Электронная Цифровая Подпись на Основе Криптосистемы McEliece

Геннадий Халимов
Кафедра Безопасности Информационных Технологий
Харьковский национальный университет радиоэлектроники
Харьков, Украина
gennadykhalimov@gmail.com

Дмитрий Шипилов
Кафедра Безопасности Информационных Технологий
Харьковский национальный университет радиоэлектроники
Харьков, Украина
dmytrii.shypilov@nure.ua

Electronic Digital Signature Based on McEliece Cryptosystem

Gennady Khalimov
Information Security Department
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
gennadykhalimov@gmail.com

Dmitry Shipilov
Information Security Department
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
dmytrii.shypilov@nure.ua

***Аннотация*—в данной статье рассмотрена цифровая подпись на основе криптосистемы McEliece. Данный результат эксплуатирует идею представления хеш кода сообщения кодовым словом. Безопасность цифровой подписи определяется сложностью решения задачи декодирования линейных кодов, которая за счет маскирования порождающей матрицы случайной невырожденной матрицей и перестановочной матрицей является NP-сложной.**

***Abstract*—This article describes a digital signature based on the McEliece cryptosystem. This result exploits the idea of representing the hash of the message code with a codeword. The security of a digital signature is determined by the complexity of solving the decoding problem for linear codes, which, due to masking the generating matrix by a random nondegenerate matrix and a permutation matrix, is NP-complex.**

Ключевые слова—цифровая подпись, криптосистема McEliece, кодирование.

Keywords—digital signature, cryptosystem McEliece, coding.

I. Введение

Криптосистема McEliece предложена в 1978 году Робертом Мак-Элисом и является одним из кандидатов в криптографии на постквантовый период. Криптоалгоритм основывается на сложности декодирования полных линейных кодов (общая задача декодирования является NP-сложной) и на данный момент не существует квантового алгоритма её решения. В первоначальной конструкции были предложены двоичные коды Гоппы [1]. Наиболее практичные из известных атак используют алгоритм декодирования множества данных и не являются эффективными [1,2]. Уровень безопасности системы McEliece остается очень стабильным и устойчивым несмотря на множество теоретических атак в течение более 40 лет. Аутентичные параметры McEliece были спроектированы только для уровня безопасности 2^{64}, система легко масштабируется до очень больших параметров, гарантирующих защиту против атак с использованием квантовых вычислений. Недостатком классической криптосистемы McEliece является большой размер ключа. Улучшения криптосистемы с кодовыми вычислениями предложены в 2015 году группой разработчиков Gaborit, Ruatta, Schrek, Tillich, Z'emor. Так для 128 битного уровня безопасности достигается размер ключа в 2809 бит [3]. Дальнейшим улучшением является криптосистема McNie на основе скоростного алгоритма Нидеррайта [4]. Применение 4 квази-циклических LRPC кодов над полем приводит к размеру ключа в 2775 бит для 128 битного уровня безопасности. Криптоалгоритм McNie

остается безопасным против структурных атак и атак подмены. Для криптосистемы McEliece предложены реализации для ассиметричного шифрования . Задачей статьи является разработка цифровой подписи на основе криптосистемы McEliece.

II. ОПИСАНИЕ АЛГОРИТМА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Криптосистема McEliece определяется матричными вычислениями над кодовыми словами *[n,k,d]* кода над конечным полем *GF(q)* с оценкой вектора ошибок. Подписываемое сообщение представляет собой вектор фиксированной длинны.

Цифровая подпись на основе ассиметричной криптосистемы определяется следующими вычислениями:

1. генерация ключа;
2. вычисление подписи;
3. проверка подписи.

Для криптосистемы McEliece содержание шагов является следующим.

Генерация ключа.

1. Алиса выбирает *[n,k,d]* – линейный код, исправляющий t ошибок. Для выбранного кода вычисляется порождающая матрица G размером $k \times n$.

2. Для маскирования порождающей матрицы кода генерируется случайная невырожденная матрица S размером $k \times k$ и перестановочная матрица P размером $n \times n$.

3. Вычисляется матрица $\hat{G} = S * G * P$.

4. Открытым ключом является пара $(\hat{G},t)$, а личным – (S,G,P).

Для вычисления цифровой подписи предлагается следующий алгоритм.

1. Фиксируется хеш-функция $h(x)$ с n символами на выходе. Для сообщения D вычисляется хеш значение $h(D)$.

Многократно вычисляется $h(h(D)||i)$, для $i = 0,1,2\ldots$, пока для некоторого минимального $i = i_{min}$ не станет возможным декодировать $h(h(D)||i)$, с вектором ошибок веса не больше t.

2. Хеш значение $h(h(D)||i_{min})$ можно представить как кодовое слово $\mathrm{A}\hat{G}$ с вектором ошибок z для некоторого информационного вектора A

$$h(h(D)||i_{min}) = \mathrm{A}\hat{G} + z.$$

Второй вариант подписи определяется значениями (R,s) и верифицируется уравнением:

$$sG = R + H(R \,||\, m)P.$$

3. Определить значение вектора A можно с помощью следующих вычислений:

• Умножение на обратную матрицу перестановки P^{-1}, которая не изменяет вес вектора ошибки

$$h(h(D)||i_{min}) * P^{-1} = (\mathrm{A}\hat{G} + z) * P^{-1} = \mathrm{A} * S * G + z * P^{-1}.$$

• Последующее декодирование $h(h(D)||i_{min}) * P^{-1}$ даст вектор $\mathrm{A}' = \mathrm{A} * S$ и вектор ошибки $z' = z * P^{-1}$.

• Умножение на обратную матрицу S^{-1} (матрица S не вырожденная) и матрицу перестановки даст искомые значения A, z

$$\mathrm{A} = \mathrm{A}' * S^{-1},$$
$$z = z' * P.$$

4. Цифровой подписью документа D является вектор значений (A, z, i_{min}).

Проверка подписи:

1. Вычисляется $v_1 = h(h(D)||i_{min})$.

2. Для значений A, z и известного ключа $\hat{G}$ вычисляем $v_2 = \mathrm{A} * \hat{G} + z$.

3. Если $v_1 = v_2$ и $wt(z) \le t$, то подпись верна.

Пример. Вычислить цифровую подпись в криптосистеме McEliece на основе двоичного кода $[12,4,5]$.

Для выбранного кода порождающая матрица $G[4 \times 12]$ имеет вид

$$G = \begin{vmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \end{vmatrix}.$$

Характеристики распределения для символов матрицы имеют значения *"1"–47,9167%* и *"0"–52,0833%*.

Выберем случайную невырожденную матрицу $S[4 \times 4]$

$$S = \begin{vmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{vmatrix}.$$

Матрица $S[4\times 4]$ имеет символов распределения $"1"-43{,}75\%$ и $"0"-56{,}25\%$.

Сформируем случайную матрицу перестановок $P[12\times 12]$

$$P=\begin{vmatrix}1&0&0&0&0&0&0&0&0&0&0&0\\0&0&1&0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0&0&0&0&0\\0&0&0&0&1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0&0&0&0&0\\0&0&0&1&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&1&0&0&0&0\\0&0&0&0&0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&0&0&0&1&0\\0&0&0&0&0&0&1&0&0&0&0&0\end{vmatrix}.$$

Вычислим матрицу $\hat{G}$:

$$\hat{G}=S*G*P=\begin{vmatrix}1&1&0&1&0&0&0&0&0&1&1&1\\1&1&0&0&0&1&0&1&0&0&1&0\\0&0&1&0&1&1&0&1&1&0&0&1\\0&1&0&0&0&1&1&0&1&0&1&1\end{vmatrix}.$$

Открытый ключ $-(\hat{G},t)$, личный ключ $-(S,G,P)$.

Пусть для сообщения D при $i_{min}=5$ имеем хеш значение

$$h(h(D)||i_{min})=|0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0|.$$

Кодовое слово $h(h(D)||i_{min})$ включает некоторый вектор A и вектор ошибки z.

Вычислим A и z. Обратная матрица P^{-1} имеет вид

$$P^{-1}=\begin{vmatrix}1&0&0&0&0&0&0&0&0&0&0&0\\0&0&0&0&0&1&0&0&0&0&0&0\\0&1&0&0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&1&0&0&0&0&0\\0&0&0&0&1&0&0&0&0&0&0&0\\0&0&0&1&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&0&1&0&0&0\\0&0&1&0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&1&0&0&0&0\end{vmatrix}.$$

$h(h(D)||i_{min})*P^{-1}=|0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0|.$

Применяя декодирование для кодового слова $decod(h(h(D)||i_{min})*P^{-1})$ получим

$$A'=A*S=|1\ \ 1\ \ 0\ \ 1|,$$

$$z'=z*P^{-1}=|1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0|.$$

Вычислим $A=A'*S^{-1}=A*S*S^{-1}$ и $z=z'*P=z*P^{-1}*P$ с помощью обратной матрицы S^{-1}.

$$S^{-1}=\begin{vmatrix}1&0&0&0\\0&1&1&0\\0&0&0&1\\1&1&0&1\end{vmatrix},$$

$$A=A'*S^{-1}=|1\ \ 0\ \ 1\ \ 0|,$$

$$z=z'*P=|1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0|.$$

Подписью D является вектор значений

$$(A,z,i_{min})=(|1\ \ 0\ \ 1\ \ 0|,\ |1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0|,5).$$

Проверка подписи.

Вычислим

$$v_1=h(h(D)||i_{min})=h(h(D)||5)=$$
$$|0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0|$$

и $v_2=A*\hat{G}+z$.

$$\hat{G}=\begin{vmatrix}1&1&0&1&0&0&0&0&0&1&1&1\\1&1&0&0&0&1&0&1&0&0&1&0\\0&0&1&0&1&1&0&1&1&0&0&1\\0&1&0&0&0&1&1&0&1&0&1&1\end{vmatrix},$$

$$A*\hat{G}=|1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0|,$$

$$v_2=A*\hat{G}+z=$$
$$|1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0|\oplus$$
$$|1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0|=$$
$$|0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0|$$

Подпись верна так, как

$$v_1=v_2=|0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0|$$

и $wt(z)\le 2$.

III. Выводы

Безопасность цифровой подписи на основе криптосистемы McEliece определяется размером порождающей матрицы кода. Для ряда кодовых конструкций эти оценки колеблются в пределах значений в несколько тысяч. Безопасность криптосистемы McEliece основана на предположении, что открытый ключ неотличим от случайной матрицы. Атаки на криптосистему подразделяются на два класса, которые пытаются восстановить секретный ключ из открытого ключа и атаки, направленные на извлечение сообщения открытого текста из одного зашифрованного текста. До сих пор нет известного субэкспоненциального алгоритма для любого типа атаки.

Криптосистема McEliece невосприимчива к квантовому алгоритму Шора, который является уязвимым для криптосистем RSA и ECDSA. В [5] Бернштейн представил в настоящее время самую эффективную атаку на Криптосистема McEliece с использованием квантового алгоритма Гровер. Для криптосистемы McEliece для сохранения постквантовой безопасности размер ключей должен быть увеличен в четыре раза.

Литература References

[1] Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: Пер. с англ. — М: Связь, 1979. — 744 с.

[2] Daniel J. Bernstein, Tung Chou, Tanja Lange and others. Classic McEliece: conservative code-based cryptography, 2017. – 38c.

[3] Gaborit, Ruatta, Schrek, Tillich, Z'emor. RankSign -a signature proposal for the NIST's call , 2017. – 37 c.

[4] Y. X. Li, R. H. Deng, and X. M. Wang. On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. IEEE Transactions on Information Theory, 40(1):271–273, January 1994.

[5] D. J. Bernstein. Grover vs. McEliece. In N. Sendrier, editor, Post-Quantum Cryptography, Third International Workshop, PQCrypto 2010, Darmstadt, Germany,May 25-28, 2010. Proceedings, volume 6061 of Lecture Notes in Computer Science, pages 73–80. Springer, 2010