УДК 004.056

Т.С. КАЛИНИНА, А.Р. ЛАХИН

Национальный исследовательский ядерный университет «МИФИ», Москва

РЮКЗАЧНАЯ КРИПТОСИСТЕМА, ИСПОЛЬЗУЮЩАЯ МАТЕМАТИКУ КОНЕЧНЫХ ПОЛЕЙ

Предлагается модификация рюкзачной криптосистемы на основе полей Галуа $GF(p\hat{}n)$. Цель – создание стойкой схемы, устойчивой к классическим атакам. Разработан метод построения последовательностей с уникальными суммами через полиномиальное представление элементов поля. Ключевой особенностью является механизм шифрования с добавлением шума и умножением на примитивный элемент поля. Представлены корректные процедуры шифрования и расшифрования. Результаты подтверждают перспективность предлагаемого решения.

Введение

В отличии от ранцевой криптосистемы Шора-Ривеста, где используется дискретное логарифмирование, предлагается модификация, работающая непосредственно в конечном поле.

В рюкзачных криптосистемах осуществляется нахождение такого набора чисел $\{a_{i_1}, a_{i_2}, \dots, a_{i_m}\}$ из последовательности $\{a_1, \dots, a_n\}$, сумма которых даёт k. Перенесём эту идею в расширенные поля Галуа $\mathrm{GF}(p^n)$.

Элементами поля $\mathrm{GF}(p^n)$ являются полиномы степени, меньшей n, с коэффициентами из конечного поля $\mathrm{GF}(p)$: $a_{k1}a_{k2}\dots a_{kn}$, где $a_{ki} \in \mathrm{GF}(p) = \{0, 1, \dots, p-1\}, i = \overline{1,n}$.

Сумма любых элементов из поля $GF(p^n)$ даёт элемент из того же поля. Но, у нас есть условие для рюкзачной криптосистемы, что любой набор чисел из последовательности должен давать уникальную сумму, иначе сообщение будет невозможно расшифровать. Не все возможные последовательности из элементов поля $\mathrm{GF}(p^n)$ будут удовлетворять такому условию, также максимальное количество элементов, входящих в удовлетворяющую условию последовательность, равно n. Чтобы определить, удовлетворяет ли последовательность длиною n такому условию, найдём её определитель по модулю p:

$$\{a_1, \dots, a_n\}, a_i = a_{i1}a_{i2}\dots a_{in}, i = \overline{1,n}$$

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \bmod p = \begin{cases} 0 \Rightarrow \text{не удовлетворяет} \\ \{1, \dots, p-1\} \Rightarrow \text{удовлетворяет.} \end{cases}$$

При этом если брать подпоследовательности из этих последовательностей, то они тоже будут удовлетворять условию уникальности.

Идея

Имеем поле $\mathrm{GF}(p^n)$, неприводимый многочлен $\varphi(x)$ степени n, примитивный элемент ω, число R $(0 < R < p^n - 1)$, последовательность $\{a_1, \dots, a_k\}$ $(a_i \in \mathrm{GF}(p^n),\ i = \overline{1,k}, k \le n)$.

Сформируем открытый ключ:

1) Добавим шум: $b_i = {*}{*}{*} \dots {*}{*}{*}\ a_i\ {*}{*}{*} \dots {*}{*}{*} = b_{i1} b_{i2} \dots b_{il}$, при этом $l \bmod n = 0, i = \overline{1,k}$.

2) Делим b_i на блоки длиной n и умножаем их на ω^R и берем по $mod\ \varphi(x)$

$$b_i = b_{i_1} \dots b_{i_a} \dots b_{i_s}, \text{где } b_{i_j} \text{ длиною } n, b_{i_a} = a_i, i = \overline{1,k}$$

$$c_i = \left(b_{i_1} * \omega^R \bmod \varphi(x)\right) \dots \left(b_{i_a} * \omega^R \bmod \varphi(x)\right) \dots \left(b_{i_s} * \omega^R \bmod \varphi(x)\right) = $$

$$= c_{i_1} \dots c_{i_a} \dots c_{i_s}, i = \overline{1,k}$$

В итоге: $PK = (p, \{c_i\}), SK = (n, \varphi(x), \omega, R)$.

Шифрование

Зашифрование

Имеется сообщение $m = m_1 m_2 \dots m_k$, где $m_i \in \{0, 1, \dots, p-1\}, i = \overline{1,k}$.

1) Находим сумму $e = m_1 c_1 + m_2 c_2 + \dots + m_k c_k$, причём

$$c_i + c_j = c_{i1} \dots c_{il} + c_{j1} \dots c_{jl} = \left((c_{i1} + c_{j1}) \bmod p\right) \dots \left((c_{il} + c_{jl}) \bmod p\right)$$

$$k * c_i = k * c_{i1} \dots c_{il} = (k * c_{i1} \bmod p) \dots (k * c_{il} \bmod p)$$

2) Отправляем эту сумму получателю

Расшифрование

1) Делим сумму e на блоки длиной n и умножаем их на $\omega^{p^n - R - 1}$ и берем по $\bmod \varphi(x)$:

$$e = e_1 \dots e_s$$

$$d = \left(e_1 * \omega^{p^n - R - 1} \bmod \varphi(x)\right) \dots \left(e_s * \omega^{p^n - R - 1} \bmod \varphi(x)\right) = d_1 \dots d_s$$

2) Делим c_i на блоки длиной n и умножаем их на $\omega^{p^n - R - 1}$ и берем по $\bmod \varphi(x)$:

$$c_i = c_{i_1} \dots c_{i_s}$$

$$b_i = \left(c_{i_1} * \omega^{p^n - R - 1} \bmod \varphi(x)\right) \dots \left(c_{i_s} * \omega^{p^n - R - 1} \bmod \varphi(x)\right) = b_{i_1} \dots b_{i_s},$$

$$i = \overline{1,k}$$

$$b_i = {*}{*}{*} \dots {*}{*}{*}\ a_i\ {*}{*}{*} \dots {*}{*}{*}, i = \overline{1,k}$$

3) Решаем задачу о рюкзаке, зная d_{i_a} и $\{a_i\}, i = \overline{1,k}$, и получим m.