Новосибирский государственный университет
Лаборатория современных компьютерных технологий

# Применение гомоморфного шифрования для построения криптосистемы с открытым ключом

Егорова Вера Владимировна

Чечулина Дарья Константиновна

Научный руководитель: Кренделев Сергей Федорович

Работа выполнена при финансовой поддержке Минобрнауки РФ (договор № 02.G25.31.0054).

# Защищенная база данных

## Проблема

Обеспечение безопасности информации, которая хранится в удаленной базе данных.

## Решение

- Шифрование данных.
- Использование гомоморфного шифрования для выполнения операций над зашифрованными данными.

# Гомоморфное шифрование
## Общий принцип

$\overline{k} = (k_1, \ldots, k_n)$ - секретный вектор

$m \in \mathbb{Z}$ - модуль

$p < m$ - исходное число

Гомоморфное шифрование сопоставляет числу $p$ вектор $\overline{c}$ :

$$(\overline{c}, \overline{k})\ mod\ m = p$$

Будем шифровать числа размера $t$ бит.

Выберем модуль $m > 2^t$.

Сгенерируем

- матрицу $W$ размера $n \times n$, обратимую по модулю $m$
- вектор $\overline{u} \in \mathbb{Z}^n$, $u_i < m$.

Найдем вектор $\overline{k}$ из системы линейных уравнений:

$$(W \cdot \overline{k}) \; mod \; m = \overline{u}$$

**Секретный ключ** - $\langle m, \overline{k}, W, \overline{u} \rangle$

Шифротекст $\overline{c}$ строится как линейная комбинация любых $s$ строк $\overline{w_1}, \ldots \overline{w_s}$ матрицы $W, s = 2, \ldots, n$:

$$\overline{c} = \sum_{i=1}^{s} \alpha_i \overline{w_i}$$

Коэффициенты $\alpha_i$ найдем из диофантова уравнения:

$$u_1\alpha_1 + \cdots + u_s\alpha_s = p$$

$\overline{a} = (a_1, \ldots, a_n)$ и $\overline{b} = (b_1, \ldots, b_n)$ - шифротексты

**Проблема**

Рост размерности данных при покомпонентном умножении:

$$\overline{a} \cdot \overline{b} = (a_1 b_1, a_1 b_2, \ldots, a_n b_n) \in \mathbb{Z}^{n^2}$$

**Решение**

Использование таблицы умножения - матрицы $(\gamma_{ijk})$ :

$$c_k = \sum_i \sum_j a_i \cdot b_j \cdot \gamma_{ijk}$$

# Применение гомоморфного шифрования

Криптосистемы с открытым ключом:

- линейная
- полиномиальная

**Открытый ключ**

$$\langle \overline{w}_1, \ldots, \overline{w}_s, u_1, \ldots, u_s, (\gamma_{ijk}) \rangle :$$

$$(\overline{w}_i, \overline{k}) \ mod \ m = u_i$$

$(\gamma_{ijk})$ - таблица умножения

Будем рассматривать случай при $s = 2$.

# Генерация ключей
## Пример

$t = 8$ бит, $m = 659$

$$\overbrace{\begin{pmatrix} 12 & 6 & 14 & 9 \\ 120 & 72 & 155 & 95 \\ 528 & 313 & 184 & 42 \\ 373 & 122 & 473 & 103 \end{pmatrix}}^{W} \cdot \overbrace{\begin{pmatrix} k_1 \\ k_2 \\ k_3 \\ k_4 \end{pmatrix}}^{\overline{k}} mod\ 659 = \overbrace{\begin{pmatrix} 360 \\ 91 \\ 273 \\ 97 \end{pmatrix}}^{\overline{u}} \Rightarrow$$

$$\overline{k} = \begin{pmatrix} 176 & 657 & 361 & 197 \end{pmatrix}$$

$$\overline{w}_1 = \begin{pmatrix} 12 & 6 & 14 & 9 \end{pmatrix} \qquad u_1 = 360$$

$$\overline{w}_2 = \begin{pmatrix} 120 & 72 & 155 & 95 \end{pmatrix} \qquad u_2 = 91$$

$m, \overline{k}$ - компоненты секретного ключа

$\overline{w}_1, \overline{w}_2, u_1, u_2$ - компоненты открытого ключа

# Линейная криптосистема с открытым ключом

Шифр Хилла:

$\overline{p} \in \mathbb{Z}$ - вектор исходных данных

$m$ - модуль

$A$ - секретная матрица, обратимая по модулю $m$

Шифрование - это нахождение вектора $\overline{c}$:

$$\overline{c} = (A \cdot \overline{p}) \ mod \ m$$

**Проблема**

Уязвимость к атаке с открытым текстом

**Решение**

Применить к матрице $A$ гомоморфное шифрование

## Секретный ключ

$m, \overline{k}$ - компоненты секретного ключа гомоморфного шифрования

$A$ - квадратная матрица, обратимая по модулю $m$

$$m = 659$$

$$\overline{k} = \begin{pmatrix} 176 & 657 & 361 & 197 \end{pmatrix}$$

$$A = \begin{pmatrix} 3 & 57 & 18 & 144 \\ 18 & 386 & 284 & 69 \\ 34 & 8 & 311 & 455 \\ 43 & 160 & 282 & 12 \end{pmatrix}$$

## Открытый ключ

$\overline{w}_1, \overline{w}_2, u_1, u_2$ - компоненты ключа гомоморфного шифрования

$(\gamma_{ijk})$ - таблица умножения

$Hom(A)$ - зашифрованная матрица $A$

$\boldsymbol{Hom(A)}$ :

$$\overline{h}_{11} = \begin{pmatrix} 6073548 & 5247570 & 9849301 & 547632 \end{pmatrix} \xleftarrow{Hom} a_{11} = 3$$

$$\dots$$

$$\overline{h}_{44} = \begin{pmatrix} 9981384 & 8623956 & 16186528 & 8999898 \end{pmatrix} \xleftarrow{Hom} a_{44} = 12$$

$\boldsymbol{(\gamma_{ijk})}$ :

$$\overline{\gamma}_{11} = \begin{pmatrix} 319 & 77 & 626 & 452 \end{pmatrix} \dots \overline{\gamma}_{44} = \begin{pmatrix} 432 & 103 & 198 & 222 \end{pmatrix}$$

Размер открытого ключа - **5 Кбайт**

# Линейная криптосистема с открытым ключом
## Шифрование

Входные данные:

вектор целых чисел $\overline{p} = (p_1, \ldots, p_n) = \begin{pmatrix} 222 & 11 & 92 & 79 \end{pmatrix}$

1. $(p_1, \ldots, p_n) \xrightarrow{Hom} (\overline{c}_1, \ldots, \overline{c}_n) : (\overline{c}_i, \overline{k}) \ mod \ m = p_i$

   $222 \rightarrow \begin{pmatrix} 42744540 & 25757574 & 55350260 & 33885615 \end{pmatrix}$

   $\ldots$

   $79 \rightarrow \begin{pmatrix} 19578936 & 11798136 & 25352927 & 15521147 \end{pmatrix}$

2. $Z = Hom(A) \cdot (\overline{c}_1, \ldots, \overline{c}_n)^T$

$$\overline{Z}_1 = \begin{pmatrix} 106689069808955665 \\ 87946701861781 3808 \\ 61229189033368 5097 \\ 99416190846239 1361 \end{pmatrix}$$

Вектор шифротекстов $Z$ - результат шифрования.

# Линейная криптосистема с открытым ключом
## Дешифрование

1. $$Z \cdot \overline{k} = \left( Hom(A) \cdot (\overline{c}_1, \ldots, \overline{c}_n)^T \right) \cdot \overline{k} = A \cdot \overline{p}$$

$$Z \cdot \overline{k} = \begin{pmatrix} 1129139547398338548908 2 \\ 2267449503725240830331 2 \\ 1912188171774568701561 0 \\ 2694998090416401563593 7 \end{pmatrix}$$

2. $$A^{-1} \cdot (Z \cdot \overline{k}) = \left( A^{-1} \cdot A \cdot \overline{p} \right) \ mod\ m = \overline{p}$$

$$\underbrace{\begin{pmatrix} 18 & 566 & 606 & 616 \\ 139 & 111 & 276 & 262 \\ 88 & 377 & 221 & 259 \\ 78 & 373 & 158 & 20 \end{pmatrix}}_{A^{-1}} \cdot \underbrace{\begin{pmatrix} 1129139547398338548908 2 \\ 2267449503725240830331 2 \\ 1912188171774568701561 0 \\ 2694998090416401563593 7 \end{pmatrix}}_{A \cdot \overline{p}} = \underbrace{\begin{pmatrix} 222 \\ 11 \\ 92 \\ 79 \end{pmatrix}}_{\overline{p}}$$

# Полиномиальная криптосистема с открытым ключом

RSA как криптосистема с секретным ключом:

$p \in \mathbb{Z}$ - исходное число

$m$ - модуль

$e, d$ такие, что $d = e^{-1}\ mod\ \phi(m)$

$\langle m, e, d \rangle$ - секретный ключ

Шифрование - это вычисление $p^e\ mod\ m$

**Основная идея**

Предварительно шифровать число $p$ с помощью гомоморфного шифрования

# Полиномиальная криптосистема с открытым ключом

## Генерация ключей

### Секретный ключ

$m, \overline{k}$ - компоненты секретного ключа гомоморфного шифрования

$m = 659,\ \overline{k} = \begin{pmatrix} 176 & 657 & 361 & 197 \end{pmatrix}$

### Открытый ключ

$\overline{w}_1, \overline{w}_2, u_1, u_2$ - компоненты ключа гомоморфного шифрования

$(\gamma_{ijk})$ - таблица умножения

$e$ - целое число, обратимое по модулю $\phi(m)$

$e = 3$

Размер открытого ключа - **2.5 Кбайта**

# Полиномиальная криптосистема с открытым ключом

## Шифрование

Входные данные: целое число $p = 123$

1. $p \xrightarrow{Hom} \overline{c} : (\overline{c}, \overline{k})\ mod\ m = p$

$$123 \rightarrow \begin{pmatrix} 27458280 \\ 16546176 \\ 35555955 \\ 21767475 \end{pmatrix}$$

2. $\overline{z} = (\overline{c})^e$

$$\overline{z} = \begin{pmatrix} 27458280 \\ 16546176 \\ 35555955 \\ 21767475 \end{pmatrix}^3 = \begin{pmatrix} 36089738652615602480506715 4756 \\ 47701913342338791292243880 9475 \\ 48878241412317922609899337 2132 \\ 52290066725950464160784392 0158 \end{pmatrix}$$

Вектор $\overline{z}$ - результат шифрования.

# Полиномиальная криптосистема с открытым ключом

## Дешифрование

1. $(\overline{z}, \overline{k})\ mod\ m = \left((\overline{c})^e, \overline{k}\right)\ mod\ m = p^e (mod\ m)$

$$\begin{pmatrix} 360897386526156024805067154756 \\ 477019133423387912922438809475 \\ 488782414123179226098993372132 \\ 522900667259504641607843920158 \end{pmatrix} \cdot \begin{pmatrix} 176 \\ 657 \\ 361 \\ 197 \end{pmatrix}\ mod\ 659 = 510$$

2. $\left(p^e\ mod\ m\right)^d = p^{ed} (mod\ m) = p$

$d = e^{-1}\ mod\ \phi(m)$

$$d = 3^{-1}\ mod\ 658 = 439$$

$$510^{439}\ mod\ 659 = 123$$

Спасибо за внимание!