Секция «Вычислительная математика и кибернетика»

Атака на криптосистему Мак-Элиса, построенную на основе кодов Рида-Маллера

Чижов И.В.[1]***, Бородин М.А.***[2]

1 - Московский государственный университет имени М.В. Ломоносова, Факультет вычислительной математики и кибернетики, 2 - МГУ - Московский государственный университет имени М.В. Ломоносова, Факультет вычислительной математики и кибернетики, Москва, Россия

E-mail: ivchizhov@gmail.com

Криптосистема Мак-Элиса — одна из старейших криптосистем с открытым ключом. Она была предложена в 1978 Р. Дж. Мак-Элисом[2]. Оригинальная криптосистема строится на основе кодов Гоппы. В. М. Сидельников в работе[1] для построения криптосистемы предложил использовать двоичные коды Рида–Маллера $RM(r,m)$. В 2007 году Л. Миндер и А. Шокроллахи[3] предложили субэкспоненциальный алгоритм восстановления секретного ключа по открытому для этой криптосистемы. В настоящей работе предлагается атака на криптосистему Мак-Элиса, построенную на основе кодов Рида–Маллера, которая имеет в ряде случае полиномиальную сложность. Идея, предложенная Л. Миндером и А. Шокроллахи, заключается в сведении задачи взлома криптосистемы, построенной на основе кода $RM(r,m)$, к такой же задачи, но для кода $RM(1,m)$. В работе предлагается новый подход к реализации такого сведения. Он заключается в использовании операции умножения $\odot$ кодов и взятия ортогонального кода $\perp$, а также суперпозиции этих операций.

Доказаны следующие теоремы.

Теорема 1. *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* $RM^{\sigma\cdot\sigma'}(r,m) = RM(r,m)$.

Теорема 2. *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* $RM^{\sigma\cdot\sigma'}(r,m) = RM(r,m)$.

Авторам удалось с помощью предложенного алгоритма на ноутбуке осуществить взлом криптосистемы Мак-Элиса на основе кода $RM(4,10)$ за 0,43 секунды при этом атаке Л. Миндера и А. Шокроллахи для вскрытия такой криптосистемы требуется 22 часа 40 минут. Для кода $RM(4,11)$ требуется только 13,4 секунды, тогда как атаке Л. Миндера и А. Шокроллахи нужно около 10 дней. Код $RM(7,16)$ может быть с помощью предложенной атаки вскрыт за 6 часов 43 минуты.

Литература

1. Сидельников В.М. Открытое шифрование на основе двоичных кодов Рида-Маллера// Дискретная математика, т.6, вып. 3, 1994, С. 3–20.

2. McEliece R.J. A public-key cryptosystem based on algebraic coding theory.// DSN Prog. Rep., Jet Prop. Lab., California Inst. Technol., Pasadena, CA, 1978, P. 114–116

3. Minder L. and Shokrollahi A. Cryptanalysis of the Sidelnikov cryptosystem // LNCS. 2007.V. 4515. P. 347–360.