over $\mathbb{Q}[x]$ to obtain $Z(x) = \sum_{i=0}^{N-1} z_i x^i \in \mathbb{Z}[x]$ such that $Z(x) \cdot G(x) = p \pmod{F(x)}$
  - $B \leftarrow z_0 \pmod{2p}$

  The public key $PK = (p, \alpha)$, the private key $SK = (p, B)$

- **Encrypt**(M, PK) :
  - Parse PK as (p, α)
  - If $M \notin \{0, 1\}$, abort
  - $R(x) \leftarrow_R B_{\infty,N}(\mu/2)$
  - $C(x) \leftarrow M + 2 \cdot R(x)$
  - $c \leftarrow C(\alpha) \pmod{p}$
  - Output c

- **Decrypt**(c, SK) :
  - Parse SK as (p, B)
  - $M \leftarrow (c - \lfloor c \cdot B/p \rceil) \pmod{2}$
  - Output M

- **Add**(c_1, c_2, PK) :
  - Parse PK as (p, α)
  - $c_3 \leftarrow (c_1 + c_2) \pmod{p}$
  - Output c_3

- **Mult**(c_1, c_2, PK) :
  - Parse PK as (p, α)
  - $c_3 \leftarrow (c_1 \cdot c_2) \pmod{p}$
  - Output c_3

Analysis of Add and Multiply

Recall decryption of $c = C(\alpha)$ *requires* $C(x) = M + 2 \cdot R(x) \in B_{\infty,N}(r_{Dec})$.

Analysis of Add and Multiply

Recall decryption of $c = C(\alpha)$ *requires* $C(x) = M + 2 \cdot R(x) \in B_{\infty,N}(r_{Dec})$.
Let c_1, c_2 *and* $C_1(x) = M_1 + N_1(x), C_2(x) = M_2 + N_2(x)$ *denote two ciphertexts and their corresponding polynomials, with* $C_i(x) \in B_{\infty,N}(r_i)$.

Analysis of Add and Multiply

Recall decryption of $c = C(\alpha)$ *requires* $C(x) = M + 2 \cdot R(x) \in B_{\infty,N}(r_{Dec})$.
Let c_1, c_2 *and* $C_1(x) = M_1 + N_1(x), C_2(x) = M_2 + N_2(x)$ *denote two ciphertexts and their corresponding polynomials, with* $C_i(x) \in B_{\infty,N}(r_i)$.
Then for the addition and multiplication of $C_i(x)$

$$C_3(x) = M_3 + N_3(x) = (M_1 + N_1(x)) + (M_2 + N_2(x)),$$
$$C_4(x) = M_4 + N_4(x) = (M_1 + N_1(x)) \cdot (M_2 + N_2(x)),$$

$C_3(x) \in B_{\infty,N}(r_1 + r_2)$, $C_4(x) \in B_{\infty,N}(\delta_\infty \cdot r_1 \cdot r_2)$
$(||g(x) \cdot h(x)||_\infty \leq \delta_\infty \cdot ||g(x)||_\infty \cdot ||h(x)||_\infty)$.

Analysis of Add and Multiply

Recall decryption of $c = C(\alpha)$ *requires* $C(x) = M + 2 \cdot R(x) \in B_{\infty,N}(r_{Dec})$.
Let c_1, c_2 *and* $C_1(x) = M_1 + N_1(x)$, $C_2(x) = M_2 + N_2(x)$ *denote two ciphertexts and their corresponding polynomials, with* $C_i(x) \in B_{\infty,N}(r_i)$.
Then for the addition and multiplication of $C_i(x)$

$$C_3(x) = M_3 + N_3(x) = (M_1 + N_1(x)) + (M_2 + N_2(x)),$$
$$C_4(x) = M_4 + N_4(x) = (M_1 + N_1(x)) \cdot (M_2 + N_2(x)),$$

$C_3(x) \in B_{\infty,N}(r_1 + r_2)$, $C_4(x) \in B_{\infty,N}(\delta_\infty \cdot r_1 \cdot r_2)$
$(||g(x) \cdot h(x)||_\infty \leq \delta_\infty \cdot ||g(x)||_\infty \cdot ||h(x)||_\infty)$.
Thus after executing a circuit of multiplicative depth d *for an initial* $C(x) \in B_{\infty,N}(\mu)$, *we get the corresponding polynomial* $C'(x) \in B_{\infty,N}(r)$ *with*

$$r \approx (\delta_\infty \cdot \mu)^{2^d}.$$

Then $r \approx (\delta_\infty \cdot \mu)^{2^d} \leq r_{Dec} \Rightarrow$

$$d \log 2 \leq \log \log r_{Dec} - \log \log(\delta_\infty \cdot \mu).$$