УДК 681.3.06

КОЛЛИЗИОННЫЕ ХАРАКТЕРИСТИКИ УНИВЕРСАЛЬНЫХ КЛАССОВ ХЕШ-ФУНКЦИЙ

Е.А. Артеменко
(Украинская государственная академия железнодорожного транспорта, Харьков)

Рассмотрены оценки секретности для универсальных классов хеш-функций. Получены выражения для вероятности имитации и подмены сообщений.

хеш-функции, коллизионные характеристики

Введение. Универсальные семейства хеш-функций являются объектами полевых структур, характеризуются прозрачными комбинаторными свойствами и имеют доказуемую секретность. Основные положения универсального хеширование приведены в работах Картера–Вегмана [1], Стинсона [2], ряд дополнений и уточнений сделаны в [3]. Для целей аутентификации важное значение имеют оценки коллизионной стойкости схем хеширования.

Основные результаты по оценке секретности MAC кодов представлены в работах [2, 4]. Задачей статьи является вывод оценок коллизионной стойкости для универсальных семейств хеш-функций. С этой целью, в статье получены выражения для вероятностей успеха имитационной атаки и атаки подмены универсальных хеш-классов.

Оценки вероятности успеха имитационной атаки и атаки подмены для универсальных классов хеш-функций. Приведем определения универсальных классов и рассмотрим их коллизионные свойства.

Определение 1. (N,n,m) хеш-семейство есть множество из N функций H такое, что

$$h : A \to B, \tag{1}$$

где $h \in H$; $|A| = n$ и $|B| = M$, $n \geq m$.

Определение 2. (N,n,m) хеш-семейство является ε-универсальным, если для любых двух различных элементов $x_1, x_2 \in A$ существует самое большее $\varepsilon \times N$ функций $h \in H$ таких, что $h(x_1) = h(x_2)$. Аббревиатура $\varepsilon - U$ используется для обозначения ε-универсальных хеш-функций.

Очевидно, если h выбирается случайно из заданного $\varepsilon - U(N,n,m)$ хеш-семейства, тогда вероятность коллизии хеш-значений для двух разных входных сообщений $x_1, x_2 \in A$ не превышает ε:

$$P_{кол} = Pr_{h \in H}[h(x_1) = h(x_2)] \le \varepsilon . \quad (2)$$

Первоначальное определение универсальных хеш-функций Картера и Вегмана было предложено для $\varepsilon = 1/m$. Очевидно, что вероятность коллизии для универсальных хеш-функций Картера и Вегмана является наименьшей и определяется мощностью пространства хеш-значений

$$P_{кол} = 1/B . \quad (3)$$

Вероятность подмены сообщения x на ложное x', $x \ne x'$ при условии, что используется один и тот же аутентификатор, т.е. $y \ne y'$, назовем это вероятностью подмены первого рода, будет равна вероятности коллизии

$$P_{под.1} = P_{кол} . \quad (4)$$

Определение 3. H является ε-почти универсальным семейством хеш-функций $\varepsilon - AU(N,n,m)$, если $P_{кол} = Pr_{h \in H}[h(x_1) = h(x_2)] \le \varepsilon$ для $x_1, x_2 \in A$, $x_1 \ne x_2$, $1/m < \varepsilon < 1$.

Очевидно, что для почти универсальных семейств несколько ослабляются требования к вероятности коллизии.

Свойство универсальности (почти универсальности) не связанно с распределением MAC значений по ключевому пространству и, следовательно, не определяет вероятностные характеристики имитационной атаки. Дальнейшим развитием универсальных схем являются строго универсальные.

Определение 4. (N,n,m) хеш-семейство является ε- строго универсальным $\varepsilon - SU(N,n,m)$, если для каждого $x \in A$ и $y \in B$ число функций $h \in H$ таких, что $h(x) = y$ равно N/m, а для любых двух различных элементов $x_1, x_2 \in A$ и не обязательно различных $y_1, y_2 \in B$ число ν функций $h \in H$ таких, что $h(x_1) = y_1$, $h(x_2) = y_2$ не превышает $\nu \le \varepsilon \cdot N/m$.

Аббревиатура $\varepsilon - SU$ используется для обозначения ε- строго универсальных хеш-функций.

Строгая универсальность определена для $\varepsilon = 1/m$. При смягчении требования к $\varepsilon > 1/m$ класс функций определяется как почти строго универсальный $\varepsilon - \mathrm{ASU}$.

Коллизионные свойства строго универсальных MAC кодов представлены следующим утверждением.

Утверждение 1. Пусть $\varepsilon - \mathrm{SU}(N, n, m)$ семейство хеш-функций. При равновероятном выборе хеш-функции вероятность успеха имитационной атаки равна

$$P_{им} = \frac{1}{m}, \tag{5}$$

а вероятность подмены

$$P_{под} \le \varepsilon. \tag{6}$$

Вероятность успеха имитационной атаки определяется вероятностью угадывания ключа $P_{им.Кл}$ или вероятностью угадывания MAC кода $P_{им.MAC}$.

В силу того, что число записей со значением y в каждом столбце матрицы отображения $A \to B$ встречается одинаковое число раз, получим

$$P_{им.} = P_{им.Кл} = P_{им.MAC} = \frac{\left|\{h \in H : y = f(x)\}\right|}{|H|} = \frac{N/m}{N} = \frac{1}{m}.$$

Вероятность подмены определяется условной вероятностью

$$P_{под} = P(h(x') = y' - \text{истинно} \,|\, h(x) = y) = \frac{\left|\{f \in H : y = f(x), y' = f(x')\}\right|}{\left|\{f \in H : y = f(x)\}\right|}.$$

Так как число h, для которого $h(x) = y$, равно N/m, а число h, для которого $h(x) = y$ – $h(x') = y'$.

В силу того, что $\nu \le \varepsilon N/m$, тогда подставляя оценки N/m и $\varepsilon N/m$ в выражение для $P_{под}$, получим

$$P_{под} = P_{под.1} = P_{под.2} \le P_{кол} = \varepsilon,$$

где $P_{под.2}$ – вероятность подмены второго рода, есть вероятность подмены сообщения x на ложное x', при условии, что $y = y'$.

Характеристики универсальных классов хеш-функций приведены в табл. 1.

Определения универсальных и почти универсальных хеш-классов не учитывают статистические распределения аутентификаторов на про-

странстве значений ключей и в ряде практических приложений не позволяют получить оценки их коллизионной стойкости. Строго универсальный хеш-класс характеризуется наименьшим значением вероятности имитации $P_{им} = 1/m$.

Таблица 1

Коллизионные свойства универсальных хеш-функций

№ п/п	Универсальные классы хеш-функций	$P_{им}$		$P_{под}$	
		$P_{им.Кл}$	$P_{им.MAC}$	$P_{под\ 1}$	$P_{под\ 2}$
1	ε–U(N;n,m)			1/m	
2	ε–AU(N;n,m)			ε	
3	ε–SU(N;n,m)	1/m	1/m	1/m	1/m
4	ε–ASU(N;n,m)	ε	1/m	ε	ε

Распределение аутентификаторов по ключевому пространству является определяющим при оценке стойкости MAC кодов к имитационной атаке.

Выводы. Определение универсальных и почти универсальных хеш-классов не учитывает статистические распределения аутентификаторов на пространстве значений ключей, знание которых позволяет уточнить оценки их имитационной стойкости.

Наличие смещения в распределении MAC значений приводит к увеличению вероятности имитационной атаки и атаки подмены.

Строго универсальный хеш-класс характеризуется наименьшим значением вероятности имитации и определяется массивом хеш-значений со смещением равным нулю.

ЛИТЕРАТУРА

1. *Carter J.L., Wegman M.N. Universal classes of hash functions // J. Computer and System. – 1979. – Sci. 18. – P. 143-154.*
2. *Stinson D. Universal hashing and authentication codes // Design, Codes and Cryptography. – 1994. – Vol. 4. – P. 369-380.*
3. *Халимов Г.З., Кузнецов А.А. Аутентификация и универсальное хеширование // Радиотехника. Всеукр. межвед. науч.-техн. сб. – 2001. – Вып. 120. – С. 100-110.*
4. *Kurosawa K., Johansson T., Stinson D. Almost k-wise independent sample spaces and their cryptologic applications // Lecture Notes in Computer Science. – 1997. – Vol. 1233. – P. 409-421.*

Поступила 14.12.2005

Рецензент: доктор технических наук, профессор Ю.В. Стасев,
Харьковский университет Воздушных Сил им. И. Кожедуба.