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

возможность восстановления эквивалентного секретного ключа криптосистемы Мак-Элиса — Сидельникова за полиномиальное время.

Ключевые слова: *криптосистема Мак-Элиса — Сидельникова, код Рида — Маллера, полиномиальная атака.*

Криптосистема Мак-Элиса — Сидельникова является криптосистемой с открытым ключом, стойкость которой основана на сложности задачи декодирования произвольного кода, исправляющего ошибки. В 1994 г. В. М. Сидельников [1] несколько изменил схему криптосистемы Мак-Элиса, предложив использовать не одну, а u копий кода, что повысило скорость передачи и стойкость криптосистемы. Предложенная схема получила название криптосистемы Мак-Элиса — Сидельникова. В качестве линейного кода, имеющего эффективный алгоритм декодирования, в работе Сидельникова используются коды Рида — Маллера. В 2007 г. Л. Миндер и А. Шокроллахи [2] построили структурную атаку на криптосистему Мак-Элиса. В 2013 г. М. Бородин и И. Чижов в работе [3] существенно понизили стойкость криптосистемы Мак-Элиса, при некоторых параметрах кода реализовав полиномиальную атаку на открытый ключ. Таким образом, вопрос стойкости криптосистемы Мак-Элиса — Сидельникова является достаточно актуальным.

Секретным ключом криптосистемы Мак-Элиса — Сидельникова является кортеж (H, P), где H — невырожденная матрица над полем $\mathrm{GF}(2)$; P — перестановочная матрица. Открытым ключом является матрица $G = (R||HR)P$, где R — порождающая матрица кода Рида — Маллера $\mathrm{RM}(r, m)$.

Определение 1. Код с порождающей матрицей вида $G = (R||HR)$ называется сегментарным кодом Рида — Маллера $\mathrm{RM}(r, m)[H]$.

Таким образом, необходимо найти такие матрицы H' и P', что $(R||HR)P = (R||H'R)P'$. Для этого необходимо выполнить следующие шаги:

1) построить формулу U над операциями произведения Шура $\odot$ кодов и взятия ортогонального $\perp$ кода, такую, что

$$U(\mathrm{RM}(r, m)[H]) \subseteq \mathrm{RM}(m - r\,(\lceil m/r \rceil - 1) - 1, m) \times \mathrm{RM}(m - r(\lceil m/r \rceil - 1) - 1, m);$$

2) используя алгоритм Сендрие [4], разделить $\mathrm{RM}(m - r(\lceil m/r \rceil - 1) - 1, m) \times \times \mathrm{RM}(m - r(\lceil m/r \rceil - 1) - 1, m)$ на две копии кода $\mathrm{RM}(m - r(\lceil m/r \rceil - 1) - 1, m)$;
3) найти перестановку для каждого сегмента, используя алгоритм Чижова — Бородина, если $(r, m - 1) = 1$, либо алгоритм Миндера — Шокроллахи, если $(r, m - 1) \neq 1$;
4) найти матрицу H' секретного ключа криптосистемы.

Полученные теоретические результаты можно разделить на два случая и кратко представить следующими теоремами.

С л у ч а й 1:

$$U(\mathrm{RM}(r, m)[H]) = \mathrm{RM}(d, m) \times \mathrm{RM}(d, m), \text{где } d = (r, m - 1).$$

Теорема 1. Если $(r, m - 1) = 1$, то существует алгоритм, который по порождающей матрице кода $\mathrm{RM}^P(r, m)[H]$ находит перестановку P', такую, что $\mathrm{RM}^{PP'}(r, m)[H] = \mathrm{RM}(r, m)[H]$. Сложность алгоритма $\mathrm{O}(n^4 \log_2 n)$.

Если $(r, m-1) \neq 1$, то существует алгоритм, который по порождающей матрице кода $\mathrm{RM}^P(r, m)[H]$ находит перестановку P', такую, что $\mathrm{RM}^{PP'}(r, m)[H] = \mathrm{RM}(r, m)[H]$. Сложность алгоритма $\mathrm{O}(n^d)$.

С л у ч а й 2:

$$U(\mathrm{RM}(r,m)[H]) \subset \mathrm{RM}(m - r(\lceil m/r \rceil - 1) - 1, m) \times \mathrm{RM}(m - r(\lceil m/r \rceil - 1) - 1, m).$$

Теорема 2. Если m делится на r без остатка, то существует алгоритм, который по порождающей матрице кода $\mathrm{RM}^P(r,m)[H]$ находит перестановку P', такую, что $\mathrm{RM}^{PP'}(r,m)[H] = \mathrm{RM}(r,m)[H]$. Сложность алгоритма $\mathrm{O}(n^{2^r})$.

Если m не делится на r без остатка и $(r, m-1) = 1$, то существует алгоритм, который по порождающей матрице кода $\mathrm{RM}^P(r,m)[H]$ находит перестановку P', такую, что $\mathrm{RM}^{PP'}(r,m)[H] = \mathrm{RM}(r,m)[H]$. Сложность алгоритма $\mathrm{O}(n^{2^{m-r\lfloor m/r \rfloor}})$.

Если m не делится на r без остатка и $(r, m-1) \neq 1$, то существует алгоритм, который по порождающей матрице кода $\mathrm{RM}^P(r,m)[H]$ находит перестановку P', такую, что $\mathrm{RM}^{PP'}(r,m)[H] = \mathrm{RM}(r,m)[H]$. Сложность алгоритма $\mathrm{O}(\max(n^{2^{m-r\lfloor m/r \rfloor}}, n^{d+1}))$.

Теоретические результаты подтверждаются практическими экспериментами: алгоритм реализован программно и исследован на ноутбуке с процессором 2,5 ГГц. Результаты приведены в табл. 1 для случая 1 и в табл. 2 для случая 2.

Т а б л и ц а 1

Данные	Параметры кодов (r,m)						
	(2,6)	(2,8)	(3,8)	(3,9)	(2,10)	(4,10)	(3,11)
Время работы	1,747 с	46,218 с	52,165 с	11 м 9 с	2 ч 39 м	4 ч 32 м	8 ч 19 м
Размер ключа	352 б	2,3 Кб	5,8 Кб	16,25 Кб	14 Кб	96,5 Кб	116 Кб

Т а б л и ц а 2

Данные	Параметры кодов (r,m)						
	(3,8)	(3,9)	(2,10)	(4,10)	(3,11)	(3,12)	(4,12)
Время работы	5 м 34 с	3 ч 13 м	4 ч 1 м	5 ч 28 м	12 ч 49 м	32 ч 54 м	51 ч 54 с
Размер ключа	5,8 Кб	16,25 Кб	14 Кб	96,5 Кб	116 Кб	299 Кб	795 Кб

ЛИТЕРАТУРА

1. *Сидельников В. М.* Открытое шифрование на основе двоичных кодов Рида — Маллера // Дискретная математика. 1994. Т. 6. № 2. С. 3–20.
2. *Minder L. and Shokrollahi A.* Cryptanalysis of the Sidelnikov cryptosystem // Ann. Intern. Conf. Theory and Appl. of Cryptographic Techniques. Berlin; Heidelberg: Springer, 2007. P. 347–360.
3. *Бородин М. А., Чижов И. В.* Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида — Маллера // Дискретная математика. 2014. Т. 26. № 1. С. 10–20.
4. *Sendrier N.* On the structure of a randomly permuted concatenated code // Proc. EUROCODE'94. Cote d'Or, France, 1994. P. 169–173.