РусКрипто

XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Алгебраический анализ шифрсистемы UFHE-ILC на основе свойств дзета-функции Дедекинда и сумм идеалов

Коновалов Александр студент, НИЯУ МИФИ

Научный руководитель: Пудовкина Марина Александровна

Шифрсистема UFHE-ILC [1]

- “Неограниченная” полностью гомоморфная шифрсистема (An Unbounded Fully Homomorphic Encryption Scheme Based on Ideal Lattices and Chinese Remainder Theorem).
- Опубликована в 2023 году.
- В открытых источниках, ссылающихся на данную работу, анализ не проводился.

1. Zheng Z., Liu F., Tian K. An Unbounded Fully Homomorphic Encryption Scheme Based on Ideal Lattices and Chinese Remainder Theorem // Journal of Information Security. — 2023. — Vol. 14, no. 4. — P. 366–395.

Основные понятия шифрсистемы UFHE-ILC [1]

- Пусть векторы $v_1, v_2, \dots, v_m \in \mathbb{R}^n, m \leq n$ линейно независимы. Множество

  $\Lambda = \Lambda(v_1, v_2, \dots, v_m) = \{\sum_{i=1}^{m} \alpha_i b_i \mid \alpha_i \in \mathbb{Z}, i \in \{1, \dots, m\}\}$

  называется *решёткой, а* набор векторов $(v_1, \dots, v_m)$ – *базисом решётки.*

- Основная структура – факторкольцо $R_g = \mathbb{Z}[x]/\big(g(x)\big)$, $g(x)$ – приведённый многочлен.

- Отображение $\tau: R_g \to \mathbb{Z}^n$ сопоставляет многочлену набор его коэффициентов.

1. Zheng Z., Liu F., Tian K. An Unbounded Fully Homomorphic Encryption Scheme Based on Ideal Lattices and Chinese Remainder Theorem // Journal of Information Security. — 2023. — Vol. 14, no. 4. — P. 366–395.

Основные понятия шифрсистемы UFHE-ILC [1]

- *Матрица идеала*: $H^*(a) = [a, Ha, \dots, H^{n-1}a]$ задаётся вектором a и матрицей H, сопровождающего многочлена $g(x)$.

- Операция свёртки $a \otimes b = H^*(a)b$.

- Кольца $(\mathbb{Z}^n, +, \otimes)$ и R_g изоморфны, дальше будем их отождествлять.

- *Идеальная решётка*: $\Lambda \subset \mathbb{Z}^n$ – идеал $(\mathbb{Z}^n, +, \otimes)$.

1. Zheng Z., Liu F., Tian K. An Unbounded Fully Homomorphic Encryption Scheme Based on Ideal Lattices and Chinese Remainder Theorem // Journal of Information Security. — 2023. — Vol. 14, no. 4. — P. 366–395.

Китайская теорема об остатках

Теорема (Китайская теорема об остатках для идеалов)

Пусть $k \in \mathbb{N}$, $\Lambda_1, \dots, \Lambda_k$ – попарно взаимно простые идеальные решётки $\mathbb{Z}^n$.

Тогда

$$\oplus_{i=1}^{k} \mathbb{Z}^n/\Lambda_i \cong \mathbb{Z}^n/\Lambda_1\Lambda_2 \dots \Lambda_k.$$

Следствие. Пусть выполняется условие Китайской теоремы об остатках для идеалов.

Тогда $\forall i \in \{1, \dots, k\}$ существует такое $A_i \in \mathbb{Z}^n$, что

$$\begin{cases} A_i = e \bmod \Lambda_i, \\ A_j = 0 \bmod \Lambda_i, j \in \{1, \dots, k\} \setminus \{i\}. \end{cases} \quad (1)$$

Основные понятия

- *Эрмитова нормальная форма матрицы* $\mathrm{B} = \left(b_{i,j}\right)_{n\times n}$ целочисленной решётки Λ*:*
  - $b_{i,j} = 0$ для всех $0 \le j < i \le n$,
  - $0 \le b_{i,j} < b_{i,i}$ для всех $0 \le i < j \le n$.

- *Ортогональная форма матрицы* B^* целочисленной решётки Λ:

$$\mathrm{B}^* = \mathrm{diag}\{\mathrm{b}_{11}, \mathrm{b}_{22}, \dots, \mathrm{b}_{\mathrm{nn}}\}.$$

- *Одномерный модуль решётки*

$$t(\Lambda) = b_{11}.$$

Описание шифрсистемы UFHE-ILC

- Закрытый ключ $SK = (\Lambda_1, \Lambda_2, \dots, \Lambda_k)$ – набор из k взаимно простых идеалов.
- Открытый ключ $PK = (\mathcal{P}, S)$:
  - $\mathcal{P} = \bigoplus_{i=1}^{k} \mathbb{Z}_{t_i}$– множество открытых текстов;
  - $t_i = t(\Lambda_i)$, для $i = 1, \dots, k$;
  - $S = (A_1, A_2, \dots, A_k)$;
  - Λ_i и $(A_1, A_2, \dots, A_k)$ удовлетворяют условию:

$$\begin{cases} A_i = e \bmod \Lambda_i, \\ A_j = 0 \bmod \Lambda_i, j \in \{1, \dots, k\} \setminus \{i\}, \end{cases}$$

для $i = 1, \dots, k$.

Критерий взаимной простоты идеалов

Для практической реализации предложены следующие параметры:

- $g(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, где p – простое число,
- $\Lambda_i = \Lambda_{q_i} = (x^{p-2} + q_i) \in SK$, где q_i – простое число.

Лемма 5.1 (взаимная простота Λ_{q_1} и Λ_{q_2} из работы [1])

Пусть q_1, q_2 – простые числа. Тогда идеалы Λ_{q_1} и Λ_{q_2} взаимно просты.

- Эта лемма обосновывается тем, что многочлен $x^{p-2} + q$ неприводим в $\mathbb{Z}[x]$, а значит и в R_g, что в общем случае неверно.

```
sage: p = 17
sage: k = CyclotomicField(p)
sage: y = k.gen()
sage: O = k.ring_of_integers()
sage: q1, q2 = 34897, 56543
sage: is_prime(q1) and is_prime(q2)
True
sage: I1 = O.ideal(y^(p - 2) + q1)
sage: I2 = O.ideal(y^(p - 2) + q2)
sage: (I1 + I2).is_one()
False
```

Рис. 1. Контрпример: простые q_1, q_2, для которых соответствующие идеалы не являются взаимно простыми

1. Zheng Z., Liu F., Tian K. An Unbounded Fully Homomorphic Encryption Scheme Based on Ideal Lattices and Chinese Remainder Theorem // Journal of Information Security. — 2023. — Vol. 14, no. 4. — P. 366–395.

Критерий взаимной простоты идеалов

Утверждение (критерий взаимной простоты главных идеалов)

Пусть $\Lambda_{q_1}, \Lambda_{q_2}$ – идеальные решётки. Они взаимно просты тогда и только тогда, когда НОД$(t(\Lambda_{q_1}), q_1 - q_2) = 1$.

- Идея доказательства: $(q_1 - q_2) \in (\Lambda_{q_1} + \Lambda_{q_2})$ и из Дедекиндовости R_g следует:
  - либо существование простого идеала $\mathfrak{p}$, для которого $\mathfrak{p} \mid (q_1 - q_2)$ и $\mathfrak{p} \mid \Lambda_{q_1}$,
  - либо взаимная простота $(q_1 - q_2)$ и Λ_{q_1}.

- Круговое поле $K = \mathbb{Q}[x]/(g(x))$, где $g(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

- В алгоритм генерации ключей семейства шифрсистем UFHE-ILC нужно добавить проверку НОД$(t(\Lambda_{q_1}), q_1 - q_2) = 1$.

Общая идея атаки

Идея: Использование аддитивной структуры открытого ключа, основанной на условии:

$$\begin{cases} A_i = e \bmod \Lambda_i, \\ A_j = 0 \bmod \Lambda_i, j \in \{1, \dots, k\} \setminus \{i\}. \end{cases}$$

Лемма (О сумме идеалов). Пусть Λ – некоторый идеал кольца R_g, $r \in \mathbb{N}$, $(I_1, \dots, I_r)$ – набор идеалов кольца R_g, где $I_i \subseteq \Lambda$ для $i = 1, \dots, r$. Тогда

$$I = \sum_{i=1}^{r} I_i \subseteq \Lambda.$$

Общая идея атаки

Определение (Уязвимая компонента). Пусть существует $i \in \{1, \dots, k\}$ такой, что $\Lambda_i \in SK$. Элемент Λ_i секретного ключа будем называть *уязвимым*, если:

$$\sum_{j=1, j\neq i}^{k} (A_j) + (A_i - e) = \Lambda_i,$$

где $A_j \in S,$ для $j = 1, \dots, k.$

Алгоритм восстановления уязвимой компоненты ключа

Вход: часть открытого ключа $S = (A_1, A_2, \dots, A_k)$, i – номер уязвимой компоненты.

- **Шаг 1. Вычислить матрицу M:**

$$M = [H^*(A_1), H^*(A_2), \dots, H^*(A_i - e), \dots].$$

- **Шаг 2. Вычислить эрмитову нормальную форму матрицы M.**

Выход: эрмитова нормальная форма матрицы M без нулевых столбцов.

Алгоритм восстановления уязвимой компоненты ключа

Сложность: Алгоритм работает за полиномиальное время

$\mathcal{O}(kn^2 + n^{\omega} \log ||\mathrm{M}||)$, где

- n – размерность пространства $\mathbb{Z}^n$,
- ω – экспонента матричного умножения, зависящая от реализации алгоритма перемножения матриц,
- $||M||$ – наибольший по модулю элемент, входящий в матрицу.

Алгоритм восстановления всего ключа.

Если каждый элемент секретного ключа является уязвимым, тогда алгоритм восстановления всего ключа можно представить в виде итеративного перебора номера уязвимой компоненты.

2. Pernet C., Stein W. Fast computation of Hermite normal forms of random integer matrices // Journal of Number Theory. — 2010. — Vol. 130, no. 7. — P. 1675–1683.

Условие уязвимости компоненты ключа

- Согласно алгоритму: $\Lambda_i = (\gamma_i) \in SK, \gamma_i \in R_g$ для $i = 1, \dots, k$.
- Без ограничения общности рассмотрим систему для Λ_1:

$$\begin{cases} A_1 - e = \gamma_2 \dots \gamma_k D_1 - e = \gamma_1 r_1, \\ A_2 = \gamma_1 \gamma_3 \dots \gamma_k D_2 = \gamma_1 r_2, \\ \vdots \\ A_k = \gamma_1 \gamma_2 \dots \gamma_{k-1} D_k = \gamma_1 r_k, \end{cases}$$

где $A_i \in S$, $D_i, r_i \in R_g$ для $i = 1, \dots, k$.

Algorithm 3: Generating Algorithm for Secret Key

- **First step.** Randomly select an non-zero vector $\alpha \in \mathbb{Z}^n$ as input, and the output is the following relatively prime two ideal I_1 and I_2, where

$$I_1 =< \alpha >, \text{ and } I_2 =< e - \alpha > .$$

- **Second step.** Randomly select two non-zero vectors $\alpha_1 \in I_1$ and $\alpha_2 \in I_2$ as input, and the output is the following ideal I_3, where

$$I_3 =< e - \alpha_1 \otimes \alpha_2 > .$$

It is easy to see that I_1, I_2, I_3 are pairwise relatively prime ideals.

- **Last step.** Suppose that $m-1$ pairwise relatively prime ideals $I_1, I_2, \dots, I_{m-1}$ are selected, then one randomly finds $\alpha_1 \in I_1$, $\alpha_2 \in I_2$, $\dots$, $\alpha_{m-1} \in I_{m-1}$, $\alpha_i \neq 0$, and the output ideal I_m given by

$$I_m =< e - \alpha_1 \otimes \alpha_2 \otimes \cdots \otimes \alpha_{m-1} > .$$

Obviously, $I_1, I_2, \dots, I_m$ are pairwise relatively prime ideals in $\mathbb{Z}^n$.

Рис. 2. Алгоритм генерации секретных ключей из работы [1].

1. Zheng Z., Liu F., Tian K. An Unbounded Fully Homomorphic Encryption Scheme Based on Ideal Lattices and Chinese Remainder Theorem // Journal of Information Security. — 2023. — Vol. 14, no. 4. — P. 366–395.

Условие уязвимости компоненты ключа

- **Условие уязвимости компоненты:**

  если $(r_1, \dots, r_k) = R_g$, то Λ_1 является уязвимой компонентой.

Algorithm 3: Generating Algorithm for Secret Key

- **First step.** Randomly select an non-zero vector $\alpha \in \mathbb{Z}^n$ as input, and the output is the following relatively prime two ideal I_1 and I_2, where

$$I_1 =< \alpha >, \text{ and } I_2 =< e - \alpha > .$$

- **Second step.** Randomly select two non-zero vectors $\alpha_1 \in I_1$ and $\alpha_2 \in I_2$ as input, and the output is the following ideal I_3, where

$$I_3 =< e - \alpha_1 \otimes \alpha_2 > .$$

It is easy to see that I_1, I_2, I_3 are pairwise relatively prime ideals.

- **Last step.** Suppose that $m-1$ pairwise relatively prime ideals $I_1, I_2, \dots, I_{m-1}$ are selected, then one randomly finds $\alpha_1 \in I_1$, $\alpha_2 \in I_2$, $\dots$, $\alpha_{m-1} \in I_{m-1}$, $\alpha_i \neq 0$, and the output ideal I_m given by

$$I_m =< e - \alpha_1 \otimes \alpha_2 \otimes \cdots \otimes \alpha_{m-1} > .$$

Obviously, $I_1, I_2, \dots, I_m$ are pairwise relatively prime ideals in $\mathbb{Z}^n$.

Рис. 2. Алгоритм генерации секретных ключей из работы [1].

1. Zheng Z., Liu F., Tian K. An Unbounded Fully Homomorphic Encryption Scheme Based on Ideal Lattices and Chinese Remainder Theorem // Journal of Information Security. — 2023. — Vol. 14, no. 4. — P. 366–395.

Вероятностная оценка уязвимости ключа

- $K = \mathbb{Q}[x]/(g(x))$ – числовое поле.
- $R_g = \mathbb{Z}[x]/(g(x))$ – кольцо целых числового поля K.
- ζ_K – дзета-функция Дедекинда для числового поля K.

Теорема (нижняя оценка успеха алгоритма восстановления секретного ключа)

Пусть

- $SK = (\Lambda_1, \Lambda_2, \dots, \Lambda_k)$ – закрытый ключ.
- $\mathfrak{a} \leq R_g, \mathfrak{a}$ – идеал,
- $I = (x) \subseteq R_g$, $P(I \leq \mathfrak{a}) = \left|\mathrm{R_g}/\mathfrak{a}\right|^{-1}$.

Тогда вероятность того, что $\Lambda_1, \Lambda_2, \dots, \Lambda_k$ будут уязвимы:

$$P(SK) \geq \zeta_{\mathrm{K}}(\mathrm{k})^{-\mathrm{k}}.$$

Экспериментальная проверка

- SageMath.
- Коэффициентом случайного многочлена является целое число, которое выбирается случайно, независимо и равновероятно из $\{-10^9, \dots, 10^9 + 1\}$.
- Функция генерации randint.
- Проводится 10^4 независимых генераций секретного ключа длины k с уровнем доверия $0{,}95$ с точностью до 2 знаков.

Результаты эксперимента

- Результаты при $R_g = \mathbb{Z}[x]/(x^4 - 2x^3 - x^2 + 4x + 1)$:

k	$P_{\text{теор}}(\Lambda_i)$	$P_{\text{практ}}(\Lambda_i)$	$P_{\text{теор}}(\mathbf{SK})$	$P_{\text{практ}}(\mathbf{SK})$
2	0,77	0,81	0,59	0,65
3	0,94	0,96	0,82	0,89
4	0,98	0,99	0,93	0,96
5	0,995	0,998	0,97	0,99

Результаты эксперимента

- Результаты при $R_g = \mathbb{Z}[x]/(x^2 + 1)$:

k	$P_{\text{теор}}(\Lambda_i)$	$P_{\text{практ}}(\Lambda_i)$	$P_{\text{теор}}(\mathbf{SK})$	$P_{\text{практ}}(\mathbf{SK})$
2	0,66	0,74	0,44	0,55
3	0,86	0,92	0,63	0,79
4	0,93	0,97	0,76	0,89
5	0,97	0,99	0,85	0,94

Результаты эксперимента

- Результаты при $R_g = \mathbb{Z}[x]/(x^3 - 49x^2 + 50x - 66)$:

k	$P_{\text{теор}}(\Lambda_i)$	$P_{\text{практ}}(\Lambda_i)$	$P_{\text{теор}}(\mathbf{SK})$	$P_{\text{практ}}(\mathbf{SK})$
2	0,44	0,55	0,19	0,31
3	0,73	0,84	0,38	0,71
4	0,87	0,94	0,56	0, 79
5	0,93	0,98	0,71	0, 88

Результаты эксперимента

- Результаты при $R_g = \mathbb{Z}[x]/((x^2 - 11x - 32)(x^2 + x - 8)(x^2 + 19x - 1))$:

k	$P_{\text{практ}}(\mathbf{SK})$	$P_{\text{практ}}(\Lambda_i)$
2	0,59	0,65
3	0,82	0,89
4	0,93	0,96
5	0,97	0,99

РусКрипто
XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Спасибо за внимание!

Коновалов Александр,
студент НИЯУ МИФИ
ytka.kek@yandex.ru

Описание шифрсистемы UFHE-ILC

- Функция зашифрования $E_{PK}: \mathcal{P} \to \mathbb{Z}^n$ такая, что $\forall u = (u_1, u_2, \dots, u_k) \in \mathcal{P}$ шифртекст определяется как

$$\mathrm{c} = \theta(\mathrm{u}_1) \otimes \mathrm{A}_1 + \theta(\mathrm{u}_2) \otimes \mathrm{A}_2 + \cdots + \theta(\mathrm{u}_\mathrm{k}) \otimes \mathrm{A}_\mathrm{k}.$$

- Функция расшифрования $\mathrm{D}_{\mathrm{SK}}: \mathrm{c} \mapsto \left(\mathrm{D}_{\Lambda_1}(\mathrm{c}), \dots, \mathrm{D}_{\Lambda_\mathrm{k}}(\mathrm{c})\right)$, где $\forall i \in \{1, \dots, k\}$:

$$\mathrm{D}_{\Lambda_i}(\mathrm{c}) = c - \sum_{j=1}^{n} k_j \, \beta_j,$$

где $k_n = \left\lceil \frac{c \cdot \beta_n^*}{\beta_n^* \cdot \beta_n^*} \right\rceil$, $\forall j \in \{n-1, \dots, 1\}$: $k_j = \left\lceil \frac{\left(c - \sum_{l=j+1}^{n} k_l \beta_l\right) \cdot \beta_j^*}{\beta_j^* \cdot \beta_j^*} \right\rceil$,

при этом $\mathrm{B} = [\beta_1, \beta_2, \dots, \beta_\mathrm{n}]$ – эрмитова нормальная форма Λ_i, $\mathrm{B}^* = [\beta_1^*, \beta_2^*, \dots, \beta_\mathrm{n}^*]$ – ортогональная форма Λ_i.