ПРОГРАММНО-
ТЕХНИЧЕСКИЕ
КОМПЛЕКСЫ

В.Е. ЧЕВАРДИН

УДК 512.742

ИЗОМОРФНЫЕ ТРАНСФОРМАЦИИ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ НАД КОНЕЧНЫМ ПОЛЕМ

Ключевые слова: *эллиптические кривые, трансформация эллиптической кривой, изоморфные эллиптические кривые, изоморфные трансформации.*

ВВЕДЕНИЕ

В настоящее время наиболее надежным несимметричным преобразованием исходя из криптографической стойкости является операция скалярного умножения точки несуперсингулярной эллиптической кривой [1–3]. Однако несимметричная операция умножения точки кривой в сравнении с операциями, используемыми в симметричных преобразованиях, требует высокой вычислительной сложности. Тем не менее последние результаты исследований криптосистем на основе эллиптических кривых показали широкий спектр их использования: с целью усовершенствования алгоритмов генерации параметров эллиптической кривой [4–6], при применении новых форм эллиптических кривых [7], а также эллиптических кривых для генерации псевдослучайных последовательностей [8–14] и др.

Одним из перспективных направлений усовершенствования криптосистем на основе эллиптических кривых является переход к абелевым группам большого порядка, например использованию групп дивизоров точек гиперэллиптической кривой. Высокая вычислительная сложность таких преобразований не позволяет применять их на практике. В результате поиска альтернативных вариантов расширения возможностей использования абелевых групп были выбраны изоморфные трансформации точек несуперсингулярной эллиптической кривой.

Изоморфные трансформации уже применялись для генерации однонаправленных псевдослучайных функций [10]. Недостатком этого подхода является возможность использования только двух изоморфных кривых для построения псевдослучайной последовательности и использования конечного поля F_q. В работах [1, 2] уделено достаточно внимания преобразованиям над полем F_q, а также предложены изоморфные трансформации эллиптической кривой для построения алгоритмов генерации параметров эллиптических кривых. Однако оценки мощностей изоморфных трансформаций в этих работах представлены не были.

Таким образом, исследование изоморфных трансформаций эллиптической кривой над расширениями конечных полей Галуа и оценка мощности их множества является актуальным научно-техническим заданием.

ЭЛЛИПТИЧЕСКАЯ КРИВАЯ И ЕЕ ИЗОМОРФНАЯ ТРАНСФОРМАЦИЯ

Исходя из результатов работы [2] рассмотрим несуперсингулярную эллиптическую кривую и способы ее трансформации.

Пусть произвольная несуперсингулярная эллиптическая кривая E определена каноническим уравнением кривой над полем F_{2^m}:

$$E: y^2 + yx = (x^3 + ax^2 + b) \bmod f(x), \tag{1}$$

где $a, b \in F_{2^m}$, $f(x)$ — неприводимый полином над полем F_{2^m}.

Несуперсингулярные эллиптические кривые E_1 и E_2 над расширением конечного поля Галуа считаются изоморфными, если существует изоморфизм φ группы точек кривой E_1 в группу точек кривой E_2, т.е. $\varphi: E_1 \to E_2$. Рассмотрим один из способов изоморфной трансформации кривой (1).

Выполним изоморфную трансформацию кривой (1) посредством введения новой переменной для некоторого $k \in F^*_{2^m}$. Тогда $y = \nu + kx$, где $\nu, x \in F_{2^m}$, и уравнение (1) в новых переменных (x, ν) примет вид

$$(\nu + kx)^2 + x(\nu + kx) = x^3 + ax^2 + b,$$

$$\nu^2 + k^2x^2 + \nu x + kx^2 = x^3 + ax^2 + b,$$

$$\nu^2 + \nu x = x^3 + (k^2 + k + a)x^2 + b.$$

Проведем замену $a' = k^2 + k + a$ и получим уравнение (1) в новых переменных:

$$\nu^2 + \nu x = x^3 + a'x^2 + b..$$

Заменой $\alpha = a' + a$ получим

$$k^2 + k = \alpha. \tag{2}$$

Утверждение 1. Для произвольной несуперсингулярной эллиптической кривой над полем F_{2^m} существование ее изоморфной трансформации определяется существованием решения уравнения (2), т.е. требованием $\mathrm{Tr}(\alpha) = 0$ или $\mathrm{Tr}(a') = \mathrm{Tr}(a)$.

Для доказательства существования изоморфной трансформации, полученной заменой $y = \nu + kx$, воспользуемся определением следа элемента $y \in F_{2^m}$:

$$\mathrm{Tr}(y) = y + y^2 + y^4 + y^8 + \ldots + y^{2^{n-1}}, \ \mathrm{Tr}(y) \in F_2.$$

Докажем справедливость утверждения 1.

Для нечетного m при условии $\mathrm{Tr}(\alpha) = 0$ определим два решения уравнения (2):

$$k = \alpha + \alpha^4 + \alpha^{16} + \alpha^{64} + \ldots + \alpha^{2^{m-1}}, \tag{3}$$

$$k' = 1 + k.$$

С использованием формулы (3) найдем k^2:

$$k^2 = \alpha^2 + \alpha^8 + \alpha^{32} + \alpha^{128} + \ldots + \alpha^{2^m} = \alpha + \alpha^2 + \alpha^8 + \alpha^{32} + \alpha^{128} + \ldots + \alpha^{2^{m-2}}. \tag{4}$$

Учитывая линейность следа $\mathrm{Tr}(\alpha) = \mathrm{Tr}(k^2 + k) = \mathrm{Tr}(k^2) + \mathrm{Tr}(k) = 0$ и условие $\mathrm{Tr}(\alpha) \neq 0$, подставим выражения (3) и (4) в (2):

$$k^2 + k = a + (a + a^2 + a^4 + a^{16} + a^{32} + \ldots + a^{2^{m-1}}) = a + \mathrm{Tr}(a) \neq a.$$

Таким образом, уравнение (2) имеет решение только при $\mathrm{Tr}(\alpha) = 0$, т.е. $\mathrm{Tr}(a') = \mathrm{Tr}(a)$.

МОЩНОСТЬ МНОЖЕСТВА ИЗОМОРФНЫХ ТРАНСФОРМАЦИЙ

Согласно утверждению 1 $\mathrm{Tr}(a') = \mathrm{Tr}(a)$, т.е. число изоморфных трансформаций при замене $y = v + kx$ равно числу комбинаций a' и a при $a' \neq a$.

Утверждение 2. Для произвольной несуперсингулярной эллиптической кривой (1) при фиксированном коэффициенте b существует ровно 2^{m-1} изоморфных трансформаций.

Доказательство этого утверждения следует из существования для фиксированного $a \in F_{2^m}$ ровно $2^{m-1} - 1$ таких элементов $a' \in F_{2^m}$, что $\mathrm{Tr}(a') = \mathrm{Tr}(a)$, причем $a' \neq a$. Общее число изоморфных трансформаций этого типа за счет изменения коэффициента a равно 2^{m-1}.

Изоморфная трансформация кривой также возможна при замене коэффициента b на b^{2^i}, где $0 \le i \le m-1$. Отсюда вытекает справедливость утверждения 3.

Утверждение 3. Для произвольной несуперсингулярной эллиптической кривой вида (1) при возведении коэффициента b в квадрат $(m-1)$ раз существует ровно m изоморфных трансформаций эллиптической кривой.

С учетом утверждений 2 и 3 получим следующее утверждение.

Утверждение 4. Для произвольной несуперсингулярной эллиптической кривой (1) существует ровно $m \cdot 2^{m-1}$ изоморфных трансформаций, полученных заменой коэффициентов $a, b \in F_{2^m}$.

Рассмотренный вариант трансформаций эллиптической кривой (1) соответствует $\mathrm{Tr}(x + a_2 + bx^{-2}) = 0$ в [2], т.е. учитываются случаи, когда $\mathrm{Tr}(a) = 1$ либо $\mathrm{Tr}(a) = 0$ при нечетном m. Кривые со следами $\mathrm{Tr}(a) = 0$ и $\mathrm{Tr}(a) = 1$ являются кривыми кручения [2].

ЗАКЛЮЧЕНИЕ

В результате проведенного анализа трансформаций несуперсингулярной эллиптической кривой $E: y^2 + yx = (x^3 + ax^2 + b) \bmod f(x)$ над полем F_{2^m} было получено число трансформаций несуперсингулярной эллиптической кривой, которое зависит от степени расширения поля Галуа. Так, общее число трансформаций несуперсингулярной эллиптической кривой (1) равно $m \cdot 2^{m-1}$. Доказанные утверждения позволяют рассчитывать мощность множества трансформаций несуперсингулярной эллиптической кривой, что свидетельствует о целесообразности разработки и усовершенствовании перспективных криптографических систем и алгоритмов на основе преобразований в группе точек эллиптической кривой. Например, уже при трансформации на основе изменения коэффициента a существует 2^{m-1} изоморфных трансформаций, что открывает новую возможность использовать изоморфные трансформации в качестве дополнительного параметра, влияющего на энтропию при восстановлении либо прогнозировании внутренних состояний криптосистемы на эллиптических кривых.

СПИСОК ЛИТЕРАТУРЫ

1. Коблиц Н. Курс теории чисел и криптографии: Пер. с англ. М.А. Михайловой и В.Е. Тараканова / Под ред. А.М. Зубкова. — М.: Науч. издательство ТВП, 2001. — 254 с.
2. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых: Учеб. пособие. — К.: ІВЦ «Видавництво «Політехніка»», 2004. — 224 с.
3. Husemöller D. Elliptic Curves, Second ed. — New York: Springer, 2002. — 487 p.

4. Konstantinou E. On the efficient generation of elliptic curves over prime fields // Lecture Notes in Computer Science. — 2002. — **2523**. — P. 333–348.
5. Baier H., Buchmann J. Efficient construction of cryptographically strong elliptic curves // In: Progress in Cryptology — INDOCRYPT 2000, LNCS, 1977. — Berlin: Springer-Verlag, 2000. — P. 191–202.
6. Broker R., Stevenhagen P. Constructing elliptic curves of prime order // Contemporary Mathematics. — 2008. — N 463. — P. 17–28.
7. Edwards H.M. A normal norm for elliptic curves // Bulletin of the American Mathematical Society.– 2007. — **44**. — P. 393–422.
8. Kaliski Jr.B.S. A pseudo-random bit generator based on elliptic logarithms // Advances in Cryptology: Proceedings of Crypto'86. — New York: Springer-Verlag, 1987. — P. 84–103.
9. Impagliazzo R. Pseudo-random generation from one-way functions // Proc. of the 21st Annual ACM Symposium on Theory of Computing, ACM, New York. — 1989. — P. 12–24.
10. Burton S. One-way permutations on elliptic curves // J. of Cryptology. International Association for Cryptologic Research. — 1991. — **3**, N 3 — P. 187–199.
11. Gjøsteen K. Comments on Dual-EC-DRBG/NIST SP 800-90, Draft, December 2005 // March 16. — 2006.
12. NIST Special Publication 800-90A. Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised) / Computer Security Division Information Technology Laboratory. National Institute of Standards and Technology. — January 2012. — P. 128.
13. Горбенко І.Д., Шапочка Н.В., Погребняк К.А. Метод побудування випадкових бітів на основі спарювання точок еліптичних кривих // Прикладная радиоэлектроника. — 2010. — **9**, № 3. — С. 386–394.
14. Бессалов А.В., Чевардин В.Е. Метод генерации псевдослучайных последовательностей на основе изоморфных трансформаций эллиптической кривой // Там же. — 2012. — **11**, № 2. — С. 234–237.

Поступила 09.07.2012