Самохина Марина Андреевна
Аспирант кафедры Радиотехники МФТИ

АНАЛИЗ МОДИФИКАЦИЙ КРИПТОСИСТЕМЫ НИДЕРРАЙТЕРА

Аннотация

В докладе рассматривается построение и атака на классическую криптосистему Нидеррайтера и различные подходы к модификации системы. Приведен анализ ряда атак на рассматриваемые криптосистемы. Сделано заключение о криптостойкости модификаций и возможности их применения.

В теории криптосистем с открытым ключом известны два основных типа систем, основанных на линейных кодах. Это система Мак Элиса (McElice) [1] и система Нидеррайтера [2]. Рассмотрим подробнее классическую криптосистему Нидеррайтера.

Идея системы Нидеррайтера состоит в следующем. В качестве секретных ключей выбираются:

- проверочная матрица $H = \left[z_j x_j^i \right]$, где $j = 1,2,\ldots,n$, $i = 0,1,\ldots,r-1$, некоторого обобщенного кода Рида-Соломона над полем $GF(q)$;
- случайно выбранная невырожденная скремблирующая матрица S порядка r над полем $GF(q)$. Эта матрица вводится для того, чтобы скрыть от криптоаналитика видимые закономерности, разрушая структуру проверочной матрицы.

Открытым ключом является скремблированная проверочная матрица $H_{cr} = SH$.

Сообщениями являются все n-векторы с координатами из поля $GF(q)$ с весом не превосходящим $r/2$. Здесь сообщения не являются кодовыми словами выбранного кода Рида-Соломона, а представляют собой всевозможные ошибки, которые этот код в состоянии исправлять.

Шифротекст, соответствующий сообщению m, представляет собой r-вектор и вычисляется следующим образом:

$$c = mH_{cr}^T = mH^T S^T .$$

Законный пользователь после приема шифротекста c, умножает его справа на матрицу $(ST)^{-1}$, а затем применяет известный лишь ему алгоримт быстрого декодирования и получает переданное сообщение m.

Описанная криптосистема оказалась нестойкой и была взломана Сидельниковым и Шестаковым. Авторам удалось угадать структуру закрытого ключа по открытому и подобрать такие матрицы $\tilde{H}$ и $\tilde{S}$, что $H_{cr} = \tilde{S}\tilde{H}$. В работе [3] приведен подробный алгоритм атаки. В последующие годы не раз предпринимались попытки модифицировать классическую криптосистему Нидеррайтера таким образом, чтобы повысить ее криптостойкость.

На сегодняшний день существует несколько модификаций криптосистемы, среди которых можно выделить три основных подхода. Во-первых, зашумление проверочной матрицы кода введением скрывающей матрицы. Например, в работе [4] в качестве скрывающей матрицы была предложена матрица единичного ранга. В работе [5] использовались

скрывающие матрицы ранга, значительно большего единицы. Второй подход к модификации заключается в использование различных метрик, отличных от классической хэмминговой метрики. Например, выбирается ранговая метрика (как в работе [6]) или вводится некая новая метрика. И третий вариант модифицирования классической криптосистемы Нидеррайтера – это построение кодов с набором специфических свойств. Стоит отметить, что в последнее время довольно успешно применяется сочетание сразу двух или более из описанных выше способов модификаций.

В докладе рассмотрены перспективные варианты модифицированных криптосистем: криптосистема на ранговых кодах, система на основе метрики, ассоциированной с матрицей Вандермонда, модификация криптосистемы на основе метрики, ассоциированной с немодифицированной матрицей Фробениуса.

Рассмотрим подробнее модификацию на основе Фробениусовской метрики. Основная идея заключается в введении нехэмминговой метрики ассоциированной с немодифицированной матрицей Фробениуса. Пусть F матрица размером N на n с элементами из поля $GF(q^N)$ такая, что $n < N$ и ранг матрицы F меньше n. Обозначим $\underline{f_1}, \underline{f_2}, \ldots, \underline{f_N}$ строки матрицы F. Для любого ненулевого вектора $\underline{x}$ из пространства $GF(q^N)^n$ его норма определяется как минимальное число ненулевых коэффициентов a_i в разложении:

$$\underline{x} = \sum_{i=1}^{n} a_i \underline{h_i}.$$

В качестве матрицы F выбирается матрица следующего вида (немодифицированная матрица Фробениуса):

$$F = \begin{pmatrix} h_1 h_1^q \ldots\ldots\ldots h_1^{q^{n-1}} \\ h_2 h_2^q \ldots\ldots\ldots h_2^{q^{n-1}} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ h_N \ldots\ldots h_N^q h_N^{q^{n-1}} \end{pmatrix},$$

где каждый элемент матрицы выбирается из поля $GF(q^N)$. Элементы $h_1, h_2, \ldots, h_N$ линейно-независимы над базовым полем.

Далее для построения кода используется конкатенация матрицы F и некоторой матрицы G_k, имеющей такой вид как и F:

$$Q = \begin{pmatrix} h_1 & h_1^q & \dots & h_1^{q^{n-1}} \\ h_2 & h_2^q & \dots & h_2^{q^{n-1}} \\ \vdots & \vdots & \dots & \vdots \\ h_{N_1} & h_{N_1}^q & \dots & h_{N_1}^{q^{n-1}} \\ g_1 & g_1^q & \dots & g_1^{q^{n-1}} \\ g_2 & g_2^q & \dots & g_2^{q^{n-1}} \\ \vdots & \vdots & \dots & \vdots \\ g_K & g_K^q & \dots & g_K^{q^{n-1}} \end{pmatrix} = \begin{pmatrix} F \\ G_k \end{pmatrix},$$

где $F = \begin{pmatrix} h_1 & h_1^q & \dots & h_1^{q^{n-1}} \\ h_2 & h_2^q & \dots & h_2^{q^{n-1}} \\ \vdots & \vdots & \dots & \vdots \\ h_{N1} & h_{N1}^q & \dots & h_{N1}^{q^{n-1}} \end{pmatrix}$ и $G_k = \begin{pmatrix} g_1 & g_1^q & \dots & g_1^{q^{n-1}} \\ g_2 & g_2^q & \dots & g_2^{q^{n-1}} \\ \vdots & \vdots & \dots & \vdots \\ g_k & g_k^q & \dots & g_k^{q^{n-1}} \end{pmatrix}$,

где $N = N_1 + K$, h_i, g_j – элементы поля $GF(q^N)$, линейно независимые в совокупности над базовым полем $GF(q)$. Верхняя часть матрицы Q с элементами $h_j^{q^i}$ используется для определения метрики, а нижняя часть с элементами $g_j^{q^i}$ используется как порождающая матрица кода:

$$G_k = \begin{pmatrix} g_1 & g_1^q & \cdots & g_1^{q^{n-1}} \\ g_2 & g_2^q & \cdots & g_2^{q^{n-1}} \\ \vdots & \vdots & \cdots & \\ g_K & g_K^q & \cdots & g_K^{q^{n-1}} \end{pmatrix}$$

При шифровании открытого текста, обозначим его через набор $\underline{a} = (a_1 \quad a_2 \quad \dots \quad a_k)$ из k информационных символов, кодовый вектор вычисляется следующим образом:

$$\underline{y} = \underline{a} G_k .$$

Вектор $\underline{y}$ можно представить в виде:

$$\underline{y} = \left(a_1 g_1 + a_2 g_2 + \dots + a_k g_k \quad a_1 g_1^q + a_2 g_2^q + \dots + a_k g_k^q \quad \dots \quad a_1 g_1^{q^{n-1}} + a_2 g_2^{q^{n-1}} + \dots + a \right.,$$

где число ненулевых a_i равно s. Пусть вектор $\underline{y}$ имеет в новой метрике норму равную $N_F = m$. Тогда $\underline{y}$ можно записать в несколько ином виде:

$$\underline{y} = \left(b_b h_1 + b_2 h_2 + \dots + b_m h_m \quad b_1 h_1^q + b_2 h_2^q + \dots + b_m h_m^q \quad \dots \quad b_1 h_1^{q^{n-1}} + b_2 h_2^{q^{n-1}} + \dots + b_m h_n^c \right.$$

.

Из полученных представлений вектора $\underline{y}$ следует, что $s+m$ строк матрицы Q линейно зависимы. Учитывая, что s и m натуральные и $s+m>n$, следовательно, $s+m \geq n+1$ или $N_F \geq n-s+1$.

Так как минимальное расстояние линейного кода равно минимальному весу ненулевых кодовых слов, то минимальное расстояние данного кода не будет превосходить N_F. Пользуясь тем, что $k>s$, получаем $d_F \geq n-k+1$. Принимая во внимание обобщенную границу Синглтона, заключаем, что $d_F = n-k+1$.

При декодировании шифротекст удобно представить несколько ином виде. Пусть $\underline{c} = \underline{g} + \underline{e}$, где $\underline{g} = (g_1 \quad g_2 \quad \ldots \quad g_{N_1})$ – кодовый вектор, $\underline{e} = (e_1 \quad e_2 \quad \ldots \quad e_{N_1})$ – вектор ошибки.

Предполагая, что норма строки ошибки в новой метрике равна t, вектор e можно представить в виде:

$$\underline{e} = m_1 h_1 + m_2 h_2 + \ldots + m_{N_1} h_{N_1},$$

причем $d_H(\underline{m}) = t$. Для кодов, описанных выше, существуют быстрые алгоритмы декодирования.

При расшифровании легальный пользователь умножает полученный шифротекст $(\underline{g}+\underline{e})S$ на S^{-1}. Затем применяет алгоритм быстрого декодирования в новой метрике. В результате пользователь получит вектора $\underline{g}$ и $\underline{e}$. После применения алгоритма быстрого декодирования родительского кода легальный пользователь получит вектор $\underline{\tilde{m}}$. Далее при умножении $\underline{\tilde{m}}$ на P^{-1} получится сам открытый текст m.

После построения криптосистемы необходимо провести ее криптоанализ. Интересно рассмотреть два основных вида атак, применимые к семейству модифицированных криптосистем: прямые и структурные атаки. Под прямыми атаками понимаются: перебор по искусственным ошибкам, перебор по сообщениям, декодирование опубликованного кода как случайного. Среди структурных атак стоит выделить различные модификации атаки Гибсона, адаптированные к изменениям в криптосистеме, а также вариант атаки Сидельникова-Шестакова. Стоит отметить, что при оценке трудоемкости каждой из атак, необходимо учитывать размер открытого ключа. Как правило, размер ключа выбирается с учетом требований, предъявляющихся сегодня на практике к ассиметричным криптосистемам. Также интересна теоретическая оценка криптостойкости системы для ключей значительно меньшего размера, так как атака, предложенная Гиббсоном оперирует только с ключами в 10-20 Кбит.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. McElice R.J. A Public Key Cryptosystem Based on Algebraic Coding Theory // DSN Progress Report 42-44. – Pasadena, CA: Jet Propulsion Lab, 1978. – P. 114-116.

2. Niederreiter H. Knapsack-Type Cryptosystem and Algebraic Coding Theory // Probl. Control and Inform. Theory, 1986. – Vol. 15 – P. 19-34.
3. Сидельников В.М., Шестаков С.О. О системе шифрования, основанной на обощенных кодах Рида-Соломона // Дискретная математика, 1992. – Т.3, вып.3.
4. Gabidulin E., Ourivski A., Pavlouchkov V., On the modified Niederreiter cryptosystem // Proc. Information Theory and Networking Workshop, Metsovo, Greece, 1999. P. 50
5. Габидулин Э.М., Обернихин В.А., Коды в F-метрике Вандермонда и их применение.
6. Габидулин Э.М., Теория кодов с максимальным ранговым расстоянием // Проблемы передачи информации, Вып. 1, 1985 – Т. XXI.