Полностью гомоморфное шифрование на основе матричных полиномов с возможностью SIMD-операций

Ф. Б. Буртыка

Южный Федеральный Университет

4 декабря 2014 г.

План работы

- Введение в гомоморфное шифрование
- Полностью гомоморфное шифрование на матричных полиномах
- Полностью гомоморфное шифрование на основе матричных полиномов с возможностью пакетной обработки.

Гомоморфное шифрование

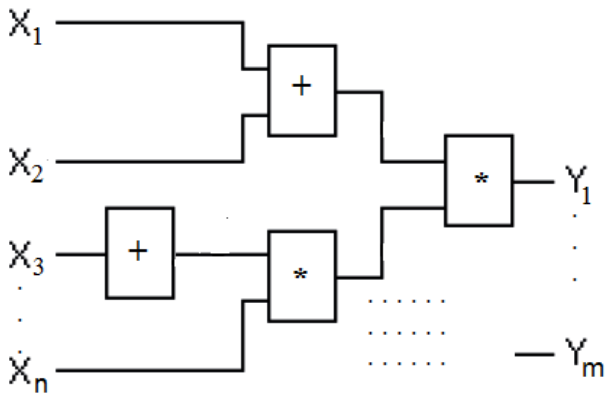
Гомоморфная схема шифрования (ГСШ) *– это криптосистема, позволяющая проводить некоторые вычисления над данными в зашифрованном виде с последующей возможностью извлечения результата вычислений над соответствующими открытыми текстами с помощью секретного ключа.*

Существует два основных типа ГСШ:

- *Полностью гомоморфные схемы шифрования (ПГСШ)* – криптосистемы, позволяющие эффективно проводить вычисление любой функции гомоморфно.
- *Частично гомоморфные схемы шифрования (ЧГСШ)* – криптосистемы, разрешающие эффективное вычисление некоторых функций (но не всех возможных) гомоморфно.

Модель программы вычисляемой над данными

- Полагаем, что исходные данные являются элементами кольца $\mathcal{M}$ с операциями $+, *$.
- Программа $\mathbb{P}$, вычисляемая над данными, представляет собой *комбинационную схему (арифметическую схему)* $\mathbb{F}(x_1, ..., x_n) = \{y_1, ..., y_m\}$ (здесь $x_1, ..., x_n$ – **входы** $\mathbb{F}$, $y_1, ..., y_m$ – **выходы** $\mathbb{F}$:



- Ясно, что $\mathbb{F}$ можно сопоставить набор полиномов $\mathbf{f_1}(x_1, ..., x_n), ..., \mathbf{f_m}(x_1, ..., x_n) \in \mathcal{M}[x_1, ..., x_n]$, вычисление которых эквивалентно вычислению $\mathbb{F}$.

$$\mathbf{f_j}(x_1, ..., x_n) = \sum_{\{i_1,...,i_t\} \in \{1,...,n\}} f^j_{i_1,...,i_t} * x_{i_1} * ... * x_{i_k}$$

Гомоморфное шифрование (уточнение определения)

Пусть для криптосистемы $\mathfrak{K}$: Исходные данные – кольцо $\mathcal{M}$ с операциями $+_M, *_M$, пространство шифртекстов – кольцо $\mathcal{C}$ с операциями $+_C, *_C$, E, D – функции зашифрования и расшифрования.

- $\mathfrak{K}$ *является* ***частично гомоморфной****, если выполняется хотя бы одно из свойств:*

$$D(E(x) +_C E(y)) = x +_M y, \quad (1)$$
$$D(E(x) *_C E(y)) = x *_M y. \quad (2)$$

- $\mathfrak{K}$ *является* ***полностью гомоморфной****, если:*

  1) выполняется (1), (2) и $+_C, *_C$ можно вычислять в неограниченном количестве над шифровками.

  2) $+_C, *_C$ должны быть вычислительно эффективны. В частности размеры шифровок после применения к ним $+_C, *_C$ должны быть ограничены сверху полиномом.

Проблемы существующих гомоморфных схем шифрования (ГСШ)

- Существует много различных ЧГСШ (Например: криптосистемы RSA, Пэйе, Голдвассер-Микали, Эль-Гамаля). Однако на практике их можно применять только для специальных приложений.
- Также сейчас разработано много ПГСШ (криптосистемы типа Джентри). Теоретически их можно назвать вычислительно эффективными. Однако в общем на практике они оказываются не очень неэффективными, поскольку для достижения высокого уровня криптойстокости размеры шифровок должны быть достаточно большими ($\approx 10^6$ битов). За счет этого вычисление над шифртекстами сильно замедляется по сравнению с вычислениями над открытыми текстами.

Организация безопасных облачных вычислений

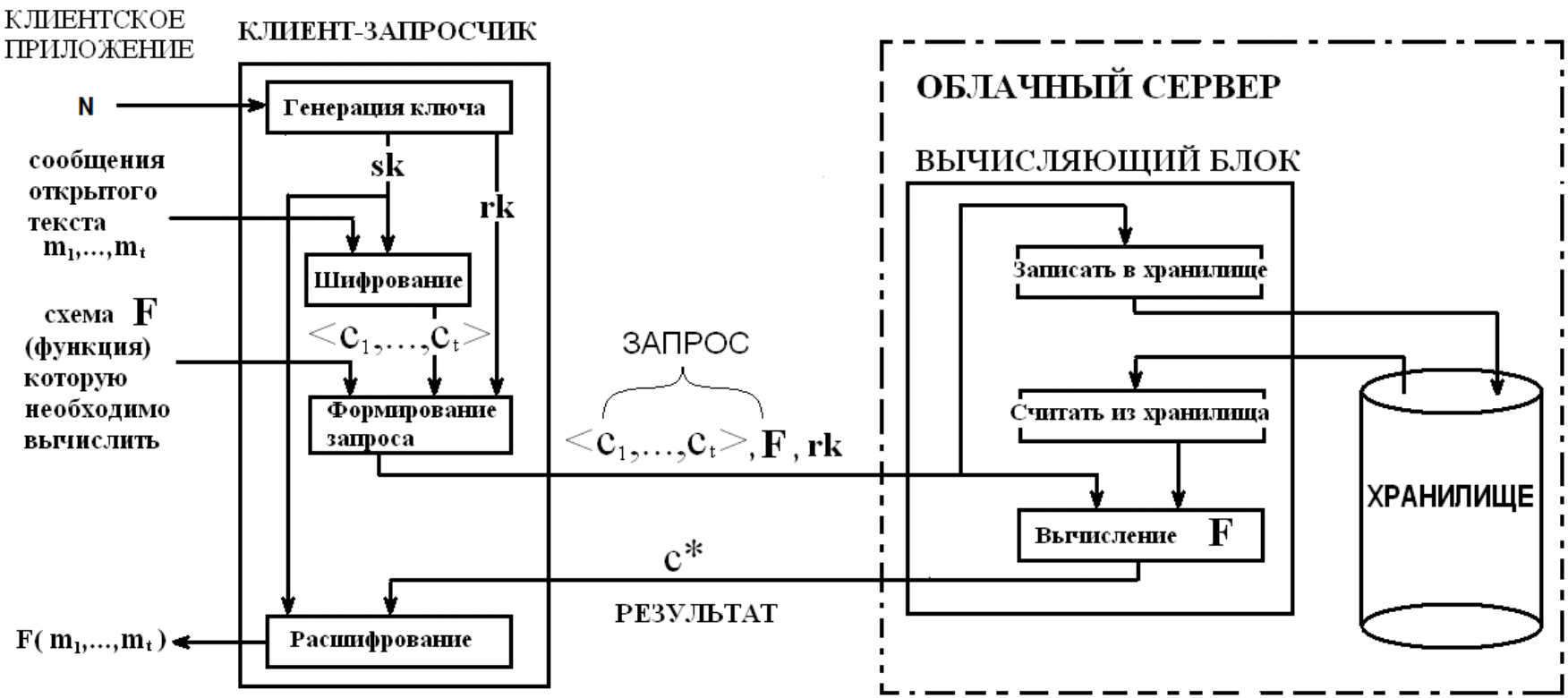


Рис. : Общая архитектура защищённых облачных вычислений

Матричные уравнения и матричные полиномы

- Матричный полином $\mathbf{F}(X) \in \mathbf{R}^{N \times N}[X]$ от переменной X представляет собой следующее:

$$\mathbf{F}(X) = \mathbf{F}_n \cdot X^n + \mathbf{F}_{n-1} \cdot X^{n-1} + \cdots + \mathbf{F}_2 \cdot X^2 + \mathbf{F}_1 \cdot X + \mathbf{F}_0,$$

$$\mathbf{F}_i = \begin{pmatrix} (f_i)_{1,1} & (f_i)_{1,2} & \cdots & (f_i)_{1,N} \\ (f_i)_{2,1} & (f_i)_{2,2} & \cdots & (f_i)_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ (f_i)_{N,1} & (f_i)_{N,2} & \cdots & (f_i)_{N,N} \end{pmatrix}, \; X = \begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,N} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ x_{N,1} & x_{N,2} & \cdots & x_{N,N} \end{pmatrix}$$

  Здесь $(f_i)_{j,k}, x_{j,k}$ принадлежат некоторому кольцу $\mathbf{R}$

- Матричное уравнение: $\mathbf{F}(X) = \mathbf{0}$, где $\mathbf{0}$ – нулевая матрица размера $N \times N$

Арифметические операции над матричными полиномами

Пусть даны $\mathbf{A} = \mathbf{A}_n \cdot X^n + \cdots + \mathbf{A}_1 \cdot X + \mathbf{A}_0$ и $\mathbf{B} = \mathbf{B}_n \cdot X^n + \cdots + \mathbf{B}_1 \cdot X + \mathbf{B}_0$, $\mathbf{A}_i, \mathbf{B}_i \in \mathbf{R}^{N \times N}$, $\mathbf{R}$ – кольцо.

- **Сумма:**

  $$\mathbf{A}(X) + \mathbf{B}(X) = (\mathbf{A}_n + \mathbf{B}_n) \cdot X^n + \cdots + (\mathbf{A}_1 + \mathbf{B}_1) \cdot X + (\mathbf{A}_0 + \mathbf{B}_0)$$

- **Произведение:**

  $$\mathbf{A}(X) \cdot \mathbf{B}(X) = \mathbf{C}(X) = \mathbf{C}_{2 \cdot n} \cdot X^{2 \cdot n} + \cdots + \mathbf{C}_1 \cdot X + \mathbf{C}_0$$

  Здесь $\mathbf{C}_k = \sum_{i+j=k} \mathbf{A}_i \cdot \mathbf{B}_j$, $k = 0, 1, 2, ..., 2 \cdot n$.

- **Деление:** Пусть $\mathbf{A}(X), \mathbf{B}(X) \in \mathbf{R}^{N \times N}[X]$, $n = deg(\mathbf{A}) \geq m = deg(\mathbf{B})$, коэффициент $\mathbf{B}_m$ – обратимая матрица. Тогда представление

  $$\mathbf{A}(X) = \mathbf{Q}(X) \cdot \mathbf{B}(X) + \mathbf{D}(X)$$

  такое, что $deg(\mathbf{B}(X)) > deg(\mathbf{D}(X))$ определено и единственно.

Симметричная ПГСШ на матричных полиномах

$N \in \mathbb{Z}_+$ – основной параметр криптосистемы, фиксируемый заранее

Пространство открытых текстов – $\mathbb{Z}_p$,

Пространство шифртекстов – $\subset \mathbb{Z}_p^{N\times N}[X]$, где $X \in \mathbb{Z}_p^{N\times N}$, p – простое число

Секретный ключ – $(K_0, \vec{k}) \in \mathbb{Z}_p^{N\times N} \times \mathbb{Z}_p^N$.

Шифрование:

- $m \in \mathbb{Z}_p \Longrightarrow \mathbf{M} \in \mathbb{Z}_p^{N\times N}$, где $\mathbf{M} \cdot \vec{k} = m \cdot \vec{k}$.
- $C(X) = R(X) \cdot (X - K_0) + \mathbf{M}$, где $R(X) = R^d \cdot X^d + ... + R_0$ – случайный полином из $\mathbb{Z}_p^{N\times N}[X]$, $d \in \{1, ..., N-2\}$ – случайная величина.

  Тогда $deg(C(X)) \in \{2, ..., N-1\}$.

Расшифрование:

- $\mathbf{M} \Longleftarrow C(K_0)$
- $m \Longleftarrow (\mathbf{M} \cdot \vec{k})_i \cdot k_i^{-1}$

Генерация матрицы, коммутирующей с заданной

Запишем матричное уравнение $\mathbf{K} \cdot X = X \cdot \mathbf{K}$ как

$$\begin{pmatrix} k_{11} & .. & k_{1N} \\ \vdots & .. & \vdots \\ k_{N1} & .. & k_{NN} \end{pmatrix} \cdot \begin{pmatrix} x_{11} & .. & x_{1N} \\ \vdots & .. & \vdots \\ x_{N1} & .. & x_{NN} \end{pmatrix} = \begin{pmatrix} x_{11} & .. & x_{1N} \\ \vdots & .. & \vdots \\ x_{N1} & .. & x_{NN} \end{pmatrix} \cdot \begin{pmatrix} k_{11} & .. & k_{1N} \\ \vdots & .. & \vdots \\ k_{N1} & .. & k_{NN} \end{pmatrix}$$

а затем в виде системы линейных уравнений:

$$\begin{cases} k_{11} \cdot x_{11} + ... + k_{1N} \cdot x_{N1} = k_{11} \cdot x_{11} + ... + x_{1N} \cdot k_{N1}, \\ \dots \\ k_{N1} \cdot x_{1N} + ... + k_{NN} \cdot x_{NN} = k_{1N} \cdot x_{N1} + ... + x_{NN} \cdot k_{NN}. \end{cases} \quad (1)$$

Заметим, что эта система всегда имеет решения, поскольку, например единичная и нулевая матрицы всегда в коммутанте. Записав ФСР этой системы и придавая свободным переменным различные значения будем получать различные матрицы коммутирующие с данной.

Гомоморфные свойства криптосистемы на матричных полиномах

Пусть есть шифртексты
$C_1(X) = R_1(X)\cdot(X - K_0) + \mathbf{M_1}$, $C_2(X) = R_2(X)\cdot(X - K_0) + \mathbf{M_2}$
шифрующие $m_1, m_2 \in \mathbb{Z}_p$.

$C_1(X), C_2(X) \in \mathbb{Z}_p^{N\times N}[X]$, $deg(C_1), deg(C_2) \in \{2, ..., N-1\}$

- **Аддитивный гомоморфизм:** полином $C_1(X) + C_2(X)$ шифрует $m_1 + m_2 \in \mathbb{Z}_p$.
- **Мультипликативный гомоморфизм:** полиномы $C_1(X) \cdot C_2(X)$ и $C_2(X) \cdot C_1(X)$ шифруют $m_1 \cdot m_2 \in \mathbb{Z}_p$ если дополнительно наложить условие

$$K_0 \cdot \mathbf{M_i} = \mathbf{M_i} \cdot K_0, i = 1, 2.$$

Доказательство корректности гомоморфных свойств

Пусть $C_1(X) = R_1(X) \cdot (X - K_0) + \mathbf{M_1}$, $C_2(X) = R_2(X) \cdot (X - K_0) + \mathbf{M_2}$.

- $C_1(X) + C_2(X) = \Big(R_1(X) + R_2(X)\Big) \cdot (X - K_0) + \mathbf{M}_1 + \mathbf{M}_2$ является корректным шифртекстом (шифртекстом правильной формы) и после расшифрования дает $m_1 + m_2$ поскольку $(\mathbf{M}_1 + \mathbf{M}_2) \cdot \vec{k} = \mathbf{M}_1 \cdot \vec{k} + \mathbf{M}_2 \cdot \vec{k} = (m_1 + m_2) \cdot \vec{k}$.
- $C_1(X) \cdot C_2(X) =$

$$= \Big(R_1(X) \cdot (X - K_0) \cdot R_2(X) + R_1(X) \cdot \mathbf{M}_2 + \mathbf{M}_1 \cdot R_2(X)\Big) \cdot (X - K_0) + \mathbf{M}_1 \cdot \mathbf{M}_2$$

(благодаря коммутативности $\mathbf{M}_1 \cdot (X - K_0) = (X - K_0) \cdot \mathbf{M}_1$) является корректным шифртекстом и после расшифрования дает $m_1 \cdot m_2$, поскольку $(\mathbf{M}_1 \cdot \mathbf{M}_2) \cdot \vec{k} = m_1 \cdot m_2 \cdot \vec{k}$ если $\mathbf{M}_1 \cdot \vec{k} = m_1 \cdot \vec{k}$ и $\mathbf{M}_2 \cdot \vec{k} = m_2 \cdot \vec{k}$.

Компактность ПГШ на основе матричных полиномов

- Отметим, что при умножении шифртекстов $C_1(X) = R_1(X) \cdot (X - K_0) + \mathbf{M_1}$, $C_2(X) = R_2(X) \cdot (X - K_0) + \mathbf{M_2}$ их размеры неограниченно и быстро возрастают.
- Для того, чтобы ограничить рост размеров шифртекстов в процессе вычислений вводится **ключ перешифрования**:

$$\mathbf{RK} = R_0(X) \cdot (X - K_0) \in \mathbb{Z}_p^{N \times N}[X]$$ (по сути он является шифровкой нуля)

$deg(\mathbf{RK}) = N$

После вычисления $C_1(X) \cdot C_2(X)$ или $C_2(X) \cdot C_1(X)$ можно привести произведение по модулю **RK**.

- Нетрудно показать, что такое преобразование не повлияет на зашифрованный в произведении открытый текст $m_1 \cdot m_2$. Однако теперь размеры шифртекстов всегда будут оставаться ограниченными заданной величиной.

Дополнительные гомоморфные свойства криптосистемы на матричных полиномах

Пусть есть $C(X) = R(X) \cdot (X - K_0) + \mathbf{M} \in \mathbb{Z}_p^{N \times N}[X]$ шифрующий $m \in \mathbb{Z}_p$, константа $\lambda \in \mathbb{Z}_p$.

- **Гомоморфное умножение на константу:** $diag(\lambda) \cdot C(X)$ и $C(X) \cdot diag(\lambda)$ шифруют $\lambda \cdot m \in \mathbb{Z}_p$, где $diag(\lambda) \in \mathbb{Z}_p^{N \times N}$ – диагональная матрица, у которой все диагональные элементы равны λ.
- **Гомоморфное сложение с константой:** $C(X) + diag(\lambda)$ шифрует $\lambda + m$.

Вычислительные издержки гомоморфного вычисления

Пусть есть
$C_1(X) = R_1(X) \cdot (X - K_0) + \mathbf{M_1}$, $C_2(X) = R_2(X) \cdot (X - K_0) + \mathbf{M_2}$
шифрующие $m_1, m_2 \in \mathbb{Z}_p$.

При гомоморфном вычислении:

- **Сумма:** вместо $m_1 + m_2 \bmod p$ нужно вычислять $C_1(X) + C_2(X)$.

  $C_1(X) + C_2(X)$ можно вычислить за $\mathbf{O(N^3)}$ арифрметических операций в $\mathbb{Z}_p$ (при последовательной реализации).

- **Произведение:** вместо $m_1 \cdot m_2 \bmod p$ нужно вычислять $(C_1(X) \cdot C_2(X)) \bmod \mathbf{RK}$

  $(C_1(X) \cdot C_2(X)) \bmod \mathbf{RK}$ можно вычислить за $\mathbf{O(N^{4.746})}$ арифрметических операций в $\mathbb{Z}_p$ (при последовательной реализации).

Вычислительные издержки гомоморфного умножения (обоснование)

Пусть есть $C_1(X), C_2(X) \in \mathbb{Z}_p^{N\times N}[X]$ шифрующие $m_1, m_2 \in \mathbb{Z}_p$.

$deg(C_1(X)), C_2(X)) < N$

Оценим сложность вычисления $(C_1(X) \cdot C_2(X))$ mod **RK**:

- При гомоморфном вычислении каждый функциональный элемент умножения заменяется на умножение матричных полиномов с последующим приведением по модулю матричного полинома.
- Для вычисления $(C_1(X) \cdot C_2(X))$ mod **RK** необходимо произвести не более чем $\mathbf{O(N^2)}$ операций с матрицами.
- Для умножения двух $N \times N$ матриц с использованием алгоритма типа Штрассена необходимо $\mathbf{N^{2.373}}$ арифметических операций в $\mathbb{Z}_p$.

Итак, общая сложность ограничена сверху величиной $\mathbf{N^{2.373} \cdot O(N^2) = O(N^{4.746})}$.

Количественные характеристики

при $N = 12$**.** (здесь для $\mathbb{Z}_2$):

- **Размер секретного ключа** $= 156$ битов.
- **Размер шифртекста** ≤ 1728 битов.
- **Время генерации ключа** $= 830$ мсек.
- **Время зашифрования** $= 140$ мсек.
- **Время расшифрования** $= 49$ мсек.
- **Время гомоморфного сложения** $= 2$ мсек.
- **Время гомоморфного умножения** $= 50$ мсек.

ПГСШ на матричных полиномах с механизмом SIMD (Single Instruction Multiple Data)

$d, N \in \mathbb{Z}_+$ – параметры криптосистемы.

Дан набор открытых текстов $\{m_i \in \mathbb{Z}_p, i = \overline{0, d-1}\}$.

Секретный ключ – $(K_0, .., , K_{d-1}, \vec{k_0}, ..., \vec{k_{d-1}})$, где $K_i \in \mathbb{Z}_p^{N \times N}$, $\vec{k_i} \in \mathbb{Z}_p^N$.

Шифрование: Вычислятся $C(X) \in \mathbb{Z}_p^{N \times N}[X]$,
$deg(C(X)) \leq N + d - 1$, такой что:

$C(K_i) = \mathbf{M_i}$, где $\mathbf{M_i} \cdot \vec{k_i} = m_i \cdot \vec{k_i}, i = \overline{0, d-1}$

Расшифрование: Для извлечения m_i из $C(X)$ нужно:

- $\mathbf{M_i} \Longleftarrow C(K_i)$
- $m_i \Longleftarrow (\mathbf{M_i} \cdot \vec{k_i})_j \cdot (k_i)_j^{-1}$

Итого: В один полином шифртекст $C(X)$ упаковано сразу несколько открытых текстов $m_i, i = \overline{0, d-1}$, каждому из которых соответствует свой секретный ключ $(K_i, \vec{k_i}), i = \overline{0, d-1}$.

Интерполяция матричных полиномов

Теорема

Для заданных m пар матриц $(\mathbf{X}_i, \mathbf{Y}_i),\ i = 1, ..., m$ существует матричный полином $\mathbf{A}(X) = \mathbf{A}_m \cdot X^m + \mathbf{A}_{m-1} \cdot X^{m-1} + ... + \mathbf{A_1} \cdot X + \mathbf{A_0}$ такой что $A(\mathbf{X}_i) = \mathbf{Y}_i,\ i = 1, ..., m$ в случае если блочно-матричная система линейных уравнений

$$(\mathbf{A}_1, \mathbf{A}_2, ..., \mathbf{A}_m) \cdot \begin{pmatrix} \mathbf{I} & \mathbf{I} & \cdots & \mathbf{I} \\ X_1 & X_2 & \cdots & X_m \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{m-1} & X_2^{m-1} & \cdots & X_m^{m-1} \end{pmatrix} = (\mathbf{Y}_1, \mathbf{Y}_2, ..., \mathbf{Y}_m)$$

имеет решение.

ПГСШ на матричных полиномах с механизмом SIMD (Single Instruction Multiple Data)

Пусть $\mathbf{RK}(X) \in \mathbb{Z}_p^{N\times N}[X]$, $deg(\mathbf{RK}(X)) = N + d$ такой, что $\mathbf{RK}(K_i) = \mathbf{0}, i = \overline{0, d-1}$.

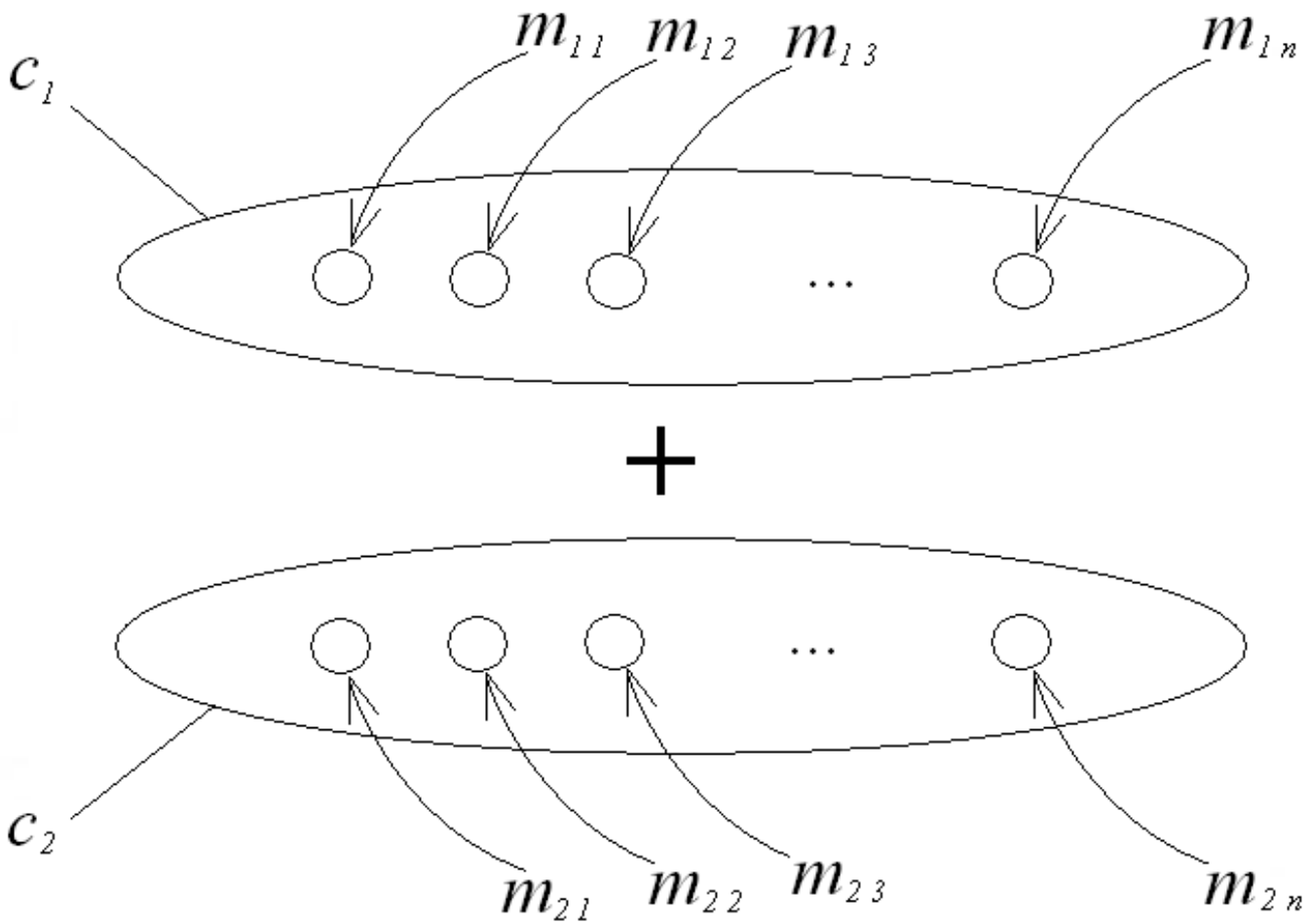
Пусть даны $C_1(X), C_2(X) \in \mathbb{Z}_p^{N\times N}[X]$, $deg(C_j) < N + d, j = 1, 2$, шифрующие наборы открытых текстов $\{m_i^1 \in \mathbb{Z}_p, i = \overline{0, d-1}\}$ и $\{m_i^2 \in \mathbb{Z}_p, i = \overline{0, d-1}\}$.

- **Аддитивный гомоморфизм:** $C_1(X) + C_2(X)$ шифрует открытые тексты $\{m_i^1 + m_i^2 \in \mathbb{Z}_p, i = \overline{0, d-1}\}$.
- **Мультипликативный гомоморфизм:** $C_1(X) \cdot C_2(X)$ mod **RK** и $C_2(X) \cdot C_1(X)$ mod **RK** шифруют открытые тексты $\{m_i^1 \cdot m_i^2 \in \mathbb{Z}_p, i = \overline{0, d-1}\}$ если дополнительно потребовать

$$K_i \cdot \mathbf{M_{i,j}} = \mathbf{M_{i,j}} \cdot K_i, i = \overline{0, d-1}, j = 1, 2.$$

Итак теперь одно сложение/умножение шифртекстов соответстсвует одновременному сложению/умножению d пар открытых текстов.

Иллюстрация механизма SIMD (Single Instruction Multiple Data)



Повышение производительности ПГШ за счет механизма SIMD

Пусть есть векторы данных $\{m_i^1 \in \mathbb{Z}_p, i = \overline{0, d-1}\}$ и $\{m_i^2 \in \mathbb{Z}_p, i = \overline{0, d-1}\}$. Нужно гомоморфно вычислить векторы $\vec{m_+} = \{m_i^1 + m_i^2 \in \mathbb{Z}_p, i = \overline{0, d-1}\}$, $\vec{m_*} = \{m_i^1 \cdot m_i^2 \in \mathbb{Z}_p, i = \overline{0, d-1}\}$.

- Если воспользоваться исходным вариантом ПГСШ, то необходимый объем памяти для хранения шифровок $= \mathbf{O(2 \cdot d \cdot N^3 \cdot \log_2(p))}$ битов. Вычисление $\vec{m_+}$ потребует $\mathbf{O(d \cdot N^3)}$ арифметических операций в $\mathbb{Z}_p$. Вычисление $\vec{m_*}$ потребует $\mathbf{O(d \cdot N^{4.746})}$ арифметических операций в $\mathbb{Z}_p$. .
- Если воспользоваться матричная ПГСШ с SIMD механизмом, то необходимый объем памяти для хранения шифровок $= \mathbf{O((N^3 + d \cdot N^2 \cdot \log_2(p))}$ битов. Вычисление $\vec{m_+}$ потребует $\mathbf{O(N^3 + d \cdot N^2))}$ арифметических операций в $\mathbb{Z}_p$. Вычисление $\vec{m_*}$ потребует $\mathbf{O((N + d)^2 \cdot N^{2.746})}$ арифметических операций в $\mathbb{Z}_p$.

Итого: матричная ПГСШ с SIMD механизмом асимптотически эффективнее (например уже при $\mathbf{d = 2, N = 10}$).

Защищенность ПГШ на основе матричных полиномов

- Можно показать, что атаки по шифртекстам, по известным открытым текстам, а также на ключ перешифрования RK сводятся к необходимости решить *полиномиальные системы уравнений от многих переменных* над $\mathbb{Z}_p$.
- При $N \geq 12$ данные системы имеют очень большие размеры и оказываются трудными для решения с помощью таких известных методов, как *вычисление базиса Гребнера, линеаризация, XL метод, SAT решатели*.

Атака на ключ перешифрования

- Предположим, что у криптоаналитика есть только ключ перешифрования:
  $\mathbf{RK}(X) = \mathbf{C}_{N+d} \cdot X^{N+d} + \mathbf{C}_{N+d-1} \cdot X^{N+d-1} + ... + \mathbf{C_1} \cdot X + \mathbf{C_0}$
  $\mathbf{C_i}, X \in \mathbb{Z}_p^{N \times N}, i = 0...N$
- Для матриц из секретного ключа $K_0, ..., K_{d-1}$ справедливо: $\mathbf{RK}(K_i) = \mathbf{0}$.
- Итак, атака на $\mathbf{RK}(X)$ заключается в том, чтобы найти корни матричного уравнения:

  $$\mathbf{C}_{N+d} \cdot X^{N+d} + \mathbf{C}_{N+d-1} \cdot X^{N+d-1} + ... + \mathbf{C_1} \cdot X + \mathbf{C_0} = \mathbf{0}$$

  Количество корней уравнения $\mathbf{RK}(X) = \mathbf{0}$ может достигнуть $C_{N \cdot (N+d)}^{N+d}$. Поэтому после вычисления корней необходимо выбрать среди них правильные K_i $K_0, ..., K_{d-1}$

Атака на ключ перешифрования (сведение к системе скалярных уравнений)

Решение матричного уравнения $\mathbf{C}_{N+d} \cdot X^{N+d} + \mathbf{C}_{N+d-1} \cdot X^{N+d-1} + ... + \mathbf{C}_1 \cdot X + \mathbf{C}_0 = \mathbf{0}$ относительно переменной $X = \{x_{i,j}\}_{i,j=1}^{N}$ с коэффициентами $\mathbf{C_k} = \{c_{i,j}^{k}\}_{i,j=1}^{N}$ эквивалентно поиску корней следующей системы скалярных полиномиальных уравнений над $\mathbb{Z}_p$:

$$\left\{ \sum_{n=1}^{N+d} \sum_{k=1}^{N} c_{i,k}^{n} \cdot (X^n)_{kj} + c_{i,j}^{0} = 0, i = 1..N, j = 1..N \right. \qquad (2)$$

$(X^n)_{kj} = \sum_{k_1,...,k_{n-1}} x_{k,k_1} \cdot x_{k_1,k_2} \cdot ... \cdot x_{k_{n-2},k_{n-1}} \cdot x_{k_{n-1},j}$,

Таким образом, количество неизвестных в этой системе – N^2, уравнений – N^2, общее число различных мономов $\alpha_{RKA} > 1 + N + N^2 + ... + N^{N+d-1} = (N^{N+d} - 1)/(N - 1)$.

Вывод: Уже при небольших N система (2) имеет большие размеры и является сложной для решения такими стандартными методами, как *вычисление базиса Гребнера, линеаризация, XL метод, SAT решатели.*

Атака только по шифртекстам

Пусть есть шифртексты $\{C_i(X)\}, i = 1..t$, где $C_i(X)$ шифрующие набор открытых текстов $\{m_{i,j}\}_{j=1}^{d} \in \mathbb{Z}_p^d$. Ясно, что ключ $K_i, \vec{k_i}, i = 1..d$ и $m_{i,j}$ удовлетворяет системе матричных уравнений:

$$\begin{cases} \mathbf{RK}(X) = \mathbf{0} \\ \mathbf{C_i}(X) \cdot X = X \cdot \mathbf{C_i}(X), i = 1..t \\ \mathbf{C_i}(X) \cdot \vec{y_j} = \lambda_{i,j} \cdot \vec{y_j}, i = 1..t, j = 1..d \end{cases} \quad (3)$$

$X = \{x_{k,l}\}_{k,l=1}^{N}$ – неизвестная матрица; $\vec{y_j} = \{y_{j,i}\}_{i=1}^{N}, j = 1..d$ – неизвестные векторы; $\lambda_{i,j}$ – неизвестные константы из $\mathbb{Z}_p$

Соответвующая система скалярных полиномиальных уравнений после всех преобразований будет содержать $d \cdot (t + N) + N^2$ неизвестных – $x_{i,j}, y_{i,j}, \lambda_{i,j}$, $d \cdot t \cdot N + (t + 1) \cdot N^2$ уравнений, общее число различных мономов $\alpha_{COA} > N \cdot (N^{N+d} - 1)/(N - 1)$.

Атака на основе известных открытых текстов

Пусть есть пары $(\{m_{i,j}\}_{j=1}^{d} \in \mathbb{Z}_p^d, C_i(X)), i = 1..t$. Ясно, что ключ $K_i, \vec{k_i}, i = 1..d$ удовлетворяет системе матричных уравнений:

$$\begin{cases} \mathbf{RK}(X) = \mathbf{0} \\ \mathbf{C_i}(X) \cdot X = X \cdot \mathbf{C_i}(X), i = 1..t \\ \mathbf{C_i}(X) \cdot \vec{y_j} = m_{i,j} \cdot \vec{y_j}, i = 1..t, j = 1..d \end{cases} \quad (4)$$

$X = \{x_{k,l}\}_{k,l=1}^{N}$ – неизвестная матрица; $\vec{y_j} = \{y_{j,i}\}_{i=1}^{N}, j = 1..d$ – неизвестные векторы;

Соответствующая система скалярных полиномиальных уравнений будет содержать $d \cdot N + N^2$ неизвестных – $x_{i,j}, y_{i,j}$, $d \cdot t \cdot N + (t+1) \cdot N^2$ уравнений, общее число различных мономов $\alpha_{KPA} > 2 \cdot N \cdot (N^{N+d} - 1)/(N-1)$.

Вывод: Уже при небольших N система (4) имеет большие размеры и является сложной для решения такими стандартными методами, как *вычисление базиса Гребнера, линеаризация, XL метод, SAT решатели.*

Приложения ПГШ с SIMD механизмом

Разделив базу данных на несколько частей ***Клиент*** *может с помощью* ***Сервера*** *обрабатывать их параллельно (например, вести поиск в них), либо с использованием сетей Бенеша переставлять биты внутри одного шифртекста без расшифрования и даже выполнять операции над числами фиксированной разрядности в битовом представлении. Тогда становится целесообразным использование ПГШ с SIMD механизмом.*

Сравнение с криптосхемами Джентри

В работе [1] предлагается следующий метод шифрования: 1) Вектор данных $(m_1, ..., m_d) \in \mathbb{Z}_p^d$ **кодируется в** $p(x) \in \mathbb{Z}_p[X]$, $deg(p(x)) = d$, **2)** $p(x) \in \mathbb{Z}_p[X] \Rightarrow c(x) \in \mathbb{Z}_q[X]$, **при** $deg(c(x)) = d$.

$\log_2 q = 238$, $d = 7866$, $p = 1000021573$, $\log_2 p \approx 20$, **(для 128 битной криптостойкости)**

Тогда на каждый бит открытого текста приходится $\approx$ **218 битов шифртекста.**

В матричной системе для достижения 144 битной криптостойкости матричный полином шифртекст должен иметь параметр $N = 12$. Если с помошью интерполяции зашифровать в него 11 битов получим, что на каждый бит открытых данных приходится примерно 157 битов шифртекста.

[1] Gentry C., Halevi S., Smart N. P. Fully homomorphic encryption with polylog overhead

Спасибо за внимание!