ЛИТЕРАТУРА

1. Сайт олимпиады NSUCRYPTO. http://nsucrypto.nsu.ru/
2. *Tokareva N., Gorodilova A., Agievich S., et al.* Mathematical methods in solutions of the problems from the Third International Students' Olympiad in Cryptography // Прикладная дискретная математика. 2018. № 40. С. 34–58.
3. *Геут К. Л., Кириенко К. А., Садков П. О. и др.* О явных конструкциях для решения задачи «A secret sharing» // Прикладная дискретная математика. Приложение. 2017. № 10. С. 68–70.
4. *Холл М.* Комбинаторика: пер. с англ. М.: Мир, 1970. 424 с.
5. *Ковалевская Д. И., Соловьева Ф. И., Филимонова Е. С.* О системах троек Штейнера малого ранга, вложимых в совершенные двоичные коды // Дискретный анализ и исследование операций. 2013. Т. 20. № 3(111). С. 3–25.
6. *Медведев Н. В., Титов С. С.* Об однородных матроидах и блок-схемах // Прикладная дискретная математика. Приложение. 2017. № 10. С. 21–23.
7. *Shamir A.* How to share a secret // Commun. ACM. 1979. No. 22. P. 612–613.
8. *Парватов Н. Г.* Совершенные схемы разделения секрета // Прикладная дискретная математика. 2008. № 2(2). С. 50–57.
9. *Асанов М. О., Баранский В. А., Расин В. В.* Дискретная математика: графы, матроиды, алгоритмы. Ижевск: НИЦ Регулярная и хаотическая динамика, 2001. 288 с.

УДК 519.7 DOI 10.17223/2226308X/12/30

ОБ АРГУМЕНТАЦИИ ОТСУТСТВИЯ СВОЙСТВ СЛУЧАЙНОГО ОРАКУЛА У НЕКОТОРЫХ КРИПТОГРАФИЧЕСКИХ ХЕШ-ФУНКЦИЙ[1]

И. А. Грибанова, А. А. Семёнов

Представлены новые алгебраические атаки на хеш-функции вида MD4-k, где k — число шагов базового алгоритма MD4, $39 \leqslant k \leqslant 48$. Для решения алгебраических уравнений используются SAT-решатели. Представленные атаки демонстрируют отсутствие свойств случайного оракула у рассматриваемых хеш-функций. Более точно, мы строим оценки доли легко обратимых выходов этих функций и показываем, что даже для полнораундовой функции MD4 эта доля весьма высока. Для построения оценок с каждой функцией вида MD4-k связывается специальная функция, длина входа которой существенно меньше 512. Показано, что любое значение такой функции является значением MD4-k. Задача обращения специальной функции, как правило, существенно проще, чем задача обращения MD4-k. Оценка доли векторов в $\{0,1\}^{128}$, являющихся значениями специальной функции, даёт оценку доли легко обратимых значений исходной функции MD4-k.

Ключевые слова: *криптографические хеш-функции, поиск прообразов хеш-функций, MD4, MD4-39, SAT.*

Случайный оракул — это гипотетический объект, обладающий рядом привлекательных с точки зрения криптографии свойств. Строго (см., например, [1]) случайный оракул определяется как отображение вида $O : \{0,1\}^* \to \{0,1\}^\infty$, которое произвольному конечному двоичному слову сопоставляет слово, являющееся бесконечной

[1]Работа выполнена при финансовой поддержке Российского научного фонда, проект № 16-11-10046. Грибанова И. А. поддержана стипендией Президента РФ СП-3545.2019.5.

последовательностью испытаний Бернулли с $p = 1/2$. Однако такое определение полностью неконструктивно. Для практических приложений необходимы функции вида $\{0,1\}^* \to \{0,1\}^*$ или даже $\{0,1\}^n \to \{0,1\}^m$, которые обладают (гипотетически) свойствами случайного оракула, но могут быть заданы посредством некоторых алгоритмов. Более точно, требуется, чтобы алгоритм, задающий функцию, был детерминированным (то есть выдавал одинаковые выходы для одинаковых входов). Почти все выходы (длины m) функции, выполняющей роль случайного оракула, должны выглядеть как последовательности Бернулли с $p = 1/2$. Соответственно для случайно сгенерированного входа такой функции сложность задачи обращения соответствующего выхода должна быть сопоставима со сложностью повторения фиксированной последовательности Бернулли в результате m-кратного подбрасывания идеальной монеты.

Существование случайных оракулов вида $O : \{0,1\}^n \to \{0,1\}^m$ было бы чрезвычайно полезно для многих криптографических приложений. Скажем, некто может сгенерировать свой секретный идентификатор $\alpha \in \{0,1\}^n$, а затем многократно доказывать свою аутентичность, используя α и несекретный алгоритм O. В [1] отмечено, что на роль реальных прототипов случайного оракула подходят стойкие криптографические хеш-функции. Эта идея получила серьезное развитие в [2, 3], после появления которых возникло целое направление, известное как «доказательства в модели случайного оракула». В настоящей работе показано, что некоторые известные криптографические хеш-функции не обладают свойствами случайного оракула. Более точно, будем рассматривать задачу обращения криптографической хеш-функции $h : \{0,1\}^* \to \{0,1\}^C$. Такие функции обычно разбивают хешируемое сообщение на блоки фиксированной длины n, соответственно рассматриваются задачи обращения функций вида $f : \{0,1\}^n \to \{0,1\}^C$ (для функций из семейств MD и SHA $n = 512$).

Основная цель работы — показать для некоторых криптографических хеш-функций, что легко обратимые выходы этих функций составляют значительную долю в $\{0,1\}^C$. Интуитивно, любая такая функция h не может быть случайным оракулом, поскольку выбор случайного входа α с высокими шансами даст выход γ, обращение которого потребует меньше вычислительных ресурсов, чем простой подбор такого $\alpha' \in \{0,1\}^n$, что $h(\alpha') = \gamma$. Будем исследовать хеш-функции вида MD4-k, где k — число базовых шагов алгоритма MD4 [4].

В основе описываемых далее атак лежат результаты [5, 6]. Основная идея этих атак заключается в использовании «ослабляющих ограничений». Впервые использовать подобные ограничения предложил Г. Доббертин в [7]. Новизна подхода из [5, 6] заключается в том, что ослабляющие ограничения строятся в автоматическом режиме в процессе решения задачи оптимизации специальной псевдобулевой функции [9], оценивающей некоторую эвристическую меру эффективности соответствующих ограничений. Ослабляющие ограничения — это нулевые значения некоторых переменных сцепления (chaining variables). Изначально Г. Доббертин предложил приравнять произвольной константе значения 12 переменных сцепления, используемых в первых двух раундах алгоритма MD4. Для решения получающейся системы булевых уравнений Г. Доббертин предложил алгоритм, позволяющий обращать на персональном компьютере функцию MD4-32. В [8] описан, по сути, вариант атаки Доббертина (т. е. ослабляющие ограничения накладываются на те же переменные сцепления), в котором для решения уравнений используется SAT-решатель, а для построения ослабляющих ограничений — константа 0. При помощи метода, предложенного в [5, 6], удалось построить различные виды ослабляющих ограничений, среди которых оказались такие, которые дали существенно более эффективную атаку на MD4-39, чем в работе [8]. Один из набо-

ров ослабляющих ограничений из [5, 6] позволил обращать менее чем за 1 мин работы SAT-решателя MINISAT2.2 примерно 65 % случайных векторов из $\{0,1\}^{128}$, рассматривая их как значения функции MD4-39.

Анализируя различные ослабляющие ограничения, построенные в [5, 6], можно заметить, что с исходной обращаемой функцией вида $f_{\text{MD4-}k} : \{0,1\}^{512} \to \{0,1\}^{128}$ естественным образом связываются специальные функции вида $g^{\lambda}_{\text{MD4-}k} : \{0,1\}^{d} \to \{0,1\}^{128}$, обладающие целым рядом интересных свойств (через λ здесь обозначен булев вектор, задающий некоторый набор ослабляющих ограничений). Во-первых, любое значение функции $g^{\lambda}_{\text{MD4-}k}$ является значением функции $f_{\text{MD4-}k}$. Во-вторых, что очень важно, d может оказаться существенно меньше, чем 512. Так, один из векторов ослабляющих ограничений для задачи обращения $f_{\text{MD4-39}}$, обозначаемый λ_1, даёт функцию $g^{\lambda_1}_{\text{MD4-39}} : \{0,1\}^{128} \to \{0,1\}^{128}$. Наконец, если γ — значение функции вида $g_{\text{MD4-}k}$ и $\alpha' \in \{0,1\}^{d}$ — его прообраз, то от α' можно эффективно перейти к такому $\alpha \in \{0,1\}^{512}$, что $f_{\text{MD4-}k}(\alpha) = \gamma$.

Функции вида $g^{\lambda}_{\text{MD4-}k}$ могут быть определены не всюду на $\{0,1\}^{d}$ и далеко не каждый $\gamma \in \{0,1\}^{128}$ является образом функции $g^{\lambda}_{\text{MD4-}k}$. Однако задача обращения функции $g_{\text{MD4-}k}$ может оказаться существенно проще, чем задача обращения $f_{\text{MD4-}k}$. Так, на обращение каждого значения функции $g^{\lambda_1}_{\text{MD4-39}}$ тратится менее минуты работы обычного последовательного SAT-решателя MINISAT2.2. При этом примерно 65 % векторов из $\{0,1\}^{128}$ имеют $g^{\lambda_1}_{\text{MD4-39}}$-прообразы. Сказанное означает, что примерно 65 % выходов функции MD4-39 являются легко обратимыми, поскольку такова доля выходов MD4-39, совпадающих с выходами функции $g^{\lambda_1}_{\text{MD4-39}}$. Это означает, что MD4-39 не удовлетворяет свойствам случайного оракула, поскольку, выбрав случайный вход $\alpha \in \{0,1\}^{512}$, с вероятностью $\approx 65\,\%$ получим $\gamma = f_{\text{MD4-39}}(\alpha)$, который имеет $g^{\lambda_1}_{\text{MD4-39}}$-прообраз. Найдя этот прообраз, мы эффективно построим по нему такой $\tilde{\alpha} \in \{0,1\}^{512}$, что $f_{\text{MD4-39}}(\tilde{\alpha}) = \gamma$.

В таблице представлены ослабляющие ограничения, задающие функции вида $g^{\lambda}_{\text{MD4-}k}$, для которых задачи обращения решаются в среднем за время $< t$ при помощи однопоточного SAT-решателя.

Ослабляющие ограничения		d	k	t, с
λ_1	00000000000001101110111011101000000000000000000000	128	39	12
λ_2	00000000000001101110111011101100000000000000000000	96	43	4,5
λ_3	00000000000011101110111011101000000000000000000000	96	44	20
λ_4	00000000010111111011101110100000000000000000000000	64	41	5,7
λ_5	00000000000011101110111011101100000000000000000000	64	47	914
λ_6	00000000000011101110111011101110000000000000000000	32	48	509

В таблице приведены булевы векторы $\lambda_i \in \{0,1\}^{48}$, $i \in \{1,\ldots,6\}$, задающие ослабляющие ограничения в форме значений «переменных переключения» [5, 6]: единичные компоненты вектора λ_i означают, что переменные сцепления, вычисляемые на шагах с соответствующими номерами, заменяются в системе уравнений, кодирующей криптоанализ функции MD4-k, 32-битной константой $K = 0$. Каждый такой набор ослабляющих ограничений позволяет построить семейство специальных функций вида $g^{\lambda_i}_{\text{MD4-}k} : \{0,1\}^{d} \to \{0,1\}^{128}$. Так, например, вектор λ_3 задаёт набор ослабляющих ограничений, в которых константой $K = 0$ означиваются переменные сцепления, вычисляемые на шагах с номерами 13, 14, 15, 17, 18, 19, 21, 22, 23, 25, 26, 27, 29. Для λ_3 можно построить специальные функции вида $g^{\lambda_3}_{\text{MD4-}k} : \{0,1\}^{96} \to \{0,1\}^{128}$. Для $k = 44$ функция $g^{\lambda_3}_{\text{MD4-44}}$ определена на $\approx 50\,\%$ случайных входов, а задача обраще-

ния $g^{\lambda_3}_{\text{MD4-44}}$-образа случайного входа из $\{0,1\}^{96}$ решается за время $\leqslant 20$ с работы SAT-решателя MINISAT2.2. Для соответствующих входов доказывается отсутствие коллизий за относительно небольшое время работы MINISAT2.2 (все эксперименты проводились на вычислительном кластере «Академик В. М. Матросов» ИДСТУ СО РАН [10]). Следовательно, доля значений функции $g^{\lambda_3}_{\text{MD4-44}}$ в $\{0,1\}^{128}$ составляет приблизительно 2^{-32}. Это означает, что вероятность для случайно выбранного входа из $\{0,1\}^{512}$ получить легкообратимое значение функции MD4-44 составляет примерно 2^{-32} — весьма большая вероятность в сравнении с 2^{-128}. Таким образом, функция MD4-44 не удовлетворяет свойствам случайного оракула. Интересно, что для полнораундовой функции MD4 (т. е. функции MD4-48) доля легко обратимых значений, как следует из шестой строки таблицы, составляет 2^{-96}, что тоже недопустимо много для случайного оракула.

ЛИТЕРАТУРА

1. *Bellare M. and Rogaway P.* Random oracles are practical: a paradigm for designing efficient protocols // Proc. CCS'93. N.Y.: ACM, 1993. P. 62–73.
2. *Pointcheval D. and Stern J.* Security proofs for signature schemes // EUROCRYPT'96. LNCS. 1996. V. 1070. P. 387–398.
3. *Pointcheval D. and Stern J.* Security arguments for digital signatures and blind signatures // J. Cryptology. 2000. V. 13. No. 3. P. 361–396.
4. *Rivest R. L.* The MD4 message digest algorithm // CRYPTO'90. LNCS. 1990. V. 537. P. 303–311.
5. *Gribanova I. and Semenov A.* Using automatic generation of relaxation constraints to improve the preimage attack on 39-step MD4 // Proc. MIPRO-2018. IEEE, 2018. P. 1174–1179.
6. *Грибанова И. А.* Новый алгоритм порождения ослабляющих ограничений в задаче обращения хеш-функции MD4-39 // Прикладная дискретная математика. Приложение. 2018. № 11. С. 139–141.
7. *Dobbertin H.* The first two rounds of MD4 are not one-way // Proc. FSE'1998. LNCS. 1998. V. 1372. P. 284–292.
8. *De D., Kumarasubramanian A., and Venkatesan R.* Inversion attacks on secure hash functions using SAT solvers // Proc. FSE'2007. LNCS. 2007. V. 4501. P. 377–382.
9. *Boros E. and Hammer P. L.* Pseudo-boolean optimization // Discr. Appl. Math. 2002. V. 123 (1–3), P. 155–225.
10. Иркутский суперкомпьютерный центр СО РАН. `http://hpc.icc.ru`.

УДК 003.26, 519.725 DOI 10.17223/2226308X/12/31

ПОИСК ЭКВИВАЛЕНТНЫХ КЛЮЧЕЙ КРИПТОСИСТЕМЫ МАК-ЭЛИСА — СИДЕЛЬНИКОВА, ПОСТРОЕННОЙ НА ДВОИЧНЫХ КОДАХ РИДА — МАЛЛЕРА

А. М. Давлетшина

Предлагается новый способ восстановления эквивалентного секретного ключа криптосистемы Мак-Элиса — Сидельникова, построенной на двоичных кодах Рида — Маллера. Рассматривается криптосистема, для построения которой используются только две копии кода. Задача восстановления эквивалентного секретного ключа криптосистемы Мак-Элиса — Сидельникова сводится к двум задачам поиска эквивалентного секретного ключа криптосистемы Мак-Элиса. Доказано, что предложенный способ имеет полиномиальную сложность. Проведены численные эксперименты на различных параметрах кода Рида — Маллера, подтверждающие