6. *Wood C. A.* Large Substitution Boxes with Efficient Combinational Implementations. Thesis. Rochester Institute of Technology, 2013.
7. *Daemen J. and Rijmen V.* The Design of Rijndael, AES — the Advanced Encryption Standard. Springer Verlag, 2002.
8. *AlTawy R. and Youssef A. M.* A meet in the middle attack on reduced round Kuznyechik // IEICE Trans. 2015. V. 98-A. P. 2194–2198.
9. *Park S., Sung S.H., Lee S., and Lim J.* Improving the upper bound on the maximum differential and the maximum linear hull probability for SPN structures and AES // LNCS. 2003. V. 2887. P. 247–260.

УДК 519.17 DOI 10.17223/2226308X/12/33

ОЦЕНКА ХАРАКТЕРИСТИК ПЕРЕМЕШИВАНИЯ ХЭШ-ФУНКЦИЙ СЕМЕЙСТВА MD

А. М. Коренева

Матрично-графовый подход (МГП), нашедший успешное применение к оценке свойств итеративных блочных шифров и генераторов ключевого расписания, впервые представлен как инструмент оценивания перемешивающих свойств алгоритмов хэширования. Особенность применения МГП к хэш-функциям связана с неочевидностью построения перемешивающих матриц, характеризующих зависимость битов сгенерированного хэш-значения от битов исходного сообщения. Для хэш-функций MD4, MD5, SHA-1, SHA-256 построены перемешивающие матрицы порядка $512 + n$, где n — длина блока, с которым оперирует односторонняя функция сжатия алгоритма хэширования при обработке 512-битового блока входного сообщения ($n = 128$ для MD4 и MD5, $n = 160$ для SHA-1 и $n = 256$ для SHA-256). К исследованным характеристикам перемешивания относятся локальные экспоненты перемешивающих матриц, то есть для каждой матрицы M определено наименьшее натуральное число γ, такое, что при любом натуральном $\tau \geqslant \gamma$ положительны все столбцы матрицы M^τ с номерами $513, 514, \ldots, 512 + n$. Значения локальных экспонентов являются нижними оценками числа итераций, после которых каждый бит сгенерированного хэш-значения может существенно зависеть от всех битов исходного сообщения. Полученные значения ($\gamma = 21$ для MD4, MD5, SHA-256 и $\gamma = 23$ для SHA-1) косвенно свидетельствуют о схожих криптографических качествах рассмотренных алгоритмов хэширования, несмотря на варианты их усиления за счёт увеличения длины блока и усложнения функции сжатия.

Ключевые слова: *алгоритмы хэширования, структура Меркла — Дамгарда, матрично-графовый подход, перемешивающие свойства.*

Введение

В основе принципа перемешивания, важного для многих криптографических алгоритмов, лежит существенная нелинейная зависимость выходных данных от элементов входа. Для оценки множества существенных переменных композиции преобразований векторного пространства применяется матрично-графовый подход, теоретические основы которого изложены в [1]. Глубина итерации преобразования, при которой каждый бит выходного значения может зависеть от всех битов входа, оценивается снизу значением экспонента примитивного перемешивающего орграфа. В течение последних лет МГП нашёл успешное применение для исследования свойств итеративных блочных шифров и генераторов ключевого расписания [2 – 4], для которых перемешиваю-

щие матрицы, характеризующие зависимость координатных функций выхода от переменных входа, строятся достаточно просто, в отличие от аналогичных матриц для алгоритмов хэширования. В работе представлен способ применения МГП для оценки характеристик перемешивания хэш-функций, реализующих структуру Меркла — Дамгарда (алгоритмы MD4, MD5, SHA-1, SHA-2).

1. Конструкция MD

Конструкция Меркла — Дамгарда, представленная в 1979 г. в диссертации Ральфа Меркла, лежит в основе большинства хэш-функций, разработанных в период с 1990 по 2008 г. Суть конструкции заключается в итеративном процессе последовательных преобразований, когда на вход каждой итерации поступает блок исходного текста и выход предыдущей итерации. Меркл и Дамгард независимо друг от друга показали, что если функция сжатия устойчива к коллизиям, то и хэш-функция будет также устойчива. В докладе рассматриваются известные хэш-функции из семейства MD с длиной блока текста 512 бит. Дадим краткое описание алгоритмов [5, 6].

Обозначим через V_r множество всех двоичных векторов длины r, $\oplus$ — операция XOR-сложения двоичных векторов, $\boxplus$ — операция сложения по модулю 2^{32}. Пусть X — исходное сообщение, разбитое на $t \geqslant 1$ блоков $x_1, \ldots, x_t$, $x_i \in V_{512}$, $i = 1, 2, \ldots, t$, последний блок x_t дополняется битовой строкой $1||0 \ldots 0$ до получения блока размером 448 бит, к которому затем добавляют длину исходного (недополненного) сообщения X, представленную в виде 64-битовой строки. Хэш-функции семейства MD построены на основе односторонней функции сжатия $\varphi(x_i, H_{i-1}) = H_i$, $i = 1, \ldots, t$, $H_i \in V_n$, H_0 — фиксированное начальное заполнение, $n = 128$ для MD4 и MD5, $n = 160$ для SHA-1 и $n = 256$ для SHA-256. Роль функции сжатия может осуществлять любой блочный шифр E_X, $\varphi(X, H) = E_X(H) \oplus H$.

Преобразования E_X алгоритмов MD4, MD5, SHA-1, SHA-2 построены на основе регистров сдвига с 32-битовыми ячейками. Регистры имеют схожие принципы функционирования. Блок открытого текста длиной 512 бит записывается в первый регистр сдвига длины 16 над V_{32} (изображён слева на рис. 1–3), выход с каждого такта подаётся на вход второго регистра над V_{32} (изображён справа на рис. 1–3), начальным заполнением которого является значение H_0. Последнее состояние, в которое перейдёт второй регистр после выполнения всех тактов, определяет искомое хэш-значение H_t. Для усложнения на каждом такте с номером j происходит суммирование с заранее заданными константами C_j и применяются функции f обратных связей нелинейных регистров, которые меняются в зависимости от такта.

Алгоритм MD4 (рис. 1, без пунктирной стрелки) реализует 48 тактов, MD5 (рис. 1, с пунктирной стрелкой) — 64 такта. В спецификации RFC 1321 для каждого такта с номером j определены циклические сдвиги влево s_j, константы C_j и функции f. Алгоритмы MD4 и MD5 не считаются надёжными, для них найдены способы нахождения коллизий с приемлемой вычислительной сложностью.

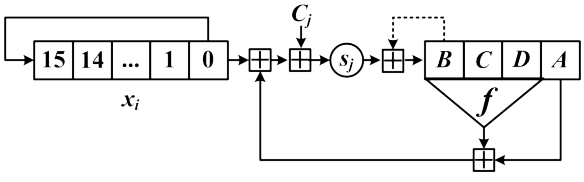

Рис. 1. Регистровое преобразование алгоритмов MD4 и MD5

Алгоритм SHA-1 реализует 80 тактов и считается усиленной версией MD5. Несмотря на известные успешные атаки, SHA-1 продолжает использоваться в почтовых программах, приложениях и сетевых протоколах передачи данных. В схеме на рис. 2 числа в кругах обозначают циклические сдвиги влево на соответствующее число бит, константы C_j и функции f определены в спецификации RFC 3174.

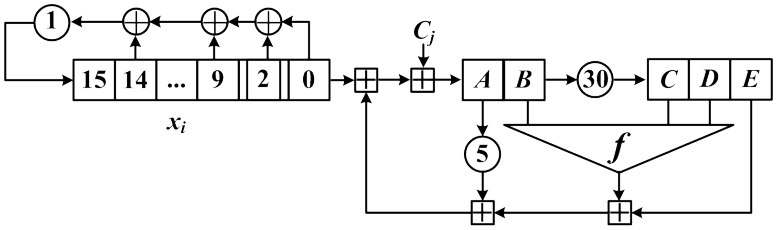

Рис. 2. Регистровое преобразование алгоритма SHA-1

К семейству SHA-2 относятся идентичные алгоритмы (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/256 и SHA-512/224), которые усиливают SHA-1 и считаются достаточно надёжными, но работают в несколько раз медленнее своих предшественников. На рис. 3 представлена схема SHA-256, алгоритм реализует 64 такта, константы C_j и преобразования $Maj, Ch, \Sigma_0, \Sigma_1, \sigma_0, \sigma_1$ описаны в стандарте FIPS PUB 180-4.

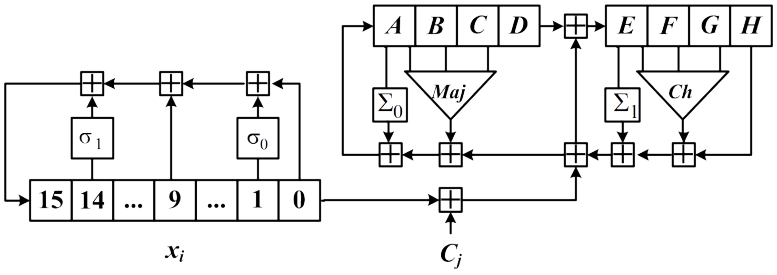

Рис. 3. Регистровое преобразование алгоритма SHA-256

2. Оценка перемешивающих свойств с использованием МГП

Особенность применения МГП к оценке перемешивающих свойств алгоритмов хэширования связана с неочевидностью построения перемешивающих матриц, характеризующих зависимость битов сгенерированного хэш-значения от битов исходного сообщения. Опишем способ построения перемешивающих матриц для регистровых преобразований хэш-функций MD4, MD5, SHA-1, SHA-256.

Используем следующие обозначения:

— $M(\varphi_1)$ — перемешивающая матрица размера 512×512 преобразования φ_1 первого регистра сдвига (слева на рис. 1–3);
— $M(\varphi_2)$ — перемешивающая матрица размера $n \times n$ преобразования φ_2 второго регистра сдвига (справа на рис. 1–3);
— J — перемешивающая матрица размера $32 \times n$, определяющая зависимость состояния регистра φ_2 от выходного значения регистра φ_1 на каждом такте;
— $O_{m\times r}$ — матрица из m нулевых строк и r нулевых столбцов.

В соответствии со схемами из п. 1, перемешивающие матрицы M регистровых преобразований MD4 и MD5 имеют порядок 640, SHA-1 — 672, SHA-256 — 768. Блоковый вид перемешивающих матриц M представлен на рис. 4.

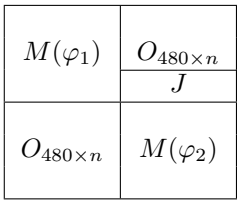

Рис. 4. Блоковый вид перемешивающих матриц M

Для каждого алгоритма хэширования построена перемешивающая $(0,1)$-матрица и применён МГП в соответствии с определениями [1]. Подсчитаны значения локальных экспонентов, то есть для каждой матрицы M определено наименьшее натуральное число γ, такое, что при любом натуральном $\tau \geqslant \gamma$ положительны все столбцы матрицы M^τ с номерами $513, 514, \ldots, 512 + n$. Получены значения $\gamma = 21$ для MD4, MD5, SHA-256 и $\gamma = 23$ для SHA-1.

Выводы

Впервые матрично-графовый подход применён для оценки свойств алгоритмов хэширования. Представлен способ построения перемешивающих матриц для регистровых преобразований хэш-функций MD4, MD5, SHA-1, SHA-256. Предложенный подход не требует трудоёмких вычислений и позволяет быстро получить существенную информацию о криптографических характеристиках алгоритмов. Подсчитаны значения локальных экспонентов перемешивающих матриц, которые являются нижними оценками числа итераций, после которых каждый бит сгенерированного хэш-значения может существенно зависеть от всех битов исходного сообщения. Полученные значения косвенно свидетельствуют о схожих перемешивающих свойствах рассмотренных алгоритмов хэширования, несмотря на варианты их усиления за счёт увеличения длины блока и усложнения функции сжатия.

ЛИТЕРАТУРА

1. *Fomichev V. M., Avezova Ya. E., Koreneva A. M., and Kyazhin S. N.* Primitivity and local primitivity of digraphs and nonnegative matrices // J. Appl. Industr. Math. 2018. V. 12. No. 3. P. 453–469.
2. *Fomichev V. M., Koreneva A. M., Miftahutdinova A. R., and Zadorozhniy D. I.* Evaluation of the maximum productivity for block encryption algorithms // VII Симп. «Современные тенденции в криптографии» CTCrypt 2018. `https://ctcrypt.ru/files/files/2018/17_Koreneva.pdf`
3. *Fomichev V. M. and Koreneva A. M.* Mixing properties of modified additive generators // J. Appl. Industr. Math. 2017. V. 11. No. 2. P. 215–226.
4. *Коренева А. М., Мартышин В. Н.* Экспериментальное исследование экспонентов раундовых перемешивающих матриц обобщённых сетей Фейстеля // Прикладная дискретная математика. Приложение. 2016. № 9. С. 48–51.
5. *Авезова Я. Э.* Современные подходы к построению хеш-функций на примере финалистов конкурса SHA-3 // Вопросы кибербезопасности. 2015. № 3 (11). С. 60–67.
6. *Черемушкин А. В.* Криптографические протоколы. Основные свойства и уязвимости: учеб. пособие для студ. учреждений высш. проф. образования. М.: Издательский центр «Академия», 2009. 272 с.