

Для рассматриваемых кодов и во введённых обозначениях справедлива следующая теорема.

Теорема 1. Пусть $C_r = C(D, G)$ — код, в котором дивизор $D = Q_1 + \dots + Q_{768}$ есть сумма всех P -рациональных точек кривой, заданной уравнением $y^3 = x^{60} + x^{57} + x^{54} + \dots + x^3 + 1$. Тогда в порождающей матрице этого кода нет одинаковых столбцов. Для каждого фиксированного кода из рассматриваемых семейств $C'_{r,m}$ при $r \leq 127$ и фиксированном m получается $\frac{1}{18} \binom{768}{m}$ различных кодов.

Доказательство теоремы конструктивно и даёт возможность выбора точек дивизора D' так, чтобы все полученные коды были различны.

Код C при указанных выше значениях r изоморфен пространству Φ_0 . Описание автоморфизмов алгебры Φ , оставляющих на месте Φ_0 , даёт следующая теорема.

Теорема 2. В указанных выше обозначениях при $39 \leq r \leq 127$ каждый автоморфизм линейной алгебры Φ , отображающий Φ_0 на себя, задается образами x, y : $\varphi(x) = ax + \delta$; $\varphi(y) = dy$, где $a, d, \delta \in P$ и $a^3 = d^3 = 1$, $\delta \in \{0, 1\}$ в поле P .

Из этой теоремы выводятся достаточные условия на выбор точек дивизора D' для получения кодов $C(D', G)$ с тривиальной группой автоморфизмов.

Обобщёнными автоморфизмами кода длины N называют композицию его автоморфизма и преобразования, заключающегося в умножении i -й координаты всех его векторов на один и тот же элемент k_i поля (зависящий от i), $i = 1, \dots, N$. Условимся последнее преобразование называть мультипликативным сдвигом на вектор $(k_1, k_2, \dots, k_N)$. При $k_1 = \dots = k_N$ будем называть его тривиальным сдвигом на k_1 .

Теорема 3. Код $C(D', G)$ имеет только тривиальные мультипликативные сдвиги на любые элементы из P .

ЛИТЕРАТУРА

1. Peters Chr. Information-set decoding for linear codes over F_q // LNCS. 2010. V. 6061. P. 81–94.
2. Bernstein D. J., Lange T, and Peters Chr. Wild McEliece // <http://eprint.iacr.org/2010/410>.
3. Сидельников В. М. Открытое шифрование на основе двоичных кодов Рида — Маллера // Дискретная математика. 1994. Т. 6. Вып. 3. С. 3–20.
4. Minder L. and Shokrollahi A. Cryptanalysis of the Sidelnikov cryptosystem // LNCS. 2007. V. 4515. P. 347–360.
5. Сидельников В. М., Шестаков С. О. О системе шифрования, построенной на основе обобщённых кодов Рида — Соломона // Дискретная математика. 1994. Т. 4. Вып. 3. С. 57–63.
6. Глухов М. М. О кодах Гошпы на одном семействе полей алгебраических функций // Дискретная математика. 2001. Т. 13. Вып. 2. С. 14–34.

УДК 519.7, 004.056.2, 004.056.53

УСЕЧЁННЫЕ ДИФФЕРЕНЦИАЛЬНЫЕ ХАРАКТЕРИСТИКИ С МИНИМАЛЬНЫМ КОЛИЧЕСТВОМ АКТИВНЫХ БАЙТ ДЛЯ УПРОЩЁННОЙ ХЭШ-ФУНКЦИИ WHIRLPOOL

А. А. Камаева

Хэш-функция *Whirlpool* (далее $\mathcal{W}$) разработана Винсентом Риджменом (*Vincent Rijmen*) и Пауло Баррето (*Paolo Barreto*) и опубликована в 2000 г. [1]. Претерпев ряд

изменений, касающихся преобразований, лежащих в её основе, она была стандартизована в окончательном варианте в [2]. Хэш-функция *Whirlpool* построена на основе *AES*-подобного блочного шифра W . В атаке отражениями (*rebound attack*) [3], предложенной Марио Ламбергером и др. (*Mario Lamberger etc.*), найдены коллизии только для пяти полных раундов блочного шифра W (из 14). Сложность такой атаки составляет 2^{120} (в то время как парадокс о днях рождения даёт сложность 2^{256}).

Будем рассматривать хэш-функции $\mathcal{V}$ и $\mathcal{U}$, которые являются упрощёнными вариантами хэш-функции $\mathcal{W}$: их блочные шифры представляют собой всего один или два раунда блочного шифра W соответственно.

Под дифференциальной характеристикой в задаче поиска одноблоковой коллизии будем понимать набор разностей $(\Delta M; \Delta H_0, \Delta H_1)$, где ΔH_0 — разность начальных хэш-значений, а ΔH_1 — разность хэш-значений после обработки одного блока сообщений. Под активным байтом в дифференциальной характеристике понимается ненулевой байт, который подается на нелинейное преобразование. В случае хэш-функции $\mathcal{W}$ (соответственно, и для $\mathcal{V}$ и $\mathcal{U}$) единственным нелинейным преобразованием является S , в основе которого лежит S -box, реализующий нелинейную подстановку.

Пусть M_1 и M_2 — пара сообщений, такая, что $M_1 \oplus M_2 = \Delta M$. Рассматривая различные значения ΔM , найдём минимальное количество активных байт в дифференциальной характеристике $(\Delta M; 0, 0)$, при которых существует коллизия, поскольку, как правило, минимизация количества активных байт ведёт к максимизации вероятности дифференциальной характеристики.

Утверждение 1. Для функции $\mathcal{V}$ наименьшее количество активных байт в дифференциальной характеристике равно 23, а для функции $\mathcal{U}$ — 45.

Для оценки вероятности дифференциальной характеристики используем следующее свойство нелинейного преобразования S : пусть $a, b \in \{0, 1\}^8$. Тогда для фиксированной пары (a, b) число решений уравнения

$$S(x) \oplus S(x \oplus a) = b$$

относительно переменной x может быть равным 0, 2, 4, 6, 8 и 256 ($a = b = 0$).

Обозначим $P_{a,b} = N/2^8$, где N — число решений уравнения для пары (a, b) . Величина $P_{a,b}$ является вероятностью дифференциальной характеристики для S -box с разностью a на входе и разностью b на выходе. Соответственно она принимает одно из следующих значений: 0, 2^{-7} , 2^{-6} , $3 \cdot 2^{-7}$, 2^{-5} и 1.

Максимальной вероятности дифференциальной характеристики $(\Delta M; 0, 0)$ можно добиться при предположении, что все её активные байты проходят через S -box с вероятностью 2^{-5} ; таким образом, получаем

Следствие 1. Максимальная вероятность нахождения коллизии для хэш-функции $\mathcal{V}$ составляет 2^{-115} , а для $\mathcal{U}$ — 2^{-225} .

Итак, даже сильно упрощённая хэш-функция *Whirlpool* обладает значительной стойкостью к нахождению коллизий.

ЛИТЕРАТУРА

1. Barreto P. S. L. M. and Rijmen V. The Whirlpool Hashing Function. Submitted to NESSIE (September 2000) (Revised May 2003). <http://www.larc.usp.br/~pbarreto/WhirlpoolPage.html> (2008/12/11)
2. Information technology — Security techniques — Hash-functions. Part 3: Dedicated hash-functions. ISO/IEC 10118-3:2004, 2004.

3. Lamberger M., Mendel F., Rechberger C., et al. The Rebound Attack and Subspace Distinguishers: Application to Whirlpool. Cryptology ePrint archive, Report 2010/198, 2010. <http://eprint.iacr.org/2010/198>

УДК 519.7, 004.056.2, 004.056.53

ОЦЕНКИ СЛОЖНОСТИ ПОИСКА КОЛЛИЗИЙ ДЛЯ ХЭШ-ФУНКЦИИ RIPEMD

Г. А. Карпунин, Е. З. Ермолаева

Хэш-функция RIPEMD [1] была разработана в 1992 г. в рамках европейского проекта RIPE (RACE Integrity Primitives Evaluation) как альтернатива популярной на то время хэш-функции MD4 [2]. Фактически, функция сжатия RIPEMD представляет собой две работающие параллельно функции сжатия MD4 (левая и правая ветки RIPEMD), отличающиеся друг от друга аддитивными константами. Уже в 1997 г. Х. Доббертин [3] нашел коллизии для урезанной до двух раундов версии RIPEMD, а в 2001 г. К. Дебарт и Г. Гилберт [4] показали, что по отдельности и левая и правая ветки RIPEMD не устойчивы к коллизиям. Для полной версии RIPEMD коллизии были построены лишь в 2004 г. и предъявлены в знаменитой заметке К. Вонг и др. [5], чуть позднее те же авторы в [6] опубликовали детали своего алгоритма поиска коллизий и привели оценку средней трудоёмкости, которая является наилучшей на сегодняшний день. Однако корректность этой оценки вызывает сомнения в силу краткого и недетального изложения алгоритма.

К текущему моменту разработаны усиленные варианты хэш-функции RIPEMD: RIPEMD-128, RIPEMD-160, RIPEMD-256, RIPEMD-320 [7, 8], которые рекомендуются к использованию во многих международных и национальных стандартах, в частности ISO/IEC 10118-3:2004. Хэш-функции семейства RIPEMD-х получили широкое распространение и на практике, например RIPEMD-160 используется для генерации ключа шифрования на основе пароля в популярном программном комплексе создания зашифрованных дисков TrueCrypt [9]. Поскольку все усиленные варианты наследуют идеологию первой конструкции RIPEMD, её подробный криптоанализ и получение точных оценок стойкости по-прежнему остается актуальным.

В настоящей работе восстанавливаются опущенные детали алгоритма [6] поиска коллизий для RIPEMD и проводится экспериментальная проверка заявленной в [6] трудоёмкости этого алгоритма. Такая необходимость возникает в силу того, что в [6] отсутствует полное обоснование оценок трудоёмкости, а приводятся лишь основные идеи алгоритма, которые состоят в следующем. Строится приводящая к коллизии дифференциальная характеристика $(\Delta M, \Delta Q)$, где ΔM — набор разностей между сообщениями, а ΔQ — набор разностей между промежуточными переменными сцепления. Выписывается некоторый набор достаточных условий на промежуточные переменные сцепления Q и неявно утверждается, что если для одного сообщения M все промежуточные значения переменных сцепления удовлетворяют этим условиям, то автоматически другое сообщение $M + \Delta M$ образует коллизию с M . Затем используются две техники для подбора такого сообщения M , что при вычислении его хэш-значения все переменные сцепления удовлетворяют набору достаточных условий. Первая техника называется однократной модификацией сообщения и позволяет добиться выполнения достаточных условий на первых 16 шагах функции сжатия. Сложность этого этапа, как неявно предполагают авторы [6], составляет от 1 до 4 условных операций, где за одну условную операцию принимается одно вычисление функции сжатия. Однако