Уязвимость криптосистемы Мак-Элиса, построенной на основе двоичных кодов Рида-Маллера

И.В. Чижов, М.А. Бородин

Московский Государственный Университет
имени М. В. Ломоносова

Москва, 2013

Введение

История

В 1978 году Роберт Мак-Элис опубликовал новую криптосистему с открытым ключем, использующую коды Гоппы.

Стойкость

Стойкость криптосистемы основана на сложности декодирования кода общего положения.

Замена кода

В 1994 году В.М. Сидельников предложил заменить код Гоппы кодом Рида–Маллера

Введение

История

В 1978 году Роберт Мак-Элис опубликовал новую криптосистему с открытым ключем, использующую коды Гоппы.

Стойкость

Стойкость криптосистемы основана на сложности декодирования кода общего положения.

Замена кода

В 1994 году В.М. Сидельников предложил заменить код Гоппы кодом Рида–Маллера

Введение

История

В 1978 году Роберт Мак-Элис опубликовал новую криптосистему с открытым ключем, использующую коды Гоппы.

Стойкость

Стойкость криптосистемы основана на сложности декодирования кода общего положения.

Замена кода

В 1994 году В.М. Сидельников предложил заменить код Гоппы кодом Рида–Маллера

Код Рида-Маллера RM(r,m)

Определение

Кодом Рида-Маллера RM(r,m) порядка r и длины 2^m называется множество всех векторов Ω_f значений булевых функций $f(v_1, v_2, ..., v_m)$, представимых полиномами Жегалкина (многочленами), степень которых не превосходит r, то есть

$$f(v_1, v_2, ..., v_m) = \bigoplus_{s=0}^{r} \bigoplus_{1 \le i_1 < i_2 < ... < i_s \le m} a_{i_1 i_2 ... i_s} v_{i_1} v_{i_2} \dots v_{i_s}.$$

Базис

Код Рида-Маллера $RM(r,m)$ состоит из всех линейных комбинаций векторов, соответствующих произведениям (мономам):

$$1, v_1, v_2, ..., v_m, v_1 v_2, v_1 v_3, \dots, v_{m-1} v_m, \dots, v_{m-r+1} v_{m-r+2} \cdots v_m.$$

Криптосистема Мак-Элиса

Параметры

- R -порождающая матрица кода $RM(r, m)$, размерность кода $k = \sum_{i=0}^{r} \binom{m}{i}$ и длина $n = 2^m$.
- S -случайная невырожденная двоичная $k \times k$ матрица.
- P -перестановочная двоичная $n \times n$ матрица.

Ключи

- Открытый ключ: $G = S \cdot R \cdot P$
- Секретный ключ: (S, P)

Криптосистема Мак-Элиса

Параметры

- R -порождающая матрица кода $RM(r, m)$,
  размерность кода $k = \sum_{i=0}^{r} \binom{m}{i}$ и длина $n = 2^m$.
- S -случайная невырожденная двоичная $k \times k$ матрица.
- P -перестановочная двоичная $n \times n$ матрица.

Ключи

- Открытый ключ: $G = S \cdot R \cdot P$
- Секретный ключ: (S, P)

Задача взлома

Известно

- Параметры кода Рида-Маллера $RM(r, m)$
- Марица $G = S \cdot R \cdot P$.

Нужно найти

Матрицы S' и P' такие, что выполняется условие $S' \cdot R \cdot P' = G$.

Задача взлома

Известно

- Параметры кода Рида-Маллера $RM(r, m)$
- Марица $G = S \cdot R \cdot P$.

Нужно найти

Матрицы S' и P' такие, что выполняется условие $S' \cdot R \cdot P' = G$.

Известная атака Л. Миндера и А. Шокроллахи

Идея атаки

1. По коду $RM^{\sigma}(r,m)$ построить код $RM^{\sigma}(1,m)$, для этого предлагается воспользоваться вложенностью кодов:

$$RM^{\sigma}(1,m) \subset RM^{\sigma}(2,m) \subset \ldots \subset RM^{\sigma}(r,m).$$

2. Найти перестановку σ' такую, что $RM^{\sigma\cdot\sigma'}(1,m) = RM(1,m)$. Тогда найденная перестановка σ' будет искомой, то есть удовлетворять условию $RM^{\sigma\cdot\sigma'}(r,m) = RM(r,m)$.

Наша атака

Нахождение $RM^{\sigma}(1, m)$

Для построения кода $RM^{\sigma}(1, m)$ из кода $RM^{\sigma}(r, m)$ можно использовать следующие операции:

1. Умножение $\odot$ кодов $RM^{\sigma}(r_1, m)$ и $RM^{\sigma}(r_2, m)$ таких, что $r_1 + r_2 \leqslant m - 2$:
   $RM^{\sigma}(r_1, m) \odot RM^{\sigma}(r_2, m) = RM^{\sigma}(r_1 + r_2, m)$.
2. Переход к дульному коду $\perp$ $RM^{\sigma}(r, m)$:
   $(RM^{\sigma}(r, m))^{\perp} = RM^{\sigma}(m - r - 1, m)$.

Можно рассматривать суперпозицию указанных операций.

Теоретические результаты

Основная теорема

Пусть НОД$(r, m-1) = 1$. 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 $RM^{\sigma \cdot \sigma'}(r, m) = RM(r, m)$.

Обобщенная теорема

Пусть НОД$(r, m-1) = d > 1$. 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 $RM^{\sigma \cdot \sigma'}(r, m) = RM(r, m)$.

Практические результаты

Результат Л. Миндера и А. Шокроллахи (CPU 2,4Gh)

(r,m)	8	9	10	11
2	0.04с	0.24с	12.14с	1.77с
3	0.18с	1.26с	16.5с	5м20с
4		2м57с	22ч50м	10д11ч55м

Наш Результат (CPU 2,1Gh)

(r,m)	8	9	10	11	12	13	14	15	16
2	0.007с	M	0.48с	M	6с	M	3м13с	M	2ч30м
3	0.01с	0.2с	M	1.35с	19с	M	5м29с	30м31с	M
4	0.043с	M	0.43с	(2,11)	15с	M	7м10с	(2,15)	3ч28м
5	0.042с	0.4с	0.8	M	16.5с	2м1с	14м12с	53м	M
6		(2,9)	(3,10)	(2,11)	23с	M	9м28с	14м16с	(3,16)
7			0.86с	3.2с	25с	3м16с	10м54с	M	6ч43м

<M> — применять алгоритм Л. Миндера.

<(d,m)> — сводит исходную задачу (r, m) к задаче с меньшей трудоемкостью (d, m).

Спасибо за внимание!

Список литературы

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