УДК 512.772

И. Д. Ильяшенко

АНАЛИЗ СТОЙКОСТИ КРИПТОСИСТЕМЫ МАК-ЭЛИСА НА АГ- КОДАХ К КВАНТОВОМУ СЭМПЛИРОВАНИЮ ФУРЬЕ

Проверяется квантовая стойкость криптосистемы Мак-Элиса, построенной на произвольном АГ-коде над некоторой эллиптической кривой. С помощью критерия, предложенного Динх, Муром и Расселом [3], доказано, что данная криптосистема является стойкой к квантовому сэмплированию Фурье. Таким образом, алгоритм Шора не сможет раскрыть групповую структуру кода и взломать криптосистему.

This article tests the quantum resistance of McEliece CS based on an AG-code over any elliptic curve. Using the criteria suggested by Dinh, Moore, and Russell [3], the author proves the resistance of this CS to quantum Fourier sampling attack. Thus, Shor's algorithm cannot identify the group structure of the code and break the CS.

Ключевые слова: квантовый алгоритм, постквантовая криптография, эллиптические кривые, алгебро-геометрические коды.

Key words: quantum algorithm, post-quantum cryptography, elliptic curves, AG-codes.

Введение

Квантовые компьютеры на данный момент далеки по производительности от своих классических «собратьев», но теоретически представляют угрозу современным стандартам шифрования. Процедура квантового сэмплирования Фурье, лежащая в основе алгоритма Шора [1] и его модификаций, за полиномиальное время решает проблему скрытой подгруппы — краеугольного камня криптографии с открытым

ключом, используемой в приложениях: дискретный логарифм, факторизация, эквивалентность кодов и т.д. Ряд криптосистем отнесен к постквантовой криптографии, то есть стойкой к квантовым атакам, одна из них — криптосистема Мак-Элиса [2], основанная на применении бинарных кодов Гоппы. Стойкость не является основанием ее практического использования ввиду больших размеров ключей. Для уменьшения размера ключа можно использовать алгебраические кривые ненулевых родов, но это может снизить безопасность системы.

Далее будет доказана стойкость модификации криптосистемы Мак-Элиса к квантовому сэмплированию Фурье. Ограничимся случаем, когда АГ-код построен над эллиптическим функциональным полем. Стойкость оригинальной криптосистемы доказана в [3], где приводится критерий стойкости, условия которого последовательно проверятся.

1. Предварительные сведения

В классическом виде криптосистема Мак-Элиса выглядит следующим образом. Выбираем натуральные числа t и n, причем n равно степени 2 и $t \ll n$. Находим произвольный неприводимый многочлен степени t из поля $\mathbb{F}_{2^m}$, где $n = 2^m$. Строим порождающую матрицу кода Гоппы G размера $k \times n$, где $k \geqslant n - tm$.

Для кодов Гоппы существует эффективный метод декодирования, поэтому необходимо скрыть структуру полученного кода. С этой целью выбираем бинарную неприводимую $k \times k$ матрицу S, $n \times n$ матрицу перестановки P. Вычисляем $G' = SGP$. В итоге получаем открытый ключ (G', t), который можно опубликовать. Закрытым ключом является $(S, \mathcal{D}_G, P)$, где $\mathcal{D}_G$ — эффективный алгоритм декодирования кода G.

Объем ключевого пространства равен

$$\frac{n^t}{t} n! \left(n^n - 1\right)\left(n^n - n\right)\ldots\left(n^n - n^{n-1}\right).$$

Код, порождаемый матрицей G', имеет ту же размерность и минимальное расстояние, что и исходный код Гоппы.

Пусть $m \in \mathbb{F}_2^k$ — исходное сообщение. Случайным образом выбираем вектор $z \in \mathbb{F}_2^n$, вес Хэмминга которого равен t. Получаем шифротекст $c = mG' \oplus z$.

Для дешифровки вычислим $cP^{-1} = (mS)G \oplus zP^{-1}$. Так как cP^{-1} имеет дистанцию Хэмминга t к коду G, то, применяя алгоритм декодирования Гоппы, получим mS. Итак, исходное сообщение $m = mSS^{-1}$.

Использующийся здесь бинарный код Гоппы является частным случаем АГ-кодов.

Пусть $F / \mathbb{F}_q$ — алгебраическое функциональное поле, $P_1, \ldots, P_n$ — попарно различные точки $F / \mathbb{F}_q$ степени 1 (то есть $\mathbb{F}_q$ — рациональные

точки кривой [5]), $D = P_1 + \ldots + P_n$, G — дивизор $F / \mathbb{F}_q$ такой, что $\mathrm{Supp}\, G \cap \mathrm{Supp}\, D = \varnothing$, $\mathcal{L}(G) = \{x \in F \mid (x) \geqslant -G\} \cup \{0\}$ — пространство Римана — Роха, ассоциированное с G.

Определение. *Алгебро-геометрическим кодом (или АГ-кодом)* $C_{D,G}$, ассоциированным с дивизорами D, G, является

$$C_{D,G} := \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n.$$

В дальнейшем будем вместо $C_{D,G}$ использовать просто C.

$\mathrm{Aut}(C) = \{\pi \in S_n \mid \pi(C) = C\}$ — группа автоморфизмов кода C.

Определение. *Минимальная степень группы автоморфизмов АГ-кода C:*

$$\min(\mathrm{Aut}(C)) = \min_{\sigma \in \mathrm{Aut}(C), \sigma \neq id_C} (\#\, c \in C : \sigma(c) \neq c).$$

Определение. *Минимальная степень группы автоморфизмов функционального поля, соответствующего кривой:*

$$\min(\mathrm{Aut}(F/\mathbb{F}_q)) = \min_{\sigma \in \mathrm{Aut}(F/\mathbb{F}_q), \sigma \neq id_F} (\#\, x \in F : \sigma(x) \neq x).$$

2. Критерий

В работе [3] был получен следующий критерий стойкости криптосистемы к квантовому преобразованию Фурье.

Теорема 1. *Пусть* $q^{k^2} \leqslant n^{0.2n}$ *и группа автоморфизмов Aut(C) имеет минимальную степень* $\Omega(n)$, r *— ранг порождающей матрицы кода C. Тогда подгруппа K кода C неразличима, если*

$$|Aut(C)| \leqslant e^{o(n)},\ r \geqslant \frac{k - o(\sqrt{n})}{m},$$

где m — степень расширения $F / \mathbb{F}_q$.

Рассмотрим сначала мощность группы автоморфизмов кода. Пусть $\sigma \in \mathrm{Aut}(C)$, тогда $c \in C$, $c = (c_1, \ldots, c_n) = (f(P_1), \ldots, f(P_n))$,

$$\sigma(c) = (c_{\sigma(1)}, \ldots, c_{\sigma(n)}) = (f(P_{\sigma(1)}), \ldots, f(P_{\sigma(n)})).$$

Итак, автоморфизм кода действует на точки функционального поля: $\sigma(P_i) = P_{\sigma(i)}$, значит, σ — автоморфизм $F / \mathbb{F}_q$ и $\mathrm{Aut}(C) \subseteq \mathrm{Aut}(F / \mathbb{F}_q)$.

Известно, что число автоморфизмов эллиптической кривой ограничено [6] и равно некоторому делителю числа 24. Таким образом,

$$|\mathrm{Aut}(F / \mathbb{F}_q)| \leqslant e^{o(n)} \Rightarrow |\mathrm{Aut}(C)| \leqslant e^{o(n)}.$$

Также для порождающей матрицы линейного кода всегда $r = k$, то есть выполняется третье условие критерия. Остается рассмотреть минимальную степень группы автоморфизмов кода.

3. Группы автоморфизмов эллиптической кривой

Число автоморфизмов эллиптической кривой ограничено и равно делителю числа 24.

Теорема 2 [6, с. 103]. *Пусть E/K – эллиптическая кривая. Тогда ее группа автоморфизмов конечного порядка – делителя 24. Возможны случаи:*

$$2, \text{ если } j(E) \neq 0,1728;\ 4, \text{ если } j(E) = 1728 \text{ и } char(K) \neq 2,3;$$

$$6, \text{ если } j(E) = 0 \text{ и } char(K) \neq 2,3;\ 12, \text{ если } j(E) = 0 = 1728 \text{ и } char(K) = 3;$$

$$24, \text{ если } j(E) = 0 = 1728 \text{ и } char(K) = 2.$$

Рассмотрим действие автоморфизмов на рациональные точки эллиптической кривой при $\mathrm{char}\ K = 2$.

1. $j(E) \neq 0 \neq 1728$. Кривая в данном случае описывается уравнением

$$y^2 + xy = x^3 + a_2x^2 + a_6, \text{ где } a_6 \neq 0.$$

Автоморфизмы представляют собой замену $x = x,\ y = y + sx$, где $s^2 + s = 0 \Rightarrow s = 0,1$: $\sigma_1 : (x,y) \mapsto (x,y)$, $\sigma_2 : (x,y) \mapsto (x, y+x)$.

Автоморфизм σ_2 фиксирует точки $(0, \pm\sqrt{a_6})$ и точку на бесконечности, то есть минимальная степень $\mathrm{Aut}(E)$ равна $n - 3 \in \Omega(\mathrm{n})$.

2. $j(E) = 0 = 1728$. Уравнение кривой:

$$y^2 + a_3y = x^3 + a_4x + a_6, \text{ где } a_3 \neq 0.$$

Здесь автоморфизмы такие: $x = u^2x + s^2$, $y = y + u^2sx + t$, где $u^3 = 1$, $s^4 + a_3s + (1-u)a_4 = 0$, $t^2 + a_3t + s^6 + a_4s^2 = 0$.

Далее будем рассматривать автоморфизмы как тройки.

Пусть $u = 1$: $(x,y) \mapsto (x + s^2, y + sx + t)$. Точки зафиксированы при условии, что $s = 0$ и $t = 0$. Получаем тождественный автоморфизм (1, 0, 0), следовательно, остальные фиксируют лишь точку на бесконечности.

Пусть $u = \alpha$, где $\mathrm{ord}\ \alpha = 3$ и $\alpha^2 = \alpha + 1$. Здесь восемь автоморфизмов:

$$(x, y) \mapsto (\alpha^2x + s^2, y + \alpha^2sx + t).$$

Подставляя $\alpha^2 = \alpha + 1$, имеем условие фиксации точек $\alpha x = s^2, \alpha s^3 = t$.

Преобразуем уравнение кривой через замену $x = \dfrac{s^2}{\alpha}$:

$$y^2 + a_3y + a_3s^3 + a_6 = 0.$$

Зафиксируем корень s_1 уравнения $s_4 + a_3s + (1+\alpha)a_4 = 0$. Тогда $t = s_1^3\alpha$. Таким образом, получаем автоморфизм $(\alpha, s_1, s_1^3\alpha)$, который фиксирует помимо точки на бесконечности еще две с координатами $(\dfrac{s_1^2}{\alpha}, y)$, где $y_2 + a_3y + a_3s_1^3 + a_6 = 0$. Аналогично и для остальных корней s_2, s_3, s_4.

Поделив $t^2 + a_3t + s^6 + a_4s_1^2$ на $t + s^3\alpha$, получим четыре автоморфизма $(\alpha, s, s^3\alpha + a_3)$, которые фиксируют только точку на бесконечности.

В итоге оказывается, что минимальная степень $\mathrm{Aut}(E)$ равна $n - 3 \in \Omega(\mathrm{n})$. Аналогично получаем, что для $\mathrm{char}\ K \neq 2$ эта величина равна $n - 4 \in \Omega(\mathrm{n})$.

Заключение

Криптосистема Мак-Элиса, построенная на АГ-кодах над эллиптическими кривыми, не может быть взломана квантовым преобразованием Фурье (то есть алгоритмом Шора) при достаточно большом размере основного поля. Было показано, что АГ-коды удовлетворяют всем условиям критерия стойкости для произвольных эллиптических кривых.

Список литературы

1. *Shor P.W.* Algorithms for quantum computation: discrete logarithms and factoring // Found. of Computer Science : Conference Publications. 1994. P. 124—134.

2. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory // DSN Progress Report. 1978. № 42—44. P. 114—116.

3. *Dinh H., Moore C., Russell A.* The McEliece cryptosystem resists quantum Fourier sampling attacks. 2010. URL: http://arxiv.org/abs/1008.2390 (дата обращения: 12.02.2015).

4. *Stichtenoth H.* On automorphisms of geometric Goppa codes // Journal of Algebra. 1990. № 130(1). P. 113—121.

5. *Stichtenoth H.* Algebraic function fields and codes. Springer, 2008.

6. *Silverman J.* Arithmetic of elliptic curves. Springer, 2009.

Об авторе

Илья Дмитриевич Ильяшенко — асп., Балтийский федеральный университет им. И. Канта, Калининград.
E-mail: tommplay@gmail.com

About the author

Ilia Ilyashenko, PhD student, I. Kant Baltic Federal University, Kaliningrad.
E-mail: tommplay@gmail.com