Модификация схемы вычисления имитовставок Вигмана – Картера

С.В. Агиевич

Аннотация

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.

1 Введение

Имитовставки предназначены для 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 снаряжаются 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 данную 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 ка-

честве таких ограничений часто используют максимальное число вопросов, которые A задает 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 $f_X \neq 0$, $f_X(0) = 0$, $\deg f_X \leq D \ll N$ и различным сообщениям соответствуют различные многочлены. Имитовставка определяется по правилу:

$$T = f_X(H) + \pi(S). \tag{1}$$

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 является результатом зашифрования некоторого фикисированного элемента K.

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

$$\mathsf{P}\left\{f_X(H) = f_{X'}(H)\right\} = \mathsf{P}\left\{H \text{ — корень } f_X - f_{X'}\right\} \leq \frac{\deg(f_X - f_{X'})}{N} \leq \frac{D}{N},$$

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 повторяет синхропосылки в вопросах G. Тогда

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

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

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

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

позволяют противнику определить H как один из корней полиномиального уравнения $f_X(H) - f_{X'}(H) = T - T'$ (для локализации H можно решить несколько таких уравнений, которые соответствуют другим 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 $V(S, X'', T'') = \texttt{ДА}$.

Уникальность синхропосылок является важным требованием, которое выдвигается для многих криптографических алгоритмов и протоколов. Однако, в большинстве

известных нам случаев повтор синхропосылок может привести к компрометации *отдельного* сообщения, 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 сихнропосылок внутри криптографических устройств без контроля со стороны противника.

3 Модификация схемы 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:

$$T = \pi(f_X(\pi(S))). \tag{2}$$

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

$$\mathsf{P}\left\{f_X(H) = f_{X'}(H')\right\} \leq \frac{\max(\deg f_X, \deg f_{X'})N}{N^2} \leq \frac{D}{N}.$$

Данная оценка 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

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

Преобладание у противника A' может быть больше, чем у противника A из теоремы 1. При этом не следует считать, что схема (2) менее надежна, чем схема (1). Действительно, A' в отличие от A может повторять имитовставки, т. е. обладает большим потенциалом.

Доказательство. **1**. Для простоты вместо X будем писать соответствующий ему многочлен f_X или даже просто f.

2. Рассмотрим взаимодействие противника с оракулом V. Будем считать, что вопросы оракулу не повторяются и при известном ответе $G(S, f)$ противник не задает V бесполезных вопросов (S, f, T), где T — произвольная допустимая имитовставка.

Атака A заканчивается ответом V на некоторый вопрос (S, f, T), который можно считать *попыткой подделки* (попытка удалась, если $V(S, f, T) = \texttt{ДА}$). Пусть A делает $q_V > 1$ таких попыток. Тогда выделим в его атаке две части:

1) первая часть атаки заканчивается первой попыткой подделки;

2) вторая часть — это вся атака с одной поправкой: симулятор, который выполняет противника-как-программу и организует взаимодействие этой программы с оракулами, контролирует первый вопрос V и дает на него ответ `НЕТ`. Можно считать, что такой контроль — это просто модификация программы A. Модифицированная программа делает $q_V - 1$ попыток подделки и удовлетворяет тем же ограничениям на ресурсы, что и первоначальная программа.

Пусть вероятности успеха первой и второй части атаки ограничены величинами p_1 и p_2. Тогда $\mathbf{Adv}(A) \le p_1 + p_2$. Если во второй части атаки A делает более одной попытки подделки, то ее снова можно разбить на две части и так далее. В конце концов, $\mathbf{Adv}(A) \le q_V p_1$ и остается рассмотреть атаку с одной попыткой подделки и получить оценку для p_1.

3. Будем считать, что A задает единственный вопрос V (попытка подделки) в последнюю очередь (вопросы G после вопроса V не изменяют вероятности успеха атаки). Будем считать, что A не повторяет вопросы и задает в точности q_G вопросов оракулу G (A может просто игнорировать ответы на некоторые вопросы). Пусть (S_i, f_i) — вопросы G, T_i — соответствующие ответы. Пусть также (S, f, T) — искомая попытка подделки — вопрос V.

4. В сделанных обозначениях атака A для случайно выбираемого ключа π может быть описана следующей игрой:

Игра G_0 (единичная подделка)

---

1. $\pi \xleftarrow{R} \mathfrak{S}(K)$, $\mathfrak{S}(K)$ — множество всех подстановок на K.
2. Для $i = 1, \ldots, q_G$:
   (a) $(S_i, f_i) \leftarrow A_{G,i}(T_1, \ldots, T_{i-1})$;
   (b) $z_i \leftarrow f_i(\pi(S_i))$;
   (c) $T_i \leftarrow \pi(z_i)$.
3. $(S, f, T) \leftarrow A_V(T_1, \ldots, T_{q_G})$.
4. $z \leftarrow f(\pi(S))$;
5. $T' \leftarrow \pi(z)$.
6. $b \leftarrow [T \stackrel{?}{=} T']$.

В ходе игры подпрограммы $A_{G,i}$ составляют вопросы, а подпрограмма A_V генерирует подделку имитовставки.

Будем упрощать G_0 и строить последовательность игр G_1, G_2. В каждой игре G_i выделим событие $\mathcal{E}_i = \{b = 1\}$. Вероятность $\mathsf{P}\{\mathcal{E}_0\}$ является искомым преобладанием $\mathbf{Adv}(A)$. Для оценки преобладания оценим $\mathsf{P}\{\mathcal{E}_2\}$ и штрафы $|\mathsf{P}\{\mathcal{E}_i\} - \mathsf{P}\{\mathcal{E}_{i-1}\}|$, $i = 1, 2$, за переходы между играми.

Игра G_1 (переход по неразличимости и модели)

---

1. Организовать поддержку оракула π, который на вопросы $a \in K$ дает ответы $\pi(a) \in K$. Ответы оракул дает во время игры. Если вопрос a повторяется, то повторяется и ответ $\pi(a)$. Если вопрос a не задавался (пишем $\pi(a) = \perp$), то ответ выбирается наудачу из K (пишем $\pi(a) \xleftarrow{R} K$).
2. Для $i = 1, \ldots, q_G$:
   (a) $(S_i, f_i) \leftarrow A_{G,i}(T_1, \ldots, T_{i-1})$;
   (b) если $\pi(S_i) = \perp$, то $\pi(S_i) \xleftarrow{R} K$; $z_i \leftarrow f_i(\pi(S_i))$;
   (c) если $\pi(z_i) = \perp$, то $\pi(z_i) \xleftarrow{R} K$; $T_i \leftarrow \pi(z_i)$.
3. $(S, f, T) \leftarrow A_V(T_1, \ldots, T_{q_G})$.
4. Если $\pi(S) = \perp$, то $\pi(S) \xleftarrow{R} K$; $z \leftarrow f(\pi(S))$.
5. Если $\pi(z) = \perp$, то $T' \xleftarrow{R} K$, иначе $T' \leftarrow \pi(z)$.
6. $b \leftarrow [T \stackrel{?}{=} T']$.

В игре G_0 неявно используется оракул π, который реализует случайный выбор подстановки. В игре G_1 оракул π описан явно, но здесь он реализует случайный выбор уже не подстановки, а произвольного преобразования.

В играх G_0 и G_1 задается $2q_G + 2$ вопросов оракулу π. Преобладание при различении между подстановками и преобразованиями ограничено величиной $(2q_G+2)(2q_G+1)/(2N)$. Поэтому справедлива оценка

$$|\mathsf{P}\{\mathcal{E}_1\} - \mathsf{P}\{\mathcal{E}_0\}| < \frac{(q_G + 1)(2q_G + 1)}{N}.$$

Игра G_2 (переход по событию-сбою)

---

1. Организовать поддержку оракула π.
2. $bad \leftarrow 0$.
3. Для $i = 1, \ldots, q_G$:
   (a) $(S_i, f_i) \leftarrow A_{G,i}(T_1, \ldots, T_{i-1})$;

(b) если $\pi(S_i) = \perp$, то $\pi(S_i) \xleftarrow{R} K$; $z_i \leftarrow f_i(\pi(S_i))$;

(c) $\boxed{\tilde{T}_i \xleftarrow{R} K;\ T_i \leftarrow \tilde{T}_i;\ \text{если } \pi(z_i) = \perp, \text{ то } \pi(z_i) \leftarrow \tilde{T}_i, \text{ иначе } bad \leftarrow 1}$.

4. $(S, f, T) \leftarrow A_V(T_1, \ldots, T_{q_G})$.

5. Если $\pi(S) = \perp$, то $\pi(S) \xleftarrow{R} K$; $z \leftarrow f(\pi(S))$.

6. $\boxed{\tilde{T} \xleftarrow{R} K;\ T' \leftarrow \tilde{T};\ \text{если } \pi(z) = \perp, \text{ то } \pi(z) \leftarrow \tilde{T}, \text{ иначе } bad \leftarrow 1}$.

7. $b \leftarrow [T \stackrel{?}{=} T']$.

В игре G_2 противник получает на вопросы оракулам случайные независимые равновероятные ответы T_i, T. При этом

$$\mathsf{P}\{\mathcal{E}_2\} = \mathsf{P}\{T = T'\} = \frac{1}{N}.$$

Введем в рассмотрение событие-сбой

$$\mathcal{F} = \{bad = 1 \text{ в игре } G_2\}$$

и оценим его вероятность.

Пусть переменная bad устанавливается равной 1, когда $\pi(z_i) = \perp$, точнее, когда $z_i = S_j$, $1 \le j \le i$. Равенство означает, что $\pi(S_i)$ является корнем многочлена $f_i - S_j$. Но

(a) многочлен имеет не более $\deg f_i$ корней в поле K,

(b) $f_i - S_j$ и $\pi(S_i)$ статистически независимы (значение $\pi(S_i)$ выбирается независимо от f_i и S_j),

(c) $\pi(S_i)$ имеет равномерное распределение на K.

Поэтому

$$\mathsf{P}\{z_i = S_j\} \le \frac{\deg f_i}{N} \le \frac{D}{N}.$$

Пусть переменная bad устанавливается равной 1, когда $\pi(z_i) = \perp$, точнее, когда $z_i = z_j$, $1 \le j < i$. Если $S_i = S_j$, то $f_i \ne f_j$ и

$$\mathsf{P}\{z_i = z_j\} = \mathsf{P}\{\pi(S_i) \text{ – корень многочлена } f_i - f_j\} \le \frac{\max(\deg f_j, \deg f_{j'})}{N} \le \frac{D}{N}.$$

Если же $S_i \ne S_j$, то

$$\mathsf{P}\{z_i = z_j\} = \mathsf{P}\{(\pi(S_i), \pi(S_j)) \text{ – корень } f(a,b) = f_i(a) - f_j(b)\} \le \frac{\deg f \cdot N}{N^2} \le \frac{D}{N}.$$

Здесь мы использовали оценку для числа корней многочлена от нескольких переменных: многочлен $f \in K[x_1, \ldots, x_n]$ степени d имеет не более dN^{n-1} корней в K^n (см. [1, теорема 6.13]).

Приведенные формулы остаются справедливыми при замене тройки (S_i, f_i, z_i), $1 \le i \le q_G$, на тройку (S, f, z). Последнюю тройку обозначим через $(S_{q_G+1}, f_{q_G+1}, z_{q_G+1})$ и дополним ею список $\{(S_i, f_i, z_i)\}$.

Перечислим равенства, которые могут привести к установке $bad \leftarrow 1$. Всего имеется:

– $(q_G + 1)(q_G + 2)/2$ равенств $z_i = S_j$, $1 \le i \le j \le q_G + 1$;

– $q_G(q_G + 1)/2$ равенств $z_i = z_j$, $1 \le j < i \le q_G + 1$.

Учитывая вероятности выполнения равенств каждого типа, получаем

$$\mathsf{P}\{\mathcal{F}\} \le \frac{D}{N}(q_G + 1)^2.$$

До начала строки, в которой переменная *bad* устанавливается равной 1, игра G_2 проходит также, как и G_1. Поэтому

$$|\mathsf{P}\{\mathcal{E}_2\} - \mathsf{P}\{\mathcal{E}_1\}| \le \mathsf{P}\{\mathcal{F}\}.$$

Собирая все найденные оценки, получаем:

$$\begin{aligned}\mathbf{Adv}(A) = \mathsf{P}\{\mathcal{E}_0\} &= \mathsf{P}\{\mathcal{E}_2\} + |\mathsf{P}\{\mathcal{E}_2\} - \mathsf{P}\{\mathcal{E}_1\}| + |\mathsf{P}\{\mathcal{E}_1\} - \mathsf{P}\{\mathcal{E}_0\}| < \\ &< \frac{1}{N} + \frac{1}{N}(q_G + 1)(2q_G + 1) + \frac{D}{N}(q_G + 1)^2 < \\ &< \frac{(D + 2)(q_G + 1)^2}{N}.\end{aligned}$$

что и требовалось доказать. □

Список литературы

[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.