УДК 621.391

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-кодовыми словами, основанием m и относительным кодовым расстоянием $1-\varepsilon$ эквивалентен универсальному классу хеш-функций с параметрами $\varepsilon^l - \mathrm{U}(\mathrm{N}^l, \mathrm{n}, \mathrm{m}^l)$, т.е. множеству H из N функций, осуществляющих отображение $\mathrm{f}:\mathrm{X}\to\mathrm{Y}$ такое, что для двух различных элементов x_1, $\mathrm{x}_2 \in \mathrm{X}$ существует не больше, чем $\mathrm{N}^l \cdot \varepsilon^l$ функций $\mathrm{f} \in \mathrm{H}$ таких, что $\mathrm{f}(\mathrm{x}_1) = \mathrm{f}(\mathrm{x}_2)$.

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 $|\mathrm{Y}| = \mathrm{m}^l$. Мощность множества H как мощность *l*-наборов из *N* символов задается $|\mathrm{H}| = \mathrm{N}^l$.

Пусть d – минимальное кодовое расстояние, т.е. минимальное число символов, в которых различаются два произвольных кодовых слова, $\varepsilon = \dfrac{\mathrm{n}-\mathrm{d}}{\mathrm{n}}$. Это означает, что два произвольных кодовых слова совпадут в $\le (\mathrm{n}-\mathrm{d})$ символах. Верхняя оценка для вероятности совпадения одного символа запишется в виде $\mathrm{P}_1 \le \dfrac{\mathrm{n}-\mathrm{d}}{\mathrm{n}} = \varepsilon$. Совпадения символов – события независимые, верхняя оценка для вероятности совпадения *l*-набора символов запишется как $\mathrm{P}_l = (\mathrm{P}_1)^l \le \left(\dfrac{\mathrm{n}-\mathrm{d}}{\mathrm{n}}\right)^l = \varepsilon^l$. Для двух различных *l*-наборов x_1 и x_2 существует не больше, чем $\mathrm{N}^l \cdot \varepsilon^l$ функций $\mathrm{f} \in \mathrm{H}$ таких, что $\mathrm{f}(\mathrm{x}_1) = \mathrm{f}(\mathrm{x}_2)$.

Утверждение 2. Композиция из универсального класса хеш-функций $\varepsilon_1^l - \mathrm{U}(\mathrm{N}_1^l, \mathrm{n}, \mathrm{u}^l)$ и строго универсального класса хеш-функций

$\varepsilon_2 - \mathrm{SU}(\mathrm{N}_2, \mathrm{n}, \mathrm{m})$ является строго универсальным классом с параметрами $\varepsilon - \mathrm{SU}(\mathrm{N}_1^l \mathrm{N}_2, \mathrm{n}, \mathrm{m})$, 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 $\varepsilon_1^l - \mathrm{U}(\mathrm{N}_1^l, \mathrm{n}, \mathrm{u}^l)$ и строго универсального класса $\varepsilon_2 - \mathrm{SU}(\mathrm{N}_2, \mathrm{n}, \mathrm{m})$, получим СУКХФ с параметрами $\varepsilon - \mathrm{SU}(\mathrm{N}, \mathrm{n}, \mathrm{m})$, где $\mathrm{N} = \mathrm{N}_1^l \mathrm{N}_2$, $\varepsilon = \varepsilon_1^l + \varepsilon_2 - \varepsilon_1^l \varepsilon_2$.

Составляющая H_2 в композиционной конструкции $\mathrm{H} = \mathrm{H}_1 \circ \mathrm{H}_2$ представляет класс строго универсальных хеш-функций, и его можно построить, используя простые ортогональные массивы [3 – 6]. Компонента H_1 в нашем случае является универсальным классом $\varepsilon_1^l - \mathrm{U}(\mathrm{N}_1^l, \mathrm{n}, \mathrm{u}^l)$. 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 $\left(\varepsilon_1^l + \varepsilon_2 - \varepsilon_1^l \varepsilon_2\right) - \mathrm{SU}(\mathrm{N}_1^l \mathrm{N}_2, \mathrm{n}, \mathrm{m})$ с алгеброгеометрическими кодами. Справедливо следующее утверждение.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Таким образом, схема аутентификации с использованием обобщенных СУКХФ (1 – 4) имеет параметры: вероятность коллизий $P_K \le \frac{2}{q^b}$, 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-

зить кратность групповых операций основного этапа формирования СУККХФ 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 СУККХФ.

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 // Designes, Codes and Criptography 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. – Х.: 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. – Х.: 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.*