Math-Net.Ru

Общероссийский математический портал

Г. А. Карпунин, О ключевом пространстве криптосистемы Мак-Элиса на основе двоичных кодов Рида-Маллера, *Дискрет. матем.*, 2004, том 16, выпуск 2, 79–84

DOI: <https://doi.org/10.4213/dm153>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.237.206.68

26 апреля 2023 г., 14:13:41

О ключевом пространстве криптосистемы Мак-Элиса на основе двоичных кодов Рида–Маллера

© 2004 г. Г. А. Карпунин

В работе изучается кодовая криптосистема Мак-Элиса с u -кратным использованием двоичных кодов Рида–Маллера $RM(r, m)$. Эта модификация криптосистемы Мак-Элиса, имеющая высокую криптографическую стойкость, скорость передачи, близкую к единице, и невысокую сложность как шифрования, так и расшифрования, была предложена В. М. Сидельниковым в 1994 г. Для произвольных параметров u , r и m в настоящей работе доказана оценка сверху мощности множества открытых ключей этой криптосистемы, а также вычислено ее точное значение в случае $u = 2$ и $r = 1$.

1. Введение

В 1978 году Мак-Элис [1] одним из первых предложил криптосистему с открытым ключом. В отличие от большинства криптосистем с открытым ключом, базирующихся на сложности теоретико-числовых задач, криптосистема Мак-Элиса основана на сложности задач теории кодирования.

Опишем криптосистему Мак-Элиса. Пусть C — линейный двоичный $[n, k]$ -код, исправляющий t ошибок и имеющий быстрый алгоритм декодирования. Обозначим через G порождающую матрицу кода C . Абонент A случайно, равномерно и независимо от других абонентов выбирает невырожденную двоичную матрицу H размера $k \times k$, а также перестановочную матрицу Γ размера $n \times n$. Пара матриц (H, Γ) является секретным ключом абонента A , а матрица $E = H\Gamma G$ — его открытым (общедоступным для всех абонентов системы) ключом.

Пусть абоненту B необходимо передать абоненту A открытый текст m , представляющий собой k -элементный двоичный вектор. Для этого абонент B случайным образом выбирает n -элементный двоичный вектор z с весом, не большим t , и вычисляет шифрованное сообщение $c = mE + z$, которое посылает по общедоступному каналу абоненту A . Для расшифрования сообщения c абонент A сначала вычисляет $c' = c\Gamma^{-1}$. Затем с помощью декодирующего алгоритма кода C находит вектор m' , для которого $m'G$ отстоит от вектора c' на расстояние, не большее t . Наконец, вычисляется $m = m'H^{-1}$.

В оригинальной криптосистеме Мак-Элиса [1] в качестве кода C был использован код Гоппы. В. М. Сидельников в [2] предложил использовать двоичные коды Рида–Маллера $RM(r, m)$, имеющие более быстрые алгоритмы декодирования по сравнению с кодом Гоппы (см. [3]), а также в целях увеличения криптографической стойкости рассмотрел модифицированную криптосистему Мак-Элиса, которая устроена следующим образом.

Обозначим через R порождающую матрицу двоичного кода $RM(r, m)$ (без ограничения общности можно считать, что первая строчка матрицы R состоит из 1); через $k = k(r)$ размерность кода $RM(r, m)$; через $N = 2^m$ его длину. Абонент A случайно, равновероятно и независимо от других абонентов выбирает набор $\mathbf{H} = (H_1, \dots, H_u)$, состоящий из u невырожденных матриц $H_1, \dots, H_u$ фиксированного размера $k \times k$ с элементами из поля $F_2 = \{0, 1\}$, а также перестановочную матрицу Γ размера $uN \times uN$. Затем он образует набор матриц

$$E_1 = H_1 R, \dots, E_u = H_u R$$

и матрицу

$$E = (E_1 | \dots | E_u) \Gamma.$$

Матрица E является открытым ключом, а пара $(\mathbf{H}, \Gamma)$ — секретным ключом абонента A . Процедуры шифрования и расшифрования остаются прежними. Назовем эту криптосистему криптосистемой Мак-Элиса-Сидельникова.

Обозначим множество всех возможных открытых ключей через $\mathcal{E}$. Возникает естественный вопрос о количестве открытых ключей $|\mathcal{E}|$. В [2] была сформулирована гипотеза о том, что это количество равно

$$|\mathcal{E}| = \frac{(uN)! (h_k)^u}{u! |G_m|^u},$$

где $h_k = (2^k - 1)(2^k - 2) \dots (2^k - 2^{k-1})$ — мощность группы всех невырожденных матриц $GL(k, F_2)$, $|G_m|$ — мощность группы G_m автоморфизмов кода $RM(r, m)$, которая, как известно [4], равна $2^m(2^m - 1) \dots (2^m - 2^{m-1})$.

В данной работе показывается, что на самом деле имеет место строгое неравенство (предложение 1)

$$|\mathcal{E}| < \frac{(uN)! (h_k)^u}{u! |G_m|^u}, \quad (1)$$

а также явно вычисляется $|\mathcal{E}|$ в случае использования кода $RM(1, m)$ и параметра $u = 2$ (предложение 2).

2. Доказательство оценки

Поскольку каждый открытый ключ E вычисляется по некоторому секретному ключу $(\mathbf{H}, \Gamma)$, имеет смысл ввести на множестве секретных ключей следующее отношение эквивалентности. Два секретных ключа $(\mathbf{H}', \Gamma')$ и $(\mathbf{H}'', \Gamma'')$ будем считать эквивалентными, если соответствующие им открытые ключи E' и E'' совпадают. Тогда очевидно, что количество открытых ключей будет совпадать с количеством классов эквивалентности секретных ключей.

Далее для удобства каждый набор матриц $\mathbf{H} = (H_1, \dots, H_u)$ секретного ключа $(\mathbf{H}, \Gamma)$ будем задавать матрицами $H, A_1, \dots, A_{u-1}$, где $H = H_u$, $A_i = H_u^{-1} H_i$, $i = 1, \dots, u-1$ (легко сделать и обратное преобразование набора $(A_1, \dots, A_{u-1}, H)$ в набор $(H_1, \dots, H_u)$).

Напомним (см. [2]), что для криптосистемы Мак-Элиса при использовании обычного кода Рида-Маллера $RM(r, m)$ класс эквивалентности секретного ключа полностью восстанавливается по представителю данного класса и группе G_m автоморфизмов кода $RM(r, m)$. Группа G_m определяется как множество перестановочных матриц $\Gamma \in S_N$, для которых

существует матрица $H \in GL(k, \mathbb{F}_2)$ такая, что справедливо равенство $R\Gamma = HR$. В частности, мощность любого класса эквивалентности секретного ключа совпадает с $|G_m|$.

Для того, чтобы сформулировать аналогичный результат для криптосистемы Мак-Элиса–Сидельникова, для каждого секретного ключа $(\mathbf{H}, \Gamma)$, $\mathbf{H} = (A_1, \dots, A_{u-1}, H)$, определим совокупность

$$\Sigma_{A_1, \dots, A_{u-1}} = \{\Gamma \in S_{uN} : \exists A'_1, \dots, A'_{u-1}, H' \in GL(k, \mathbb{F}_2) \\ (A_1 R | \dots | A_{u-1} R | R)\Gamma = H'(A'_1 R | \dots | A'_{u-1} R | R)\}.$$

Обозначим через $[\mathbf{H}, \Gamma]$ класс эквивалентности секретного ключа $(\mathbf{H}, \Gamma)$. Легко показывается, что между секретными ключами из класса $[\mathbf{H}, \Gamma]$ и перестановочными матрицами из $\Sigma_{A_1, \dots, A_{u-1}}$ существует взаимно-однозначное соответствие, откуда вытекает следующее утверждение.

Лемма 1. *Мощность класса эквивалентности $[\mathbf{H}, \Gamma]$ секретного ключа $(\mathbf{H}, \Gamma)$, $\mathbf{H} = (A_1, \dots, A_{u-1}, H)$, совпадает с мощностью совокупности $\Sigma_{A_1, \dots, A_{u-1}}$, то есть*

$$|[\mathbf{H}, \Gamma]| = |\Sigma_{A_1, \dots, A_{u-1}}|.$$

Лемма 2. *Для любых матриц $A_1, \dots, A_{u-1} \in GL(k, \mathbb{F}_2)$ имеет место неравенство*

$$|\Sigma_{A_1, \dots, A_{u-1}}| \geq u! |G_m|^u.$$

Доказательство. Поскольку любая матрица Γ' из группы G_m обладает следующим свойством: существует матрица $H \in GL(k, \mathbb{F}_2)$ такая, что $R\Gamma' = HR$, то блочно диагональная перестановочная матрица $\Gamma^{(1)}$ размера $uN \times uN$, составленная из принадлежащих группе G_m матриц $\Gamma_1, \dots, \Gamma_u$, будет принадлежать совокупности $\Sigma_{A_1, \dots, A_{u-1}}$. Количество $|\Gamma^{(1)}|$ таких матриц равно $|G_m|^u$.

Очевидно также, что любая матрица $\Gamma^{(2)}$, переставляющая блоки $(A_i R$ или $R)$ в матрице $(A_1 R | \dots | A_{u-1} R | R)$ также принадлежит совокупности $\Sigma_{A_1, \dots, A_{u-1}}$. Количество $|\Gamma^{(2)}|$ таких матриц равно $u!$.

Так как произведение $\Gamma^{(1)}\Gamma^{(2)}$ двух перестановочных матриц первого и второго типа соответственно принадлежит $\Sigma_{A_1, \dots, A_{u-1}}$, отсюда следует утверждение леммы.

Лемма 3. *Пусть I — единичная матрица. Тогда имеет место равенство*

$$|\Sigma_{I, \dots, I}| = (u!)^N |G_m|^u.$$

Доказательство. Рассмотрим случай $u = 2$. Для этого случая необходимо доказать равенство $|\Sigma_I| = 2^N |G_m|^2$. Пусть $\Gamma \in \Sigma_I$, то есть $(R | R)\Gamma = (H_1 R | H_2 R)$. Умножая справа матрицу $(R | R)$ на матрицу Γ , мы делаем некоторую перестановку столбцов матрицы $(R | R)$. Покажем, что после этой перестановки два одинаковых столбца из разных блоков не могут попасть в один блок. В самом деле, пусть какой-то столбец e из правого блока и такой же столбец из левого блока после перестановки Γ попадают, например, в левый блок. Тогда $e = H_1 e'$ и $e = H_1 e''$, где e' и e'' — столбцы матрицы R . Следовательно, $e' = e''$. Но у порождающей матрицы R кода Риды–Маллера не может быть двух одинаковых столбцов.

Таким образом, перестановочную матрицу Γ можно представить в виде произведения двух перестановочных матриц $\Gamma'\Gamma''$. Здесь матрица Γ' выделяет некоторые пары одинаковых столбцов (один из левого блока, другой из правого) матрицы $(R | R)$ и переставляет

столбцы в этих парах; при этом получаем $(R \mid R)\Gamma' = (R \mid R)$. Матрица Γ'' , в свою очередь, действует отдельно в каждом блоке, то есть является блочно диагональной:

$$\Gamma'' = \begin{pmatrix} \Gamma_1 & 0 \\ 0 & \Gamma_2 \end{pmatrix}.$$

Тогда $(R \mid R)\Gamma = (R \mid R)\Gamma'' = (R\Gamma_1 \mid R\Gamma_2) = (H_1 R \mid H_2 R)$, и поэтому матрицы Γ_1 и Γ_2 принадлежат группе G_m .

Количество матриц типа Γ' равно 2^N , а количество матриц типа Γ'' равно $|G_m|^2$. Утверждение леммы доказано для случая $u = 2$. Для случая произвольного u рассуждения полностью аналогичны.

Предложение 1. *Имеет место оценка*

$$|\mathcal{E}| < \frac{(uN)!(h_k)^u}{u!|G_m|^u}.$$

Доказательство. Количество секретных ключей равно $(uN)!(h_k)^u$. Согласно лемме 1 мощность класса эквивалентности $[H = (H, A_1, \dots, A_{u-1}), \Gamma]$ секретных ключей совпадает с мощностью совокупности $\Sigma_{A_1, \dots, A_{u-1}}$, которая по лемме 2 не меньше $u!|G_m|^u$. Следовательно,

$$|\mathcal{E}| \leq \frac{(uN)!(h_k)^u}{u!|G_m|^u}.$$

Если же найдется класс эквивалентности, мощность которого строго больше $u!|G_m|^u$, то эта оценка будет строгой. В качестве такого класса можно, например, взять $[H = (H, I, \dots, I), \Gamma]$ (см. лемму 3).

3. Случай $u = 2$ и $r = 1$

В этом параграфе мы получим точное выражение мощности $|\mathcal{E}|$ множества открытых ключей для криптосистемы Мак-Элиса-Сидельникова, использующей код Риды-Маллера 1-го порядка и параметр $u = 2$. Далее R — порождающая матрица размера $(m+1) \times 2^m$ кода $RM(1, m)$, первая строчка которой состоит из 1.

Лемма 4. *Пусть матрица $A \in GL(m+1, \mathbb{F}_2)$ такова, что первая строка матрицы AR состоит из 1. Тогда*

$$|\Sigma_A| = 2^N |G_m|^2.$$

Доказательство. У матрицы AR (как и у R) нет двух одинаковых столбцов, количество столбцов равно 2^m , их длина равна $m+1$ и на первом месте в каждом столбце стоит 1, поэтому (из мощностных соображений) матрицы AR и R состоят из всех столбцов длины $m+1$, на первом месте которых стоит 1.

Далее доказательство дословно повторяет доказательство леммы 3.

Любая матрица из леммы 4 (назовем ее матрицей первого типа) представляется в виде

$$A = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ a' & & A' & \end{pmatrix},$$

где A' — невырожденная двоичная матрица размера $m \times m$, a' — произвольный двоичный вектор длины m . Тогда количество невырожденных матриц первого типа равно $N_1(A) = 2^m h_m$.

Лемма 5. Пусть $A \in GL(m+1, \mathbb{F}_2)$ такова, что первая строка матрицы AR не состоит сплошь из 1. Тогда

$$|\Sigma_A| = 2^{N/2+1} |G_m|^2.$$

Доказательство. Первая строчка матрицы AR является кодовым словом c кода $RM(1, m)$. Кодовое слово c не может состоять только из 1 по условию леммы и не может состоять только из 0 в силу невырожденности матрицы A . Известно [4], что вес любого кодового слова (за исключением $(0 \dots 0)$ и $(1 \dots 1)$) кода $RM(1, m)$ должен быть равен $2^{m-1} = N/2$. Поэтому в первой строчке матрицы AR ровно половина единиц и половина нулей.

Пусть Γ — перестановочная матрица из Σ_A , то есть существуют матрицы $H_1, H_2 \in GL(m+1, \mathbb{F}_2)$, такие, что $(AR | R)\Gamma = (H_1 R | H_2 R)$. Следовательно, первая строчка в первом блоке и первая строчка во втором блоке матрицы $(AR | R)\Gamma$ должны быть кодовыми словами кода $RM(1, m)$. И поскольку количество нулей в каждой из строчек матрицы AR равно либо $N/2$, либо нулю, матрица Γ либо переставляет все столбцы матрицы $(AR | R)$ с нулем в верхней позиции из первого (левого) блока во второй, либо оставляет их в первом блоке.

Предположим теперь для определенности, что матрица Γ оставляет все столбцы матрицы $(AR | R)$ с нулем в верхней позиции в первом блоке. Тогда матрица Γ обязана оставить набор столбцов первого блока с единицей в верхней позиции также в первом блоке, возможно заменив некоторые из них на точно такие же столбцы из второго блока. В противном случае во втором блоке матрицы $(AR | R)\Gamma$ оказалось бы два одинаковых столбца, что невозможно (см. доказательство леммы 3).

Таким образом, матрицу $\Gamma \in \Sigma_A$ можно представить в виде произведения трех перестановочных матриц $\Gamma' \Gamma'' \Gamma'''$. Матрица Γ' либо просто меняет местами первый и второй блок, либо является тождественной перестановкой. Таких матриц всего 2. Матрица Γ'' меняет некоторые из столбцов одного блока с единицей в верхней позиции на точно такие же столбцы из другого блока. Поскольку максимальное число возможных замен равно $N/2$, количество матриц типа Γ'' равно $2^{N/2}$. Как и в доказательстве леммы 3, матрица Γ действует отдельно в каждом блоке, то есть является блочно диагональной:

$$\Gamma''' = \begin{pmatrix} \Gamma_1 & 0 \\ 0 & \Gamma_2 \end{pmatrix},$$

где $\Gamma_1, \Gamma_2 \in G_m$. Число матриц типа Γ''' равно $|G_m|^2$. Произведение $|\Gamma'| |\Gamma''| |\Gamma'''|$ дает требуемое в лемме выражение для $|\Sigma_A|$.

Количество матриц A из леммы 5 (назовем их матрицами второго типа) равно $N_2(A) = h_{m+1} - N_1(A) = h_{m+1} - 2^m h_m$.

Из лемм 4 и 5 вытекает, что два секретных ключа, у которых матрицы A относятся к разным типам не могут быть эквивалентны. Поэтому совокупность классов эквивалентности секретных ключей разбивается на два типа в зависимости от типа матрицы A какого-нибудь представителя. Количество классов эквивалентности первого типа равно

$$\frac{(2N)! h_{m+1} N_1(A)}{2^N |G_m|^2},$$

количество классов эквивалентности второго типа равно

$$\frac{(2N)! h_{m+1} N_2(A)}{2^{N/2+1} |G_m|^2}.$$

Складывая эти два равенства, получаем следующее утверждение.

Предложение 2. Для количества $|\mathcal{E}|$ открытых ключей в криптосистеме Мак-Элиса–Сидельникова на основе двоичного кода Рида–Маллера 1-го порядка с параметром $u = 2$ справедливо равенство

$$|\mathcal{E}| = \frac{(2N)!}{2^{N/2+1}|G_m|^2} \left(h_{m+1} - 2^m h_m \left(1 - \frac{1}{2^{N/2-1}} \right) \right).$$

Автор выражает глубокую благодарность В. М. Сидельникову за постановку задач и внимание к работе.

Список литературы

1. McEliece R. J., A public-key cryptosystem based on algebraic coding theory. *DSN Prog. Rep.*, Jet Prop. Lab., California Inst. Technol., Pasadena, 1978, 114–116.
2. Сидельников В. М., Открытое шифрование на основе двоичных кодов Рида–Маллера. *Дискретная математика* (1994) **6**, №2, 3–20.
3. Сидельников В. М., Першаков А. С., Декодирование кодов Рида–Маллера при большом числе ошибок. *Пробл. передачи информации* (1992) **28**, №3, 80–94.
4. Мак-Вильямс Ф. Дж., Слоэн Н. Дж., *Теория кодов, исправляющих ошибки*. Связь, Москва, 1979.

Статья поступила 16.07.2002.