ГОМОМОРФНОЕ ШИФРОВАНИЕ В КОЛЬЦЕ РАЦИОНАЛЬНЫХ ЧИСЕЛ

Докладывает: **Вишневский Артем Константинович**, КТН, старший преподаватель кафедры защиты информации в системах и комплексах вооружения Военной академии РВСН им. Петра Великого.

Кренделев Сергей Федорович, КФ-МН, доцент НГУ, Jetbrains.

Под полностью гомоморфным шифрованием будем понимать отображение $\varphi: A \to B$ если $\forall x, y \in A$: выполняется сохранение операций:

$$\varphi(x \cdot y) = \varphi(x) \odot \varphi(y),$$
$$\varphi(x + y) = \varphi(x) \oplus \varphi(y),$$

отображение φ – является секретным ключом.

Полностью гомоморфное шифрование – форма шифрования, позволяющая выполнять вычисления с зашифрованными исходными данными и получать зашифрованный результат, который соответствует результату вычисления с открытыми исходными данными.

Из самого определения полностью гомоморфного шифрования можно понять, что разработка эффективных методов полностью гомоморфного шифрования открывает уникальные возможности в построении новых моделей вычислений, которые позволят решать до настоящего времени не решенные прикладные задачи разных отраслевых направлений.

Рассмотрим формулировку одной из таких задач, которая требует разработки методов защищенных вычислений для рациональных чисел.

Прикладная задача. Применение методов полностью гомоморфного шифрования для передачи управления космическими аппаратами в критических ситуациях иностранным государствам.

Решение данной задачи можно сформулировать таким образом: С КА (при возникновении критической ситуации, вне зоны радиовидимости своего наземного пункта управления) передается телеметрическая информация и текущие навигационные параметры в зашифрованном виде на наземный пункт управления иностранного государства, где выполняется выработка командно-программной информации в защищенном виде, которая далее расшифровывается на борту КА.

Выработка командно-программной информации связана с решением сложных вычислительных задача, к которым относится моделирование, управление, обработка сигналов, изображений и т.п.

Особенностью реализации таких вычислительных задач является необходимость использования рациональных чисел.

Первым препятствием на пути решения поставленной задачи является отсутствие эффективных методов полностью гомоморфного шифрования обеспечивающих реализацию защищенных вычислений с рациональными числами.

Вторым препятствием – является плохо контролируемый рост данных, особенно при умножении, что в основном связано с моделью вычислений (обычно для вычислений используется бинарная логика, это означает, что моделируется стандартный компьютер с фон Неймановской архитектурой с бинарными операциями).

Для устранения данных препятствий построен вариант полностью гомоморфного шифрования для рациональных чисел, с использованием модулярной арифметики. (Предлагается использовать модулярную арифметику, которая применялась при разработке компьютеров К304А и Алмаз, что позволяет сильно распараллеливать арифметические вычисления.)

АЛГОРИТМ 1. ПОЛНОСТЬЮ ГОМОМОРФНОГО ШИФРОВАНИЯ ДЛЯ ЦЕЛЫХ ЧИСЕЛ

Шаг 1. Построение криптосхемы для защищенных вычислений.

Шаг 1.1. Генерация секретного ключа *(секретный ключ расшифрования):*

$$\mathbf{X} = \begin{bmatrix} x_1 & x_2 & \dots & x_n \end{bmatrix}^{\mathrm{T}},$$

$$x_i \perp x_j, (i = 1, 2, \dots, n;\ j = 1, 2, \dots, n).$$

Шаг 1.2. Генерация матрицы **A** размера m x n (Det **A**=0) (секретный ключ зашифрования):

$$\mathbf{A} = \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{bmatrix},$$

$$a_{i,t} \in Z, (i = 1, 2, \dots, n;\ j = 1, 2, \dots, n).$$

Шаг 1.3. Построение вектора оснований представления для исходных данных (вектор оснований):

$$\mathbf{D} = \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{bmatrix},$$

$$a_{i,t} \in Z, (i = 1, 2, \dots, n;\ j = 1, 2, \dots, n).$$

Шаг 1.4. Построение таблицы умножения *(таблица умножения):*

$$\mathbf{M} \Leftrightarrow \mathbf{X} \otimes \mathbf{X}.$$

Элементы матрицы **M** находятся путем решения уравнений:

$$d_1\alpha_1^{(i,j)} + d_2\alpha_2^{(i,j)} + \ldots + d_n\alpha_n^{(i,j)} = x_i \cdot x_j.$$

Шаг 2. Зашифрование.

Шаг 2.1. Выбор исходных данных защищенных вычислений p_1и p_2; *(открытые исходные данные)*

$$\{p_1, p_2 \mid p_1 \in Z, p_2 \in Z\}.$$

Шаг 2.2. Построение векторов представления исходных данных : *(вектор представления исходных данных)*

$$\boldsymbol{\lambda}^{(1)} = \left[\boldsymbol{\lambda}_1^{(1)} \quad \boldsymbol{\lambda}_2^{(1)} \quad \ldots \quad \boldsymbol{\lambda}_n^{(1)}\right], \boldsymbol{\lambda}^{(1)} : p_1 = \boldsymbol{\lambda}^{(1)} \cdot \mathbf{D},$$
$$\boldsymbol{\lambda}^{(2)} = \left[\boldsymbol{\lambda}_1^{(2)} \quad \boldsymbol{\lambda}_2^{(2)} \quad \ldots \quad \boldsymbol{\lambda}_n^{(2)}\right], \boldsymbol{\lambda}^{(2)} : p_2 = \boldsymbol{\lambda}^{(2)} \cdot \mathbf{D}.$$

Шаг 2.3. Умножение векторов представления чисел на матрицу **A** *(секретный ключ зашифрования)*

$$\mathbf{v}^{(1)} = \mathbf{A}^{\mathbf{T}} \cdot \boldsymbol{\lambda}^{(1)^{\mathbf{T}}},$$

$$\mathbf{v}^{(2)} = \mathbf{A}^{\mathbf{T}} \cdot \boldsymbol{\lambda}^{(2)^{\mathbf{T}}}.$$

$\mathbf{v}^{(1)}$ – зашифрованное значение числа p_1. *(зашифрованные исходные данные)*

$\mathbf{v}^{(2)}$ – зашифрованное значение числа p_2.

Шаг 3. Защищенное вычисление. *(защищенное вычисление)*

$$p_1 + p_2 \Leftrightarrow \mathbf{W}_+ = \mathbf{v}^{(1)} + \mathbf{v}^{(2)},$$
$$p_1 \cdot p_2 \Leftrightarrow \mathbf{W}_\otimes = (\mathbf{v}^{(1)} \otimes \mathbf{v}^{(2)}) \cdot \mathbf{M}.$$

Применение таблиц умножения приводит размерность вектора-результата защищенного умножения к n:

$$\left[v_1^{(1)} \cdot v_1^{(2)} \quad \dots \quad v_1^{(1)} \cdot v_n^{(2)} \quad \dots \quad v_n^{(1)} \cdot v_1^{(2)} \quad \dots \quad v_n^{(1)} \cdot v_n^{(2)}\right] \cdot \begin{bmatrix} \alpha_{1,1} & \dots & \alpha_{1,n} \\ \alpha_{2,1} & \dots & \alpha_{1,n} \\ \vdots & \vdots & \vdots \\ \alpha_{n^2,1} & \dots & \alpha_{n^2,n} \end{bmatrix} = \left[w_1 \quad w_2 \quad \dots \quad w_n\right].$$

Шаг 4. Расшифрование. *(расшифрование результата защищенного вычисления)*

$$p_1 + p_2 \Leftrightarrow \mathbf{W}_+ \cdot \mathbf{X},$$
$$p_1 \cdot p_2 \Leftrightarrow \mathbf{W}_\otimes \cdot \mathbf{X}.$$

ИДЕЯ ПОСТРОЕНИЯ МЕТОДА ПОЛНОСТЬЮ ГОМОМОРФНОЕ ШИФРОВАНИЯ ДЛЯ РАЦИОНАЛЬНЫХ ЧИСЕЛ ОСНОВАНА:

На представлении рационального числа в виде пары чисел (p, q) .

где сумма двух рациональных чисел принимает вид:

$$(p_1, q_1) + (p_2, q_2) = (p_1 \cdot q_2 + p_2 \cdot q_1, q_1 \cdot q_2)$$

Произведение двух рациональных чисел принимает вид:

$$(p_1, q_1) + (p_2, q_2) = (p_1 \cdot p_2, q_1 \cdot q_2)$$

Зашифрование каждого из чисел p и q выполняется отдельно по алгоритму 1.

Рассмотрим алгоритм подробно с учетом особенностей сложения и умножения рациональных чисел.

АЛГОРИТМ 2. ПОЛНОСТЬЮ ГОМОМОРФНОГО ШИФРОВАНИЯ ДЛЯ РАЦИОНАЛЬНЫХ ЧИСЕЛ

Шаг 1. Построение криптосхемы для защищенных вычислений (алгоритм 1).

Шаг 1.1. Выбор секретного ключа расшифрования: $\mathbf{X}$.

Шаг 1.2. Выбор секретного ключа зашифрования **A** размера m x m (Det **A**=0). $\mathbf{A}$

Шаг 1.3. Построение вектора оснований представления исходных данных: $\mathbf{D}$.

Шаг 1.4. Построение таблицы умножения: **M**.

Шаг 2. Зашифрование.

Шаг 2.1. Выбор исходных данных (p_1, q_1)и (p_2, q_1):

Шаг 2.2. Построение векторов представления исходных данных для (p_1, q_1)и (p_2, q_1) по алгоритму 1:

$$\boldsymbol{\lambda}^{(1)} = \left[\boldsymbol{\lambda}_1^{(1)} \quad \boldsymbol{\lambda}_2^{(1)} \quad \dots \quad \boldsymbol{\lambda}_n^{(1)}\right], \boldsymbol{\lambda}^{(1)} : p_1 = \boldsymbol{\lambda}^{(1)} \cdot \mathbf{X}.$$
$$\boldsymbol{\lambda}^{(2)} = \left[\boldsymbol{\lambda}_1^{(2)} \quad \boldsymbol{\lambda}_2^{(2)} \quad \dots \quad \boldsymbol{\lambda}_n^{(2)}\right], \boldsymbol{\lambda}^{(2)} : p_2 = \boldsymbol{\lambda}^{(2)} \cdot \mathbf{X}.$$
$$\boldsymbol{\gamma}^{(1)} = \left[\boldsymbol{\gamma}_1^{(1)} \quad \boldsymbol{\gamma}_2^{(1)} \quad \dots \quad \boldsymbol{\gamma}_n^{(1)}\right], \boldsymbol{\gamma}^{(1)} : q_1 = \boldsymbol{\gamma}^{(1)} \cdot \mathbf{X}.$$
$$\boldsymbol{\gamma}^{(2)} = \left[\boldsymbol{\gamma}_1^{(2)} \quad \boldsymbol{\gamma}_2^{(2)} \quad \dots \quad \boldsymbol{\gamma}_n^{(2)}\right], \boldsymbol{\gamma}^{(2)} : q_2 = \boldsymbol{\gamma}^{(2)} \cdot \mathbf{X}.$$

Шаг 2.3. Умножение векторов представления исходных данных на секретный ключ зашифрования **A**:

$$\mathbf{v}^{(1)} = \mathbf{A}^{\mathbf{T}} \cdot \boldsymbol{\lambda}^{(1)^{\mathbf{T}}}, \quad \mathbf{v}^{(2)} = \mathbf{A}^{\mathbf{T}} \cdot \boldsymbol{\lambda}^{(2)^{\mathbf{T}}},$$
$$\mathbf{u}^{(1)} = \mathbf{A}^{\mathbf{T}} \cdot \boldsymbol{\gamma}^{(1)^{\mathbf{T}}}, \quad \mathbf{u}^{(2)} = \mathbf{A}^{\mathbf{T}} \cdot \boldsymbol{\gamma}^{(2)^{\mathbf{T}}},$$

$(\mathbf{v}^{(1)}, \mathbf{u}^{(1)})$ – зашифрованное значение рационального числа (p_1, q_1).

$(\mathbf{v}^{(2)}, \mathbf{u}^{(2)})$ – зашифрованное значение рационального числа (p_2, q_2).

Шаг 3. Защищенное вычисление.

Произведения двух рациональных чисел:

$$(q^{(1)}, p^{(1)}) \cdot (q^{(2)}, p^{(2)}) \Leftrightarrow (\mathbf{W}_{\otimes}^{(1)}, \mathbf{W}_{\otimes}^{(2)}),$$

где $\mathbf{W}_{\otimes}^{(1)} = (\mathbf{v}^{(1)} \otimes \mathbf{v}^{(2)}) \cdot \mathbf{M},$
$\mathbf{W}_{\otimes}^{(2)} = (\mathbf{u}^{(1)} \otimes \mathbf{u}^{(2)}) \cdot \mathbf{M}.$

Суммы двух рациональных чисел:

$$(q^{(1)}, p^{(1)}) + (q^{(2)}, p^{(2)}) \Leftrightarrow (\mathbf{W}_{+}^{(1)}, \mathbf{W}_{\otimes}^{(2)}),$$

где $\mathbf{W}_{+}^{(1)} = (\mathbf{v}^{(1)} \otimes \mathbf{u}^{(2)} + \mathbf{v}^{(2)} \otimes \mathbf{u}^{(1)}) \cdot \mathbf{M},$
$\mathbf{W}_{\otimes}^{(2)} = (\mathbf{u}^{(1)} \otimes \mathbf{u}^{(2)}) \cdot \mathbf{M}.$

Шаг 4. Расшифрование.

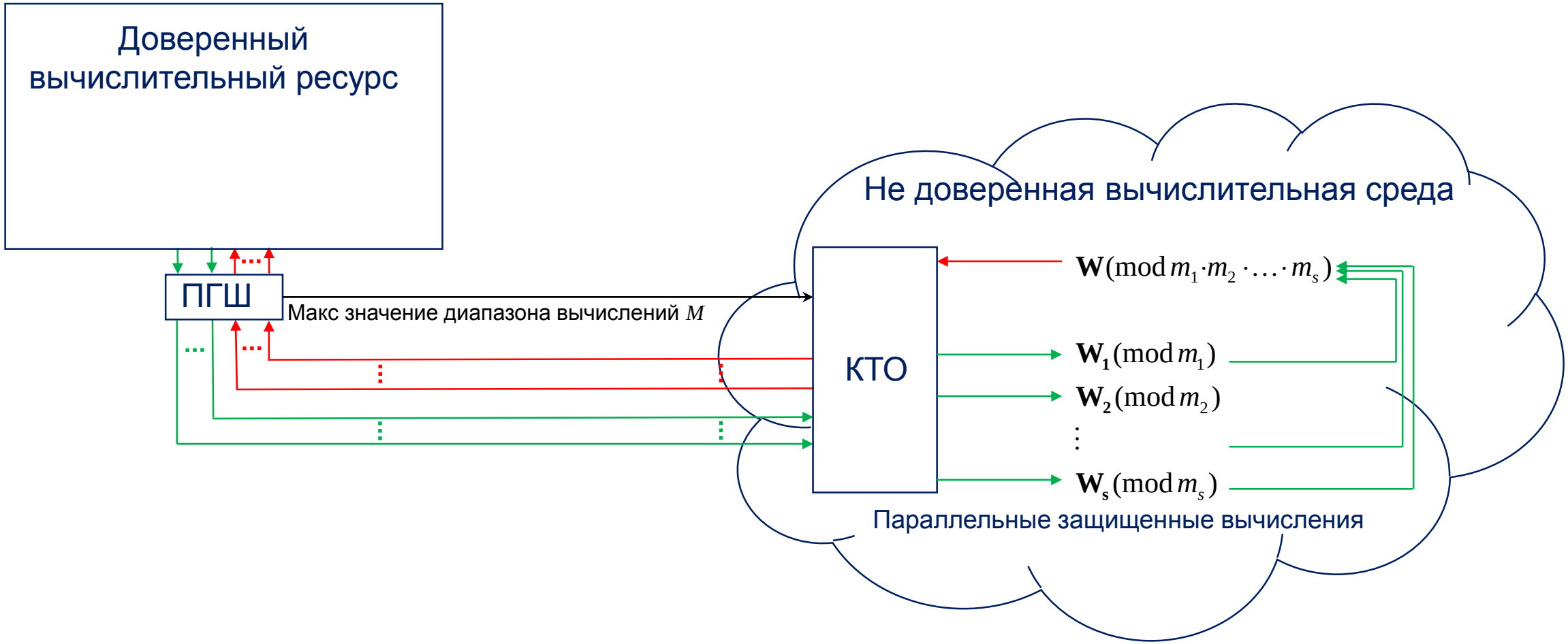
Произведения двух рациональных чисел:

$$(p_1, q_1) \cdot (p_1, q_1) \Leftrightarrow (\mathbf{W}_{\otimes}^{(1)} \cdot \mathbf{X}, \mathbf{W}_{\otimes}^{(2)} \cdot \mathbf{X}),$$

Суммы двух рациональных чисел:

$$p_1 \cdot p_2 \Leftrightarrow (\mathbf{W}_{+}^{(1)} \cdot \mathbf{X}, \mathbf{W}_{\otimes}^{(2)} \cdot \mathbf{X}).$$

УМЕНЬШЕНИЕ РАЗМЕРНОСТИ ДАННЫХ
достигается путем применение
МЕТОДОВ МОДУЛЯРНОЙ АРИФМЕТИКИ:



Заключение:

1. Разработанный метод полностью гомоморфного шифрования обеспечивает реализацию защищенных вычислений с рациональными числами.
2. Стойкость метода достигается недостаточным количеством данных : Det**A**=0.
3. Размерность вектора-результата защищенных вычислений сохраняется равной размерности секретного вектора расшифрования путем применения таблиц умножения **M**.
4. Сохранение размерности элементов вектора-результата защищенных вычислений обеспечивается путем применения методов модулярной арифметики.