МОДИФИКАЦИЯ СХЕМЫ ВЫЧИСЛЕНИЯ ИМИТОВСТАВОК ВИГМАНА – КАРТЕРА

С.В. Агиевич

Белорусский государственный университет
НИИ прикладных проблем математики и информатики
пр. Независимости, 4 – 802, г. Минск, Беларусь
телефон: +(375)172095071; факс: +(375)172095104; e-mail: agievich@bsu.by

Схема Вигмана – Картера является одним из распространенных способов вычисления имитовставок – контрольных характеристик, которые определяются с использованием секретного ключа и открытых синхропосылок. Существенным недостатком схемы Вигмана – Картера является требование уникальности синхропосылок. Предлагается модификация схемы, лишенная данного недостатка.

Ключевые слова – контроль целостности, имитовставка, синхропосылка, схема Вигмана – Картера.

1 ВВЕДЕНИЕ

Имитовставки предназначены для криптографического контроля целостности сообщений. Стороны, располагающие общим секретным ключом θ, могут организовать такой контроль, используя алгоритм вычисления имитовставок G и алгоритм проверки имитовставок V. Алгоритм G берет на вход синхропосылку S, контролируемое сообщение X и вычисляет имитовставку $T = T_\theta(S, X)$. Алгоритм V берет на вход тройку (S, X, T) и возвращает ДА, если имитовставка T действительно вычислена для (S, X) на ключе θ, и НЕТ в противном случае. Фигурирующие здесь синхропосылки являются несекретными и, как правило, уникальными параметрами, которые отвечают за криптографическую надежность алгоритмов при многократном использовании одного и того же ключа.

При оценке надежности систем выработки имитовставки алгоритмы G и V принято называть оракулами, их входные данные – вопросами, а выходные – ответами. Считается, что оракулы снабжаются одинаковыми ключами θ, выбранными случайно равновероятно из множества допустимых ключей.

Оценка надежности проводится при следующих максимально благоприятных для противника условиях. Противник A (можно считать, что это некоторый вероятностный алгоритм) может задавать оракулам произвольные вопросы, анализировать ответы, строить по ним новые вопросы, снова получать ответы и т. д. Задачей противника является построение вопроса (S, X, T) такого, что $V(S, X, T) =$ ДА и вопрос (S, X) до этого не задавался оракулу G. Противник решает задачу с некоторой вероятностью $\mathbf{Adv}(A)$, которая называется преобладанием и определяется случайными данными, используемыми A в своей работе, а также случайным способом формирования θ.

Система выработки имитовставки считается стойкой, если преобладание $\mathbf{Adv}(A)$ мало для любого противника A с разумными ограничениями на его ресурсы. В качестве таких ограничений часто используют максимальное число вопросов, которые A может задать каждому из оракулов.

2 СХЕМА ВИГМАНА – КАРТЕРА

Пусть K – поле из N элементов. В схеме вычисления имитовставок Вигмана – Картера [4] синхропосылка S является элементом K, а в качестве ключа используется пара (H, π), где $H \in K$, π – подстановка на K. По сообщению X строится многочлен f_X над полем K такой, что $f_X \neq 0$, $f_X(0) = 0$, $\deg f_X \le D$, D много меньше N и различным сообщениям соответствуют различные многочлены. Имитовставка определяется по правилу:

$$T = f_X(H) + \pi(S). \qquad (1)$$

Считается, что преобразования зашифрования надежной блочной криптосистемы неотличимы от реализаций случайной подстановки с равномерным распределением на множестве всех подстановок. Поэтому на практике π выбирается как преобразование зашифрования некоторой блочной криптосистемы, а H определяют как результат зашифрования некоторого фиксированного элемента K.

Ограничения на образы отображения $X \mapsto f_X$ означают, что при случайном равновероятном выборе H для различных сообщений X и X' вероятность

$$\mathbf{P}\{f_X(H) = f_{X'}(H)\} = \mathbf{P}\{H \text{ – корень } f_X - f_{X'}\} \le \frac{D}{N},$$

т. е. невелика.

Данное наблюдение позволяет получить следующее обоснование надежности схемы Вигмана – Картера.

Теорема 1 (Бернштейн [2]). Пусть оракулы G, V реализуют схему вычисления имитовставок Вигмана – Картера вида (1), в которой ключ (H, π) выбран случайно равновероятно. Пусть противник A задает не более q_G вопросов оракулу G, не более q_V вопросов оракулу V и не по-

вторяет синхропосылки в вопросах G. Тогда

$$\mathbf{Adv}(A) \le \frac{q_V D}{N}\left(1-\frac{q_G}{N}\right)^{-(q_G+1)/2}.$$

Легко проверить, что оценка теоремы остается полезной, пока отношение q_G^2 / N невелико.

Важно, что обоснование надежности схемы Вигмана – Картера выполняется при условии уникальности синхропосылок в вопросах G. Дело в том, что ответы

$$T = f_X(H) + \pi(S), \quad T' = f_{X'}(H) + \pi(S), \quad X \ne X',$$

позволяют противнику определить H как один из корней полиномиального уравнения $f_X(H) - f_{X'}(H) = T - T'$ (*для локализации H нужно решить несколько таких уравнений, которые соответствуют нескольким повторам синхропосылок*). После определения H противник может вычислить $\pi(S) = T - f_X(H)$ и для любого X'' построить имитовставку $T'' = f_{X''}(H) + \pi(S)$ такую, что $V(S, X'', T'') = \text{ДА}$.

Уникальность синхропосылок является важным требованием, которое выдвигается для многих криптографических протоколов. Однако, в большинстве известных нам случаев повтор синхропосылок может привести к компрометации *отдельного* сообщения протокола, но не к обходу контроля целостности *любого* сообщения, как в схеме Вигмана – Картера.

Проблема уникальности синхропосылок рассмотрена в стандарте [3], который определяет режим одновременного шифрования и имитозащиты GCM, основанный на схеме Вигмана - Картера. Фактически в стандарте предлагается ряд инженерных решений по генерации синхропосылок внутри криптографических устройств без контроля со стороны противника.

3 МОДИФИЦИРОВАННАЯ СХЕМА ВИГМАНА – КАРТЕРА

Вместо достаточно сложных способов обеспечения уникальности синхропосылок мы предлагаем модифицировать схему Вигмана – Картера так, чтобы ее надежность можно было обосновать даже при повторе синхропосылок.

В предлагаемой схеме ключом является подстановка π, действующая на K. Как и в схеме Вигмана – Картера, по сообщению X строится многочлен f_X с предыдущими ограничениями. Имитовставки определяются по правилу:

$$T = \pi(f_X(\pi(S))). \qquad (2)$$

В модифицированной схеме значения многочленов f_X вычисляются, вообще говоря, в различных точках $H = \pi(S)$. Известно (см. [1, теорема 6.13]), что многочлен $f(y,z) = f_X(y) - f_{X'}(z) \in K[y,z]$ имеет не более $\deg f \cdot N$ корней в K^2. Поэтому для случайных равновероятных независимых H, H' и для любых сообщений X, X' справедлива оценка:

$$\mathbf{P}\{f_X(H) = f_{X'}(H')\} \le \frac{\max(\deg f_X, \deg f_{X'})N}{N^2} \le \frac{D}{N}.$$

Данное наблюдение позволяет доказать следующую теорему.

Теорема 2. Пусть оракулы G, V реализуют схему вычисления имитовставок вида (2), в которой ключ π выбран случайно равновероятно. Пусть противник A' задает не более q_G вопросов оракулу G и не более q_V вопросов оракулу V. Тогда

$$\mathbf{Adv}(A') \le \frac{q_V (D+2)(q_G+1)^2}{N}.$$

Как и в предыдущей теореме, полученная оценка остается полезной, пока отношение q_G^2 / N невелико. При этом последняя оценка хуже и преобладание у противника A' может быть больше, чем у противника A из теоремы 1. Сказанное не означает, что схема (2) менее надежна, чем схема (1). Действительно, A' в отличие от A может повторять имитовставки, т. е. обладает большим потенциалом.

ЛИТЕРАТУРА

[1] Лидл, Р., Нидеррайтер, Г. Конечные поля: В 2 т. М.: Мир. 1988.

[2] Bernshtein D. Stronger security bounds for permutations // Unpublished manuscript. – 2005. Avail. at: http://cr.yp.to/antiforgery/permutations-20050323.ps. This work refines "Stronger security bounds for Wegman Carter – Shoup authenticators", Advances in Cryptology – EUROCRYPT 2005, Springer-Verlag, LNCS 3494. – 2005. – P. 164–180.

[3] Recommendation for Block Cipher Modes of Operation: Galois-Counter Mode (GCM) for Confidentiality and Authentication // NIST Special Publication 800-38D. – 2007. – Avail. at: http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf.

[4] Wegman, M., Carter, J. New hash functions and their use in authentication and set equality // Journal of Computer and System Sciences. – 1981. – Vol. 22. – P. 265–279.