

8. Агибалов Г. П. Элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом // Прикладная дискретная математика. 2008. № 1. С. 34–42.
9. Пестунов А. И. О вероятности протяжки однобитовой разности через сложение и вычитание по модулю // Прикладная дискретная математика. 2012. № 4. С. 53–60.
10. Selçuk A. A. On probability of success in linear and differential cryptanalysis // J. Cryptology. 2007. No. 21. P. 131–147.
11. Словарь криптографических терминов / под ред. Б. А. Погорелова и В. Н. Сачкова. М.: МНЦМО, 2006. 94 с.
12. Погорелов Б. А., Черемушкин А. В., Чечета С. И. Об определении основных криптографических понятий // Доклад на конф. «Математика и безопасность информационных технологий», МаБИТ-03, МГУ, 23–24 октября 2003. М., 2003.
13. Knudsen L. R., Robshaw M. J. B., and Wagner D. Truncated differentials and Skipjack // LNCS. 1999. V. 1666. P. 165–180.

УДК 056.55

УЯЗВИМОСТЬ КРИПТОСИСТЕМЫ МАК-ЭЛИСА, ПОСТРОЕННОЙ НА ОСНОВЕ ДВОИЧНЫХ КОДОВ РИДА — МАЛЛЕРА

И. В. Чижев, М. А. Бородин

Предлагается новый алгоритм восстановления секретного ключа по открытому для криптосистемы Мак-Элиса, построенной на основе двоичных кодов Рида — Маллера $RM(r, m)$. В случае, если значение $d = (r, m - 1)$ ограничено, алгоритм имеет полиномиальную сложность $O(n^d + n^4 \log_2 n)$, где $n = 2^m$. Практические результаты показывают, что предложенная атака позволяет осуществить взлом криптосистемы Мак-Элиса, построенной на основе двоичного кода Рида — Маллера длины $n = 65526$ битов, менее чем за 7 ч на персональном компьютере.

Ключевые слова: *криптосистема Мак-Элиса, коды Рида — Маллера, полиномиальная сложность атаки.*

Рассматривается криптосистема Мак-Элиса, оригинальная версия которой использует коды Гоппы [1]. В 1994 г. В. М. Сидельников в работе [2] предложил использовать для построения криптосистемы Мак-Элиса коды Рида — Маллера, которые позволяют увеличить скорость расшифрования и передачи криптограммы.

На сегодняшний день самым успешным из опубликованных алгоритмов восстановления секретного ключа по открытому для криптосистемы Мак-Элиса, основанной на двоичных кодах Рида — Маллера $RM(r, m)$, является алгоритм Л. Миндера и А. Шокроллахи, предложенный ими в 2007 г. в [3]. Этот алгоритм имеет субэкспоненциальную сложность, его идея заключается в сведении задачи взлома криптосистемы с параметрами кода $RM(r, m)$ к такой же задаче, но для кода $RM(1, m)$. В данной работе предложен другой алгоритм сведения, который имеет полиномиальную сложность для некоторого подмножества кодов Рида — Маллера.

Полученные теоретические результаты можно кратко представить в виде теорем.

Теорема 1. Пусть $(r, m - 1) = 1$. Тогда существует алгоритм со сложностью $O(n^4 \log_2 n)$ битовых операций, который по порождающей матрице кода $RM^\sigma(r, m)$ находит перестановку σ' , такую, что $RM^{\sigma \cdot \sigma'}(r, m) = RM(r, m)$.

И обобщение теоремы 1:

Теорема 2. Пусть $(r, m - 1) = d > 1$. Тогда существует алгоритм со сложностью $O(n^d + n^4 \log_2 n)$ битовых операций, который по порождающей матрице кода $RM^\sigma(r, m)$ находит перестановку σ' , такую, что $RM^{\sigma \cdot \sigma'}(r, m) = RM(r, m)$.

Это означает, что для параметров кода $RM(r, m)$, у которых $(r, m - 1)$ ограничен, предложенная атака имеет полиномиальную сложность.

Теоретические результаты подтверждаются практическими исследованиями (табл. 1 и 2): алгоритм реализован программно и запускался на ноутбуке с процессором 2,1 ГГц. Для тех параметров криптосистемы, когда применение алгоритма не даёт асимптотического ускорения, используется символ «М». Если алгоритм сводит исходную задачу (r, m) к задаче с меньшей трудоёмкостью (d, m) , то это отмечено в табл. 2 символами (d, m) .

Т а б л и ц а 1
Результат Л. Миндера и
А. Шокроллахи (процессор 2,4 ГГц)

r	m			
	8	9	10	11
2	0,04 с	0,24 с	12,14 с	1,77 с
3	0,18 с	1,26 с	16,5 с	5 м 20 с
4		2 м 57 с	22 ч 50 м	10 д 11 ч 55 м

Т а б л и ц а 2
Наш результат (2,1 ГГц)

r	m								
	8	9	10	11	12	13	14	15	16
2	0,007 с	М	0,48 с	М	6 с	М	3 м 13 с	М	2 ч 30 м
3	0,01 с	0,2 с	М	1,35 с	19 с	М	5 м 29 с	30 м 31 с	М
4	0,043 с	М	0,43 с	(2,11)	15 с	М	7 м 10 с	(2,15)	3 ч 28 м
5	0,042 с	0,4 с	0,8 с	М	16,5 с	2 м 1 с	14 м 12 с	53 м	М
6		(2,9)	(3,10)	(2,11)	23 с	М	9 м 28 с	14 м 16 с	(3,16)
7			0,86 с	3,2 с	25 с	3 м 16 с	10 м 54 с	М	6 ч 43 м

ЛИТЕРАТУРА

1. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. Теория кодов, исправляющих ошибки. М.: Связь, 1979.
2. Сидельников В. М. Открытое шифрование на основе двоичных кодов Рида — Маллера // Дискретная математика. 1994. Т. 6. № 2. С. 3–20.
3. Minder L. and Shokrollahi A. Cryptanalysis of the Sidelnikov cryptosystem // LNCS. 2007. V. 4515. P. 347–360.