УДК 621.396(024)

Фам Суан Нгиа

АНАЛИЗ ПРИМЕНЕНИЯ АЛГОРИТМА МАК-ЭЛИС ДЛЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Предложено применение алгоритмов системы кодирования Мак-Элис для электронной цифровой подписи. Показано, что в этом случае использование алгоритма Мак-Элис повышает скрытность информации в 10^{50} раз. Применение параллельных кодов в алгоритме Мак-Элис, кроме расширения пространства ключей, позволяет значительно повысить криптостойкость информации, а также увеличить криптостойкость цифровой подписи по сравнению с исходным алгоритмом на основе простых линейных кодов.

Введение. В настоящее время задачи криптографии выходят далеко за рамки обеспечения секретности данных [1]. По мере автоматизации процессов передачи и обработки информации, а также интенсификации информационных потоков, криптографические методы приобретают уникальное значение. Новые информационные технологии в своей основе имеют криптографию с открытым ключом (двухключевая криптография), которая позволяет реализовать протоколы, предполагающие, что секретный ключ известен только одному пользователю. Эти протоколы ориентированны на взаимное недоверие взаимодействующих сторон [1, 2].

Криптография с открытым ключом может реализовать протоколы взаимодействия сторон, которые не доверяют друг другу, данная характеристика очень важна для электронной цифровой подписи (ЭЦП), являющейся важным элементом применения криптографии. При использовании криптографии с открытым ключом ЭЦП позволяет с высокой степенью гарантии удостовериться в том, что полученное сообщение было составлено владельцем секретного ключа. Двухключевая криптография обеспечивает строгую доказательность факта составления того или иного сообщения конкретными абонентами криптосистем. Кроме того, при использовании симметричной криптографии для ЭЦП передача секретных ключей по закрытому каналу является трудной проблемой, но данная проблема имеет простое решение для двухключевой криптографии [1] .

Для системы ЭЦП возможно использование алгоритма Мак-Элис [3], который позволяет обеспечить как скрытность, так и удобство использования.

Цель работы. Анализ применения алгоритма Мак-Элис для системы электронной цифровой подписи.

Алгоритм кодирования. Алгоритм Мак-Элис, обеспечивающий информационную скрытность передаваемой информации, основан на выборе корректирующего кода, исправляющего определенное количество ошибок, для которого существует эффективный алгоритм декодирования. С помощью закрытого ключа этот код «маскируется» под линейный код, декодирование которого не имеет эффективного решения [3]. На рис. 1 показан алгоритм Мак-Элис.

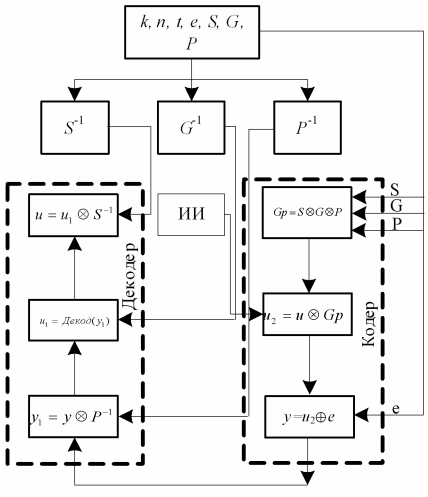

Рис. 1

Параметрами, общими для всех абонентов, являются целые числа *k, n* и *t,* где *k* – длина информационного сообщения, *n* – длина кодового слова, *t* – количество искусственно вводимых ошибок.

Каждому абоненту системы для получения открытого и соответствующего закрытого ключа следует выполнить следующие действия:

- определить порождающую матрицу $G_{k\times n}$ двоичного (n, k) - линейного кода, исправляющего t ошибок, для которого известен эффективный алгоритм декодирования;

- выбрать двоичную невырожденную матрицу $S_{k\times k}$;

- выбрать подстановочную матрицу $P_{n\times n}$;

- вычислить произведение матриц $G_p = S \cdot G \cdot P$.

Открытым ключом является пара (G_p, t), закрытым - тройка (S, G, P).

Для кодирования сообщения M, предназначенного для абонента B, абонент A должен:

- представить M в виде двоичного вектора u длины k;

- выбрать случайный бинарный вектор ошибок e длины n, содержащий не более t ошибок;

- вычислить бинарный вектор $y = uG_p \oplus e$ и передать его абоненту В.

Получив сообщение y, абонент В вычисляет вектор $y_1 = yP^{-1}$, с помощью которого, используя алгоритм декодирования кода с порождающей матрицей G, получает далее векторы u_1 и $u = u_1 S^{-1}$.

Корректность приведенного алгоритма подтверждает следующее выражение [3]:

$$y_1 = yP^{-1} = (uG_p \oplus e)P^{-1} = \\ = (uSGP \oplus e)P^{-1} = (uS)G \oplus eP^{-1}, \quad (1)$$

где eP^{-1} – вектор, содержащий не более t единиц. Поэтому алгоритм декодирования кода с порождающей матрицей G декодирует y в вектор

$$u_1 = u\,S^{-1}. \quad (2)$$

На основе исходного алгоритма кодирования информации Мак-Элис, приведенного в [3], можно предложить другой способ повышения скрытности информации и пространства ключа, основанный на использовании параллельного кода.

На рис. 2 предложена структурная схема данного алгоритма, содержащая две ветви; структура каждой аналогична исходному алгоритму с закрытыми - (S_1,G_1,P_1), (S_2, G_2, P_2) и открытыми ключами (t_1, $G_{p1} = S_1G_1P_1$), (t_2, $G_{p2} = S_2G_2P_2$), где ИИ – источник информации, ЛК – линейный код, ГО – группообразование, ФКО – формирователь коэффициента объедения. Информация на выходе источника информации состоит из двух частей.

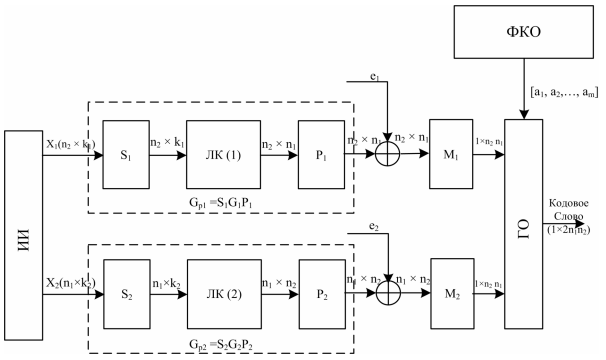

Рис. 2

Входная информация для каждой ветви представляется строками матриц $X_{1(n_2\times k_1)}$ и $X_{2(n_1\times k_2)}$. Кодирование в каждой ветви выполняется по строкам матриц X_1 и X_2. Блоки M_1 и M_2 объединяют кодовые слова, поступающие из соответствующей ветви в последовательность длиной n_1n_2, в чем и состоит особенность данного алгоритма. Выходная последовательность кодера имеет длину $2n_1n_2$. Декодирование основано на разделении кодовой последовательности на две подпоследовательности длиной n_1n_2 , декодирование которых осуществляется на основе исходного алгоритма.

Из анализа схемы алгоритма (рис. 2) следует, что объединение двух кодовых последовательностей значительно повышает скрытность передаваемой информации. При таком объединении криптостойкость информации повышается на $2^{n_1n_2}$ по сравнению с исходной схемой, изображенной на рис. 1. Например, при использовании в данном алгоритме двух кодов с длиной кодового слова $n = 7$ выигрыш составит порядка $\sim 5\times10^{14}$. Кроме того, при использовании закона объединения [a_1, a_2, … a_m] расширяется пространство закрытых ключей в m! раз. Пример работы блока объединения представлен на рис. 3.

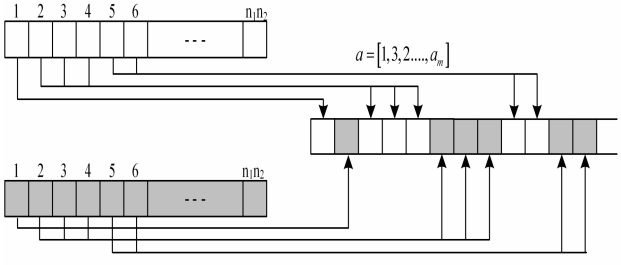

Рис. 3

Электронная цифровая подпись. В общем случае цифровая подпись представляет собой

некоторое число со специфической структурой, которое допускает проверку с помощью открытого ключа того факта, что оно было выработано для некоторого сообщения с использованием секретного ключа. Для реализации цифровой подписи необходимо выбрать такую одностороннюю функцию с потайным ходом (с секретом) f_z, для которой при всех значениях параметра z область определения функции f_z, совпадает с областью её значений. При этом условии для любого сообщения, которое может быть представлено в виде числа из области определения функции $f_z(x)$, абонент i может сформировать с помощью секретного алгоритма число [1]

$$П = f_{z_i}^{-1}(M). \quad (3)$$

Каждый пользователь криптосистемы может по значению $П$ восстановить сообщение M, используя открытый алгоритм шифрования E_{z_i}. Если M представляет собой осмысленное сообщение или может быть сопоставлено с таковым по некоторому заранее оговоренному правилу, то значение $П$ может рассматриваться как цифровая подпись абонента i под сообщением M. Реально только владелец секретного алгоритма D_{z_i} может получить «открытый» текст $П$, который с помощью алгоритма E_{z_i} зашифровывается в осмысленную криптограмму M, поскольку лишь абонент i знает способ вычисления $f_{z_i}^{-1}$.

Абонент i может послать абоненту j также секретное сообщение с подписью. Для этого он зашифровывает S_i с помощью открытого алгоритма E_{z_j}, получая криптограмму [1]

$$C_i = E_{z_j}(П_i). \quad (4)$$

Получив зашифрованное сообщение, j-й абонент расшифровывает его своим секретным алгоритмом [1]

$$D_{z_j}(C_i) = П_i, \quad (5)$$

затем число $П_i$ зашифровывает открытым алгоритмом i-го абонента [1]

$$E_{z_i}(П_i) = M_i. \quad (6)$$

Таким образом, по полученной криптограмме C_i абонент j восстанавливает подпись абонента i и исходное сообщение.

Анализ известных вариантов ЭЦП показал следующие недостатки [1, 2]:

- передача секретного алгоритма (или ключа) между абонентами в сети требует использования канала, имеющего высокую скрытность;

- требование распределения чрезмерно большого объёма ключевого материала, делает использование данных систем ЭЦП очень дорогим.

Рассмотренные ниже ЭЦП, использующие двухключевую криптографию, позволяют устранить представленные недостатки.

Исследование применения алгоритма Мак-Элис для ЭЦП. При использовании алгоритма Мак-Элис для ЭЦП абонент i может послать абоненту j секретное сообщение M с подписью $П_i$, для этого абоненты должны выполнить следующую работу.

1. Абонент j берёт закрытые ключи - тройка двоичных матриц (S, G, P).

2. Абонент j вычисляет открытый ключ (матрицу произведения) $G_{pj(n\times k)} = SGP$, затем он публикует пару ($G_{pj(n\times k)}$, t_j) в справочнике открытых ключей сети.

3. Абонент i берет из справочника открытые ключи абонента j, выбирает случайный вектор e, имеющий длину n, вес $t \leq t_j$, и затем рассчитывает кодовое слово C по формуле

$$C = MG_{pj} + e, \quad (7)$$

где М- секретное сообщение, которое будет передано j-му абоненту. Здесь вектор e играет роль цифровой подписи i-го абонента.

4. Получая кодовое слово C, j-й абонент выполняет декодирование с использованием матриц (S, G, P) (как декодирование алгоритма Мак-Элис), после этого получает секретное сообщение M. Таким образом, без передачи секретного ключа между абонентами в сети i-й абонент послал j-му абоненту секретное сообщение со своей подписью, а j-й абонент открыл данное сообщение. Причем данный абонент может рассчитать (если он хочет проверить) цифровую подпись i-го абонента по формуле

$$e = C + MG_{pj}. \quad (8)$$

Таким образом, абонент j тоже может послать абоненту i секретное сообщение M_j с подписью $П_j$.

Использование алгоритма на рис. 2 для ЭЦП аналогично применению исходного алгоритма (рис.1). Различием между ЭЦП данных алгоритмов является состав ЭЦП. При применении алгоритма на рис. 2 для ЭЦП подпись включает две части $П_1$ и $П_2$, соответствующие векторам ошибки e_1 и e_2. Кроме того, при использовании данного алгоритма необходима передача объединенного закона [a_1, a_2, … a_m] между абонентами в сети по закрытому каналу.

Экспериментальные исследования. Результаты сравнения криптостойкости передаваемой информации исходной схеме ЭЦП и в случае использования алгоритма Мак-Элис (рис.

1 и рис. 2) с применением кода Гоппы (1024, 524) представлены в таблице.

Таблица

Алгоритм / Параметр	Исходная схема ЭЦП	Алгоритм рис. 1	Алгоритм рис. 2
$К_{ИО}$	–	$1{,}37\times10^{16}$	$>1{,}37\times10^{16}$
$К_{ИЗ}$	$6{,}5.10^{148}$	10^{197}	$>>10^{197}$
$К_{Э}$	3.10^{85}	3.10^{85}	6.10^{85}
$И_{Э}$	Закрытый ключ (G)	Открытый ключ (G_p,t)	Открытые ключи (G_{p1},t_1), (G_{p2},t_2) и [a_1, a_2, …a_m]
$С_{ИЭ}$	Закрытый канал	Справочник	Закрытый канал и справочник

где $К_{ИО}$ – криптостойкость информации по открытым ключам, $К_{ИЗ}$ – криптостойкость информации по закрытым ключам, $К_{Э}$– криптостойкость ЭЦП, $И_{Э}$ – передаваемая информация для ЭЦП между абонентами, $С_{ИЭ}$– среда передачи информации для ЭЦП между абонентами.

Выводы. Из анализа представленных ранее результатов следует, что в случае использования алгоритма Мак-Элис на рис. 1 не требуется передача секретного алгоритма (или ключа), при этом данный алгоритм обладает преимуществом по скрытности информации (~10^{50}). Кроме того, использование модифицированного алгоритма Мак-Элис (рис. 2) позволяет значительно повысить криптостойкость информации и увеличить в два раза криптостойкость системы ЭЦП по сравнению с применением исходной схемы (рис. 1).

Библиографический список

1. *Молдовян Н. А, Молдовян А. А*. Введение в криптосистемы с открытым ключом. С-Пб, 2005. 286 с.

2. *Венбо Мао.* Современная криптография теория и практика. М., С-Пб. Киев, 2005. 763 с.

3. *Алферов А.П. Зубов А.Ю*., *Кузьмин А.С*., *Черемушкин А.В*. Основы криптографии. М.: Гелиос АРВ, 2001. 480 с.