Реализация алгоритма UMAC на крипто-кодовых конструкциях

УДК 681.3.06

Ольга Король[1], Алла Гаврилова[2]

Харьковский национальный экономический университет имени Семена Кузнеца, [1]olha.korol@hneu.net, [2]alla.gavrylova@hneu.net

В условиях современных угроз и реализации алгоритмов криптоанализа с применением полномасштабных квантовых компьютеров в будущем, использование известных алгоритмов SHA-3 и Европейского криптографического конкурса NESSIE в алгоритмах аутентификации и цифровой подписи из-за возможности их взлома ставится под сомнение.

Целью данной работы является обоснование расчетным путем на основании алгоритма UMAC необходимости использования крипто-кодовых конструкций Мак-Элиса с эллиптическими кодами для выявления модификаций открытого текста при передачи через открытый канал.

При разработке математической модели формирования хеш-кода в алгоритме UMAC, используется псевдослучайная последовательность, которая обеспечивает криптостойкость данного хеш-кода. В качестве алгоритма формирования подложки выступает крипто-кодовая конструкция Мак-Элиса на эллиптических кодах (ЕС).

Кодирование открытого сообщения отправителя для передачи по каналам связи выполнялось на основании следующих процедур.

I процедура. Формирование хеш-кода в алгоритме UMAC. Указанные преобразования проводим параллельно с формированием кодограммы. Данная процедура является итеративной и складывается из трехслойной структуры: 1) Y_{L1M} – первый слой, который является значением функции UHASH-hash первого уровня хеширования; 2) Y_{L2M} – второй слой, который является значением функции POLY-hash второго уровня хеширования; 3) Y_{L3M} – третий слой, который является значением функции Carter-Wegman-hash третьего уровня хеширования.

II процедура. Формирование криптограммы (C_X) с учетом одноразового сеансового секретного ключа *e.*

III процедура. Формирование псевдослучайной подкладки/подложки (*Pad*) для обеспечения криптостойкости алгоритма UMAC проводим с помощью функции *PDF*, причем различные части *Pad* можно будет использовать как дополнительный вектор инициализации.

IV процедура. Формирование кода контроля целостности и аутентичности кодограммы *Tag* рассчитывается на основании значений функций Y_{L3M} и *Pad*.

V процедура. Формирование значения суммарного кода достоверности передаваемого текста *(Y)* проведем на основании найденного значения хеш-кода Y_{L3M} и *Tag*.

Верификация хеш-кода на приемной стороне с использованием алгоритма UMAC осуществлялась следующим образом.

I процедура. Строим вектор, который является кодовым словом кода с порождающей матрицей *G*, искаженной не более чем в *t* разрядах.

II процедура. Получаем синдром ошибок S .

III процедура. Находим многочлен локатора ошибок ($\Lambda(x)$) с последующей локализацией ошибок по процедуре Ченя.

IV процедура. Определяем кратности ошибочных позиций, решив систему уравнений (расчет S').

V процедура. Получаем криптограмму C_X^* с учетом вектора ошибок e' .

VI процедура. C_X^* используется в качестве основы для формирования подложки по алгоритму UMAC.

Таблиця 1

Формализация показателей и результаты расчетов

№	***Показатель***	***Формула расчета***	***Значение показателя***
1	Y_{L3M} ,	$((Y_{L1I} \bmod(2^{36}-5)) \bmod 2^{32}) xor Y_{L32I}$,	10000000010
2	C_X	$I \times G_X^{EC} + e$	23023322
3	*Pad*	$PDF(K, Nonce, Taglen)$,	1101010
4	*Tag*	$Y_{L3M} \oplus Pad$	10001101100
5	*Y, Y'*	$Y_{L3M} \oplus Tag$	1101110
6	C_X^*	$C_X \times D^{-1} \times P^{-1}$	22202221
7	S	$C_X^* \times H^T$	1,1,1,0,0,0
8	$\Lambda(x)$	$a_{00} + a_{10}x + y = 0$	$x + y = 0$
9	S'	$H \times e'$	00020003
10	$C_X^{'}$	$C_X^* + e'$	22222224

Результат верификации, полученный при проведенных расчетах положителен, так как при сравнении хеш-кодов (полученного от отправителя и сформированного получателем) их длины совпадают. Следовательно, открытый текст, полученный через открытый канал получателем, не модифицирован.

В результате исследований разработаны практические алгоритмы формирования хеш-кода и его верификации на основе алгоритма UMAC с использованием крипто-кодовых конструкций Мак-Элиса на ЕС. Данный механизм аутентичности сообщений возможно использовать не только на эллиптических кодах, но и модифицированных (укороченных, и/или удлиненных) эллиптических кодах, а также на ущербных кодах с использованием гибридных крипто-кодовых конструкций. Такой подход позволяет практическую реализацию быстрого алгоритма хеширования с уровнем стойкости в постквантовой криптографии.