

**МЕТОД ФОРМИРОВАНИЯ ОБОБЩЕННЫХ ХЕШИРУЮЩИХ ФУНКЦИЙ
НА ОСНОВЕ АЛГЕБРАИЧЕСКИХ КОДОВ**

к.т.н. А.А. Кузнецов, А.В. Ивашкин, Я.Ю. Стасева
(представил д.ф.-м.н., проф. С.В. Смеляков)

Разрабатывается метод формирования обобщенных хеширующих функций (ХФ) на основе использования алгебраических кодов. Предлагается композиционная конструкция формирования строго универсальных классов на их основе.

Постановка проблемы в общем виде. Известные методы имитозащиты цифровых сообщений основаны на внесении избыточности (имитовставки, кода аутентификации, цифровой подписи) в передаваемую последовательность. Одним из перспективных направлений в развитии методов имитозащиты является использование строго универсальных классов хеширующих функций (СУКХФ). Предложенные в работах [1 – 7] схемы имитозащиты с использованием СУКХФ имеют существенное преимущество, заключающееся в том, что для них получены точные выражения, связывающие вероятность коллизии с объемом ключевых данных. Несмотря на потенциально высокие показатели стойкости, в виду высокой сложности реализации, практическое использование подобных схем ограничено. Актуальной научно-технической задачей является разработка и исследование эффективных методов формирования СУКХФ, допускающих простую реализацию.

Анализ последних исследований и публикаций. Впервые классификация хеш-функций по классам универсальных и строго универсальных функций предложена в [1 – 2]. В работах [3 – 5] предложена композиционная схема формирования СУКХФ, снимающая основное ограничение по практическому использованию таких схем – большой объем ключа. В работах [6 – 7] предложены методы построения СУКХФ на основе композиционных конструкций с использованием алгеброгеометрических кодов. Однако для получения малой величины вероятности коллизий в рассмотренных схемах необходимо реализовать операции над расширенными полями $GF(2^{50}) - GF(2^{100})$. Практические схемы для подобных вычислений громоздки и малоэффективны.

Целью статьи является теоретическое обобщение универсального класса хеш-функций (УКХФ), основанного на использовании алгебраи-

ческих кодов, разработка практических схем, позволяющих снизить кратность групповых операций при сохранении высоких показателей стойкости.

Основная часть. Предлагаемый метод формирования СУКХФ основан на использовании композиционной схемы универсального и строго универсального классов ХФ. На первой ступени композиции предлагается использовать алгебраический код, тождественный множеству функций отображения кодовых слов в l -наборы кодовых символов, $l \in Z^+$. Справедливо следующее утверждение.

Утверждение 1. Код длины N с n -кодowymi словами, основанием m и относительным кодовым расстоянием $1-\varepsilon$ эквивалентен универсальному классу хеш-функций с параметрами $\varepsilon^l - U(N^l, n, m^l)$, т.е. множеству H из N функций, осуществляющих отображение $f: X \rightarrow Y$ такое, что для двух различных элементов $x_1, x_2 \in X$ существует не больше, чем $N^l \cdot \varepsilon^l$ функций $f \in H$ таких, что $f(x_1) = f(x_2)$.

Доказательство. Действие функций f из множества H состоит в отображении m -ичного кодового слова длиной N символов в l -набор кодовых символов. Мощность множества образов $|Y| = m^l$. Мощность множества H как мощность l -наборов из N символов задается $|H| = N^l$.

Пусть d – минимальное кодовое расстояние, т.е. минимальное число символов, в которых различаются два произвольных кодовых слова, $\varepsilon = \frac{n-d}{n}$. Это означает, что два произвольных кодовых слова совпадут в $\leq (n-d)$ символах. Верхняя оценка для вероятности совпадения одного символа запишется в виде $P_1 \leq \frac{n-d}{n} = \varepsilon$. Совпадения символов – события независимые, верхняя оценка для вероятности совпадения l -набора символов запишется как $P_l = (P_1)^l \leq \left(\frac{n-d}{n}\right)^l = \varepsilon^l$. Для двух различных l -наборов x_1 и x_2 существует не больше, чем $N^l \cdot \varepsilon^l$ функций $f \in H$ таких, что $f(x_1) = f(x_2)$.

Утверждение 2. Композиция из универсального класса хеш-функций $\varepsilon_1^l - U(N_1^l, n, u^l)$ и строго универсального класса хеш-функций

$\varepsilon_2 - \text{SU}(N_2, n, m)$ является строго универсальным классом с параметрами $\varepsilon - \text{SU}(N_1^l N_2, n, m)$, где $\varepsilon = \varepsilon_1^l + \varepsilon_2 - \varepsilon_1^l \varepsilon_2$.

Доказательство. Действительно, используя определения композиционной конструкции и результат теоремы 5, подставим параметры универсального класса $\varepsilon_1^l - U(N_1^l, n, u^l)$ и строго универсального класса $\varepsilon_2 - \text{SU}(N_2, n, m)$, получим СУКХФ с параметрами $\varepsilon - \text{SU}(N, n, m)$, где $N = N_1^l N_2$, $\varepsilon = \varepsilon_1^l + \varepsilon_2 - \varepsilon_1^l \varepsilon_2$.

Составляющая N_2 в композиционной конструкции $N = N_1 \circ N_2$ представляет класс строго универсальных хеш-функций, и его можно построить, используя простые ортогональные массивы [3 – 6]. Компонента N_1 в нашем случае является универсальным классом $\varepsilon_1^l - U(N_1^l, n, u^l)$.

Очевидно, что для его построения необходимо использовать коды с большим основанием, большой длины и большим относительным кодовым расстоянием, так как в этом случае получим большой объем ключей аутентификации и малую вероятность коллизии аутентификаторов.

Рассмотрим композиционную конструкцию обобщенного СУКХФ $(\varepsilon_1^l + \varepsilon_2 - \varepsilon_1^l \varepsilon_2) - \text{SU}(N_1^l N_2, n, m)$ с алгеброгеометрическими кодами. Справедливо следующее утверждение.

Утверждение 3. Пусть q – простое число, a, b, l – натуральные числа, причем $a > b$. Тогда строго универсальный класс хеш-функций в композиционной конструкции с алгебраическим кодом имеет параметры:

$$\frac{2}{q^b} - \text{SU} \left(q^{2a+l+b}, q^{aq^{a-b/l}}, q^b \right) \text{ (RS-код);} \quad (1)$$

$$\frac{2}{q^b} - \text{SU} \left((2q^{a/2} + q^a + 1)^l \cdot q^{la+b}, q^a (2q^{a/2-b/l} + q^{a-b/l} + q^{-b/l}), q^b \right) \text{ (EC-код);} \quad (2)$$

$$\frac{2}{q^b} - \text{SU} \left(q^{\frac{5a}{2}+b}, q^{\frac{a(2q^{3a/2-b/l} - q^a + q^{a/2} + 2)}{2}}, q^b \right) \text{ (HC-код, } a \text{ – четное);} \quad (3)$$

$$\frac{2}{q^b} - \text{SU} \left(q^{3a+l+b}, q^{\frac{a(2q^{5a/2-b/l} - q^{2a} + q^a + 2q^{a/2})}{2q^{a/2}}}, q^b \right) \text{ (SC-код, } a \text{ – нечетное).} \quad (4)$$

Доказательство. Используя код Рида-Соломона и простой ортогональный массив, построим обобщенный СУКХФ. Имеем $\frac{k^l}{q^{la}} + \frac{1}{q^b} - \text{SU}\left(q^{2la+b}, q^{ak}, q^b\right)$. Зафиксируем вероятность коллизии

$\varepsilon = \frac{2}{q^b}$, т.е. $\frac{k^l}{q^{la}} + \frac{1}{q^b} = \frac{2}{q^b}$. Выразив k , получим $k = q^{a-b/l}$. Подставив ε и k в получим $\frac{2}{q^b} - \text{SU}\left(q^{2al+b}, q^{aq^{a-b/l}}, q^b\right)$.

Используя код, построенный по эллиптической кривой и простой ортогональный массив, построим обобщенный СУКХФ. Имеем $\frac{k^l}{\left(2q^{a/2} + q^a + 1\right)^l} + \frac{1}{q^b} - \text{SU}\left(\left(2q^{a/2} + q^a + 1\right) \cdot q^{la+b}, q^{ak}, q^b\right)$. Зафиксируем

вероятность коллизии $\varepsilon = \frac{2}{q^b}$, т.е. $\frac{k^l}{\left(2q^{a/2} + q^a + 1\right)^l} + \frac{1}{q^b} = \frac{2}{q^b}$. Выразив k , получим $k = 2q^{a/2-b/l} + q^{a-b/l} + q^{-b/l}$. Подставив ε и k в получим

$$\frac{2}{q^b} - \text{SU}\left(\left(2q^{a/2} + q^a + 1\right) \cdot q^{la+b}, q^a \left(2q^{a/2-b/l} + q^{a-b/l} + q^{-b/l}\right), q^b\right).$$

Используя код, построенный по кривой Эрмита, и простой ортогональный массив, построим обобщенный СУКХФ. Имеем

$$\frac{\left(k + \frac{q^a - q^{\frac{a}{2}}}{2} - 1\right)^l}{q^{\frac{3al}{2}}} + \frac{1}{q^b} - \text{SU}\left(q^{\frac{5al}{2}+b}, q^{ak}, q^b\right).$$

Зафиксируем вероятность коллизии $\varepsilon = \frac{2}{q^b}$, т.е.

$$\frac{\left(k + \frac{q^a - q^{\frac{a}{2}}}{2} - 1\right)^l}{q^{\frac{3al}{2}}} + \frac{1}{q^b} = \frac{2}{q^b}.$$

Выразив k , получим $k = q^{3a/2-b/l} - \frac{q^a - q^{a/2}}{2} + q^{-b/l}$. Подставив ε и k в получим

$$\frac{2}{q^b} - \text{SU} \left(q^{\frac{5a}{2}+b}, q^{\frac{a(2q^{3a/l-b/l} - q^a + q^{a/2} + 2)}{2}}, q^b \right).$$

Используя код, построенный по кривой Сузуки, и простой ортогональный массив, построим обобщенный СУКХФ. Имеем

$$\frac{\left(k + \frac{q^{2a} - q^a}{2q^{a/2}} - 1 \right)^l}{q^{2la}} + \frac{1}{q^b} - \text{SU} \left(q^{3a+b}, q^{ak}, q^b \right).$$

Зафиксируем вероятность коллизии $\varepsilon = \frac{2}{q^b}$, т.е.

$$\frac{\left(k + \frac{q^{2a} - q^a}{2q^{a/2}} - 1 \right)^l}{q^{2la}} + \frac{1}{q^b} = \frac{2}{q^b}.$$

Выразив k , получим $k = q^{2a-b/l} - \frac{q^{2a} - q^a}{2q^{a/2}} + 1$. Подставив ε и k получим

$$\frac{2}{q^b} - \text{SU} \left(q^{3a+b}, q^{\frac{a(2q^{5a/2-b/l} - q^{2a} + q^a + 2q^{a/2})}{2q^{a/2}}}, q^b \right).$$

Таким образом, схема аутентификации с использованием обобщенных СУКХФ (1 – 4) имеет параметры: вероятность коллизий $P_K \leq \frac{2}{q^b}$, длина аутентификатора равна l -набору q^b -ичных символов, объем ключа аутентификации и объем хешируемых данных соответственно определяются первым и вторым параметрами в обозначении SU.

Выводы. Полученное обобщение УКХФ, построенных по алгебраическим кодам, расширяет область практического использования композиционных СУКХФ на их основе. Предложенные схемы позволяют сни-

зять кратность групповых операций основного этапа формирования СУКХФ при сохранении высоких показателей стойкости. Одним из **перспективных направлений дальнейших исследований** является разработка программно-аппаратных моделей, практически реализующих разработанный метод, проведение экспериментальных исследований стойкости и быстродействия алгоритмов формирования СУКХФ.

ЛИТЕРАТУРА

1. Wegman M. N., Carter J. L. *New hash functions and their use in authentication and set equality* // *J. Computer and System Sci.* – 1981. – 22. – P. 265 – 279.
2. Carter J. L., Wegman M. N. *Universal classes of hash functions* // *J. Computer and System Sci.* – 1979. – 18. – P. 143 – 154.
3. Stinson D. R. *Universal Hashing and Authentication Codes* // *Designs, Codes and Cryptography* 4. – 1994. – P. 369 – 380.
4. Stinson D. R. *A preliminary version appeared in the Proceedings of CRYPTO 91* // *Lecture Notes in Computer Science* – 1992. – 576. – P. 74 – 85.
5. Stinson D.R. *Combinatorial techniques for universal hashing* // *Journal of Computer and Systems Science.* – 1994. – 48. – P. 337 – 346.
6. Халимов Г.З., Кузнецов А.А. *Аутентификация и универсальное хеширование* // *Радиотехника: Всеукр. межвед. науч.-техн. сб. – X.: ХТУРЭ, 2001. – Вып. 119. – С. 88 – 94.*
7. Халимов Г.З., Кузнецов А.А. *Аутентификация с применением алгеброгеометрических кодов* // *Радиотехника: Всеукр. межвед. науч.-техн. сб. – X.: ХТУРЭ, 2001. – Вып. 119. – С. 81 – 87.*

Поступила 3.02.2004

КУЗНЕЦОВ Александр Александрович, канд. техн. наук, нач. научно-исследовательской лаборатории Харьковского военного университета. В 1996 году окончил Харьковский военный университет. Области научных интересов – криптографическое преобразование информации, алгебраическая теория кодов и их применение в системах передачи данных.

ИВАШКИН Александр Викторович, старший научный сотрудник научно-исследовательской лаборатории Харьковского военного университета. В 1997 году окончил Харьковский военный университет. Области научных интересов – криптографическое преобразование информации, алгебраическая теория кодов и их применение в системах передачи данных.

СТАСЕВА Яна Юрьевна, инженер-программист научно-исследовательской лаборатории. В 2002 году окончила Харьковский национальный университет радиоэлектроники. Области научных интересов – криптографическое преобразование информации, алгебраическая теория кодов и их применение в системах передачи данных.