Электронная подпись на кодовых криптосистемах

УДК 004.056.55 Александр Кузнецов[1], Андрей Пушкарев[2], Анастасия Киян[1]

[1] *Харьковский национальный университет имени В.Н. Каразина, kuznetsov@karazin.ua, nastya93-1@mail.ru*
[2] *Администрация Госспецсвязи Украины*

В данной работе рассмотрены наиболее известные кодовые криптосистемы Мак-Элиса и Нидеррайтера, а также алгоритмы формирования и проверки электронной цифровой подписи (ЭЦП) на их основе. В частности, с использованием криптопреобразований по схеме Мак-Элиса предложена новая схема ЭЦП, которая по своим основным параметрам (стойкости, длине ключей и длине подписей) сопоставима с уже известной схемой CFS (Courtois, Finiasz, Sendrier). Основное отличие предложенной схемы ЭЦП состоит в способе формирования подписи: информационная последовательность (ее сжатый образ) интерпретируется не как синдром кодового слова (как в схеме CFS), а как искаженное ошибками кодовое слово.

Предлагаемый алгоритм формирования ЭЦП с

Шаг 1. Хеширование открытого текста M, т.е. вычисление хеш-кода $h(M)$. Присваивание переменной i значения $i=1$;

Шаг 2. Вычисление хеш-кода $h(h(M)\|i)$, где $h(M)\|i$ – конкатенация (объединение) значений $h(M)$ и i, представленных в виде двух последовательностей;

Шаг 3. Значение $h(h(M)\|i)$ интерпретируется как кодовое слово с ошибками $c_X^* = (c*_0, c*_1, ..., c*_{n-1})$, вычисленное для некоторых $I = (I_0, I_1, ..., I_{k-1})$ и $e = (e_0, e_1, ..., e_{n-1})$, причем $c = IG_X$, $c_X^* = c + e$, т.е. предполагается выполнение равенства $c_X^* = I \cdot G_X + e$ для соответствующего открытого ключа $G_X = X \cdot H \cdot P \cdot D$;

Шаг 4. Вычисление значения вектора

$$\overline{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1},$$

который (как предполагается) представляет собой искаженное не более чем в t разрядах кодовое слово алгебраического (n,k,d) кода с порождающей матрицей G и его можно декодировать быстрым алгоритмом полиномиальной сложности, т.е. предполагается, что

$$\overline{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1} = I \cdot X \cdot H + e \cdot D^{-1} \cdot P^{-1}$$

и алгоритм быстрого декодирования позволит найти вектор $I' = I \cdot X$ посредством декодирования слова $\overline{c}^* = I' \cdot G + e'$, $e' = e \cdot D^{-1} \cdot P^{-1}$;

Шаг 5. Для слова $\overline{c}^* = I' \cdot G + e'$ реализуется выполнение быстрого алгоритма декодирования:

– если декодирование успешно – выводятся найденные векторы $I' = I \cdot X$ и $e' = e \cdot D^{-1} \cdot P^{-1}$, которые соответствует вектору $\overline{c}^{*} = I' \cdot G + e'$;

– если декодирование не успешно – выдается сообщение о невозможности найти векторы $I' = I \cdot X$ и $e' = e \cdot D^{-1} \cdot P^{-1}$ для введенного вектора $\overline{c}^{*}$. Присваивание переменной i значения $i = i + 1$ и переход на Шаг 2;

Шаг 6. Вычисление векторов

$$I = I' X^{-1} \text{ и } e = e' \cdot D \cdot P;$$

Шаг 7. Формирование ЭЦП $Y = (I, e, i)$ для открытого текста M.

Таким образом, для формирования ЭЦП, вычисляется такое наименьшее положительное целое число i, для которого значение $h(h(M)\|i)$, интерпретируемое как кодовое слово с ошибками c_X^{*}, соответствует кодовому слову $c = IG_X$ и вектору ошибок e, т.е. формально запишем:

$$Y = (I, e, i) : IG_X + e = \left(h(h(M)\|i)\right).$$

Задача вычисления векторов I и e по известному вектору $h(h(M)\|i)$ сопряжена с решением задачи декодирования (n, k, d) кода:

– для уполномоченного пользователя (знающего секретный ключ) это вычислительно простая задача (полиномиальной сложности);

– для злоумышленника (знающего только открытый ключ) это вычислительно сложная задача декодирования случайного кода (относящаяся к классу сложности NP-полных задач).

Проверка подписи осуществляется посредством матричного умножения элементов подписи с проверкой полученного результата. Предложенная схема ЭЦП защищена от быстрой подделки подписи на основе добавления произвольного кодового слова применяемого кода. Указанное преимущество дополнительно усилено введенной проверкой веса Хемминга, которая предназначена для защиты от других гипотетических атак (например, одновременной подделки нескольких элементов подписи).

Проблемным вопросом практического применения ЭЦП на алгебраических кодах остается чрезвычайно высокая сложность формирования подписи. Ввиду того, что реальные кодовые характеристики при большой длине кода значительно уступают верхним кодовым границам, сложность формирования ЭЦП растет как факториал от исправляющей способности кода. Фактически, это означает, что с увеличением исправляющей способности практическое использование таких ЭЦП вычислительно недостижимо. Однако для совершенных кодов (удовлетворяющих верхней кодовой границе Хемминга) сложность формирования ЭЦП минимальна, она определяется сложностью быстрого декодирования используемого алгебраического кода. В этом смысле поиск кодов, удовлетворяющих верхним кодовым границам, приобретает особую актуальность.