

2. Атакующая сторона выбирает такие варианты реализации атаки на АС, чтобы у формирующего КСЗИ не хватило финансовых средств для построения эффективной КСЗИ (“тактика истощения”).

Для построения эффективной КСЗИ, следует учитывать возможности атакующей стороны, а также возможные стратегии их действий.

### Заключение

В перспективе представляется рациональным использовать методы математической теории игр для описания процесса защиты информации как процесса бесконечной антагонистической игры с неполной информацией. При этом могут быть рассмотрены различные стратегии игроков, в том числе вопросы формирования коалиций (как атакующей стороной, так и формирующей КСЗИ АС).

### Список литературы

1. Грездов Г.Г. Методика построения модели распределенной атаки на автоматизированную систему. Научно-практичний журнал “Сучасна спеціальна техніка”, №3, 2009. - сс. 82-90.
2. Грездов Г.Г. Модифицированный способ решения задачи формирования эффективной комплексной системы защиты информации автоматизированной системы. Монография, Киев – ГУИКТ, 2009.- 32 с.
3. Грездов Г.Г. Методика построения теста на проникновение в автоматизированную систему, основанная на математической теории игр. Наукові записки українського науково-дослідного інституту зв'язку, 2010, № 3. - сс. 88-94.
4. Лукацкий А.В. Обнаружение атак. - Санкт - Петербург: ВНУ, 2001. - 611 с.
5. Майника Э. Алгоритмы оптимизации на сетях и графах. – М. : Мир, 1981. - 328 с.
6. Мак-Кинси,Д. Введение в теорию игр.- Киев: Издательство КВИРТУ, 1959. - 347 с.

*Рецензент: Корнийчук М.Т.*

*Поступила 26.05.2011*

**Бессалов А.В., Дихтенко А.А., Третьяков Д.Б.**

### Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем

#### Введение

В работе профессора университета Нью-Йорка Г. Эдвардса [1] предложена нормальная форма представления эллиптических кривых, которая изучалась еще Абелем в 1828 году. Эта форма, получившая в научном мире название формы Эдвардса, обладает рядом замечательных свойств для криптографических приложений. Одной из первых публикаций в развитие этого направления следует отметить работу [2]. Оказалось, что наряду с симметрией, свойствами полноты и универсальности закона сложения, заменой точки на бесконечности аффинной точкой (нуль группы), кривые Эдвардса среди известных являются наиболее производительными: в проективных координатах групповая операция выполняется минимальным числом  $10M + 1S + 1U$  операций в поле ( $M$  - умножение,  $S$  – возведение в квадрат,  $U$  – умножение на параметр кривой). В настоящей работе мы даем детальный сравнительный анализ вычислительной сложности групповой операции в проективных координатах для кривых в форме Эдвардса и канонической эллиптической кривой над полем характеристики, не равной 2 и 3.

#### Сложность групповой операции для кривой Эдвардса

В наиболее общем виде кривая Эдвардса над конечным полем  $\mathbb{F}_q$  ( $q = p^m$ ) характеристики  $p > 3$  может быть выражена как [2]

$$E_{ED}: \quad x^2 + y^2 = c^2(1 + \tilde{d}x^2y^2), \quad \tilde{d} = c^{-4}d, \tilde{d}(1 - \tilde{d}c^4) = 1, \tilde{d} = d/c^4. \quad (1)$$

Закон сложения двух точек этой кривой имеет вид

$$(x_1, y_1) + (x_2, y_2) = \left( \frac{x_1y_2 + x_2y_1}{c(1 + \tilde{d}x_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{c(1 - \tilde{d}x_1x_2y_1y_2)} \right) \quad (2)$$

Варьирование параметра  $c$  дает изоморфные кривые. Поэтому с точностью до изоморфизма можно полагать  $c = 1$ ,  $\tilde{d} = d$ . Наличие 2-х инверсий в (2) заставляет обращаться к проективным координатам [4]. Введем третью координату  $Z$  как общий знаменатель в (2). Полагаем  $x = \frac{X}{Z}$ ,  $y = \frac{Y}{Z}$ , тогда гомогенизованное уравнение кривой (1) в проективных координатах имеет вид

$$(X^2 + Y^2)Z^2 = Z^4 + dX^2Y^2.$$

Сумма двух точек теперь записывается как  $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3 : Y_3 : Z_3)$ . С учетом подстановок выразим координаты суммарной точки  $(X_3 : Y_3 : Z_3)$

$$\begin{aligned} x_3 = \frac{X_3}{Z_3} &= \frac{\left(\frac{X_1Y_2 + X_2Y_1}{Z_1Z_2} + \frac{X_2Y_1}{Z_1Z_2}\right)\left(1 - d\frac{X_1X_2Y_1Y_2}{Z_1^2Z_2^2}\right)}{\left(1 + d\frac{X_1X_2Y_1Y_2}{Z_1^2Z_2^2}\right)\left(1 - d\frac{X_1X_2Y_1Y_2}{Z_1^2Z_2^2}\right)} = \\ &= \frac{Z_1Z_2(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)(X_1Y_2 + X_2Y_1)}{(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)} \\ y_3 = \frac{Y_3}{Z_3} &= \frac{Z_1Z_2(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(X_1Y_2 - X_2Y_1)}{(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)} \end{aligned}$$

Обозначим:

$$A = Z_1Z_2; \quad B = A^2; \quad C = X_1X_2; \quad D = Y_1Y_2; \quad E = dCD; \quad F = B - E; \quad G = B + E$$

Тогда

$$\begin{aligned} X_3 &= A \cdot F \cdot ((X_1 + Y_1) \cdot (X_2 + Y_2) - C - D), \\ Y_3 &= A \cdot G \cdot (D - C), \\ Z_3 &= F \cdot G. \end{aligned}$$

Игнорируя простую операцию сложения (вычитания) в поле, найдем сложность вычисления суммы различных точек  $V_{ED} = 10M + 1S + 1U$ . Заметим, что сложность возведения в квадрат оценивается приблизительно как  $1S \cong \frac{2}{3}M$  [2].

Нетрудно подобным же образом определить сложность умножения точек как  $W_{ED} = 3M + 4S$ . Экономия в вычислениях здесь достигается заменой сложения знаменателей в (2)  $(1 + dx_1^2y_1^2)$  на  $(x_1^2 + y_1^2)$ , а  $(1 - dx_1^2y_1^2)$  – на  $(2 - (x_1^2 + y_1^2))$ .

### Сложность групповой операции для канонической кривой

Обратимся теперь к канонической эллиптической кривой над полем  $\mathbb{F}_q$

$$E: \quad y^2 = x^3 + ax + b,$$

с законом сложения различных точек [4]

$$(x_1, y_1) + (x_2, y_2) = \left( \left( \frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2, -y_1 - \left( \frac{y_2 - y_1}{x_2 - x_1} \right) (x_3 - x_1) \right)$$

В проективных координатах с заменой  $x = \frac{X}{Z}, y = \frac{Y}{Z}$  имеем

$$\frac{\frac{Y_2}{Z_2} - \frac{Y_1}{Z_1}}{\frac{X_2}{Z_2} - \frac{X_1}{Z_1}} = \frac{u}{v}, \quad u = Y_2 Z_1 - Y_1 Z_2, \quad v = X_2 Z_1 - X_1 Z_2.$$

Тогда

$$\frac{X_3}{Z_3} = \left( \frac{u}{v} \right)^2 - \frac{X_1}{Z_1} - \frac{X_2}{Z_2} = \frac{Z_1 Z_2 u^2 - v^2 (X_1 Z_2 + X_2 Z_1)}{Z_1 Z_2 v^2} = \frac{vg}{Z_3},$$

где

$$Z_3 = Z_1 Z_2 v^3, \quad g = Z_1 Z_2 u^2 - v^3 - 2v^2 X_1 Z_2.$$

Далее

$$\frac{Y_3}{Z_3} = -\frac{Y_1}{Z_1} + \left( \frac{u}{v} \right) \left( \frac{X_1}{Z_1} - \frac{vg}{Z_1 Z_2 v^3} \right) = \frac{-Y_1 Z_2 v^3 + u(X_1 Z_2 v^2 - g)}{Z_1 Z_2 v^3}$$

Итак, имеем

$$\begin{aligned} X_3 &= vg, \\ Y_3 &= -Y_1 Z_2 v^3 + u(X_1 Z_2 v^2 - g), \\ Z_3 &= Z_1 Z_2 v^3. \end{aligned}$$

Расчет числа операций дает сложность вычисления суммы точек канонической кривой  $E$   $V_E = 12M + 2S$ . Аналогичный расчет для удвоения точек приводит к результату [4]  $W_E = 7M + 5S$ .

### Сравнение сложности вычислений для кривых $E_{ED}$ и $E$

Принимая вычислительную сложность возведения в квадрат  $1S = 0.67M$ , а умножения на параметр кривой  $1U = 0.5M$ , получим оценки сложности сложения и удвоения на кривой Эдвардса  $V_{ED} = 11.17M$ ,  $W_{ED} = 3M + 4S = 5.68M$ . Удвоение, как видим, практически вдвое быстрее сложения. Для канонической эллиптической кривой имеем  $V_E = 13.33M$ ,  $W_E = 10.35M$ . В среднем кривые Эдвардса обеспечивают выигрыш в производительности в  $\gamma = (V_E + W_E) / (V_{ED} + W_{ED}) = 1.41$  раза.

При вычислении скалярного произведения  $rQ$  точки  $Q$  число  $r$  представляется в двоичной форме, тогда работает алгоритм последовательного сложения-удвоения, а приведенный результат для  $\gamma$  справедлив при равновероятных 0 и 1 в числе  $r$ . Пусть  $v_0$  – относительная частота знаков 0 в двоичной последовательности  $r$ ,  $(1 - v_0)$  – относительная частота знаков 1, тогда в более общей форме выигрыш

$$\gamma = \frac{v_0 W_E + (1 - v_0) V_E}{v_0 W_{ED} + (1 - v_0) V_{ED}} = \frac{10.35v_0 + 13.33(1 - v_0)}{5.68v_0 + 11.17(1 - v_0)}.$$

При преобладании знаков 0 в числе  $r$ , например, со значением  $v_0 = 0.75$ , получаем выигрыш  $\gamma = 1.573$ . В пределе для числа  $r = 2^m$  максимальный выигрыш достигает значения  $\gamma_{\max} = 1.82$ . Это ясно, так как удвоение выполняется гораздо быстрее сложения точек. При преобладании единиц в последовательности  $r$  результат будет обратным. В частности, при  $r = 2^m - 1$  минимальный выигрыш равен  $\gamma_{\min} = 1.193$ . Заметим, что приведенные результаты относительно нижней границы  $\gamma$  в некоторой степени условны, так как мы приняли  $1U = 0.5M$ . В частных случаях параметр  $d$ , использующийся при вычислении сложения точек, может принимать малые значения, тогда величиной  $1U$  вообще можно пренебречь (при этом  $\gamma_{\min} = 1.249$ ).

В заключение резюмируем, что кривые Эдвардса имеют неоспоримые преимущества как перед каноническими эллиптическими кривыми, так и перед другими известными изоморфными формами кривых [5]. Главные из них – быстроедействие и удобство программирования. Хотя класс этих кривых приблизительно в 4 раза уже класса всех кривых, их применение в криптосистемах перспективно.

### Список литературы

1. Edwards H.M. A normal form for elliptic curves. Bulletin of the American Mathematical Society, Volume 44, Number 3, July 2007, Pages 393-422.
2. Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme under Contract IST-2002-507932 ECRYPT, 2007, PP. 1-20.
3. Bernstein Daniel J., Lange Tanja, Farashahi R.R. Binary Edwards Curves. IST Programme under Contract IST-2002-507932 ECRYPT, 2008, PP.1..23.
4. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых. Учеб. пособие. – К.: ИВЦ «Політехніка», 2004. – 224с.
5. Daniel J. Bernstein, Tanja Lange, Explicit-formulas database (2007). <http://explicitformulas.org> EFD.

Рецензент: Дудикевич В.Б.

Надійшла 9.06.2011

УДК 621.391

Кувшинов О.В., Жук О.Г., Бортнік Л.І., Толюпа С.В.  
(Військовий інститут телекомунікацій та інформатизації  
Національного технічного університету України „  
Київський політехнічний інститут”, ДУІКТ)

### НАПРЯМКИ ВДОСКОНАЛЕННЯ ТЕХНОЛОГІЇ OFDM ПРИ ВПЛИВІ НАВМИСНИХ ЗАВАД

В даний час технологія ортогонального частотного мультиплексування – OFDM (Orthogonal Frequency Division Multiplex) широко застосовується в мережах безпроводного доступу стандартів IEEE 802.11 та IEEE 802.16, системах цифрового радіомовлення T-DAB та DRM, цифрового телебачення DVB-T, xDSL-модемах тощо [1 – 5].

При формуванні OFDM-сигналу інформаційний потік зі швидкістю  $B$  ділиться на  $N$  паралельних підпотоків, швидкість кожного з яких в  $N$  разів менша ( $B/N$ ). Кожний з цих підпотоків модулює індивідуальну піднесучу, які ортогональні між собою. Спектри сигналів на індивідуальних несучих перекриваються, але завдяки ортогональності сигнали розділяються на прийомі без спотворень. Група несучих частот, яка в даний момент часу переносить біти паралельних цифрових потоків, називається символом OFDM. Для модуляції піднесучих застосовують КАМ-М ( $M$ -позиційну квадратурну амплітудну модуляцію) або ФМ-М ( $M$ -позиційну фазову модуляцію) [2].