ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ И СИГНАЛОВ

УДК 681.3

О ВЫБОРЕ НЕПРИВОДИМЫХ МНОГОЧЛЕНОВ ДЛЯ АЛГОРИТМА SEA

Бабенко М.Г., Червяков Н.И.

В статье проводится анализ алгоритма SEA для нахождения количества точек эллиптической кривой, заданной над простым полем. В случае, когда «простое число Аткина» предлагается для построения квадратичных полей, авторы рекомендуют использовать неприводимые двучлены, которые позволяют наиболее эффективно реализовать арифметические операции в квадратичном поле Галуа.

Ключевые слова: эллиптическая кривая, алгоритм SEA, модулярные многочлены, многочлены деления, квадратичные поля Галуа, неприводимые двучлены, примитивные элементы квадратичного поля Галуа.

Введение. Постановка задачи

Современные информационные системы требуют особого подхода к передаче электронных документов по открытым каналам связи. При этом возникает задача сохранения секретной информации в документе, которая решается с использованием асимметричных алгоритмов.

Эллиптические кривые – один из самых перспективных инструментов для построения криптографических алгоритмов [1]. Это обусловлено тем, что они обеспечивают максимально возможную для криптосистемы с открытым ключом стойкость на один бит размера задачи [2]. Эллиптическая кривая E, заданная уравнением в форме Вейерштрассе, имеет вид

$$E(F_p): y^2 = x^3 + ax + b\,, \qquad (1)$$

где p – простое число.

Одним из основных требований, предъявляемых к эллиптической кривой (1), является содержание большого простого числа в порядке группы точек. Соответствие этому требованию нельзя определить, не находя порядок группы. Одним из самых быстрых универсальных алгоритмов нахождения количества точек на эллиптической кривой над простым полем является алгоритм SEA.

Постановка задачи. Провести анализ алгоритма SEA и разработать эффективный метод нахождения образующего элемента в квадратичном поле Галуа и выбора двучленов для случая, когда в алгоритме SEA простое число является «простым числом Аткина».

Основная часть

Аткин [3] разработал алгоритм, вычисляющий порядок ϕ_l в $PGL_2(F_l)$, и показал возможности его использования для вычисления количества точек в $E(F_p)$. Элкис [4-5] разработал другой метод, заменяющий многочлен деления степени $\frac{l^2-1}{2}$ на множитель степени $l+1$ для простых чисел l.

Алгоритм, включающий в себя алгоритм Шуфа и модификации алгоритмов Аткина и Элкиса, называется алгоритмом SEA. В изложении алгоритма SEA используются модулярные многочлены из [6-7].

Определение 1. Классическим модулярным многочленом называется многочлен, вычисляемый по следующей формуле:

$$\Phi_l(X, j(\tau)) = \left(X - j(l\tau) \prod_{i=0}^{l-1} \left(X - j\left(\frac{-l}{\tau + i} \right) \right) \right),$$

где $j(\tau) = \frac{1728 E_4(\tau)^3}{E_4(\tau)^3 - E_6(\tau)^2} = \frac{1}{\tau} + 744 + 196884\tau ...$

$$E_4(\tau) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) \tau^n = 1 + 240\tau + 2160\tau^2 ...$$

$$E_6(\tau) = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) \tau^n = 1 - 504\tau - 16632\tau^2 ...,$$

$\sigma_k(n)$ – сумма k степеней делителей числа n.

Приведем пример классического модулярного многочлена при $l = 3$:

$$\begin{aligned}
&\Phi_3(X,Y) = X^4 - X^3Y^3 + Y^4 + \\
&+ 2232\left(X^3Y^2 + X^2Y^3\right) - 1069956\left(X^3Y + XY^3\right) \\
&+ 36864000\left(X^3 + Y^3\right) + 2587918086X^2Y^2 + \\
&+ 8900222976000\left(X^2Y + XY^2\right) + \\
&+ 452984832000000\left(X^2 + Y^2\right) - \\
&- 770845966336000000XY + \\
&1855425871872000000000\left(X + Y\right).
\end{aligned}$$

Аткин предложил использовать канонический модулярный многочлен.

Определение 2. Канонический модулярный многочлен обозначается $\Phi_l^c(X, j(r))$ и задается формулой $\Phi_l^c(X,j(\tau))=(X-f_l(\tau))\prod_{i=0}^{l-1}\left(X-f_l\left(\frac{-1}{\tau+i}\right)\right)$, где $f_l(\tau)=l^s\left(\frac{\eta(l\tau)}{\eta(\tau)}\right)^{2s}$, функция Дедекинда $\eta(\tau)=q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$, $s=\frac{12}{НОД\ (12,l-1)}$, $q=e^{2i\pi\tau}$.

Пример канонического многочлена для $l=5$:

$$\Phi_5^c(X,Y)=X^6+30X^5+315X^4+1300X^3+$$
$$+1575X^2+(-Y+750)X+125.$$

Алгоритм SEA основан на том, что простые числа разбиваются на два класса: «простые числа Аткина» и «простые числа Элкиса». Для разделения простых чисел на два указанных типа используют модулярные многочлены. Алгоритм SEA базируется на следующих утверждениях.

Утверждение 1 [3]. Пусть E – несупервырожденная эллиптическая кривая над F_p с инвариантом $j\neq 0{,}1728$. Пусть $\Phi_l(x,j)=h_1h_2...h_s$ есть разложения многочлена $\Phi_l(x,j(E))\in F_p[x]$ в виде произведения неприводимых многочленов. Тогда значения степеней $h_1,h_2,h_3,...,h_s$ могут быть следующими:

1. $(1,1...1)$ или $(1,l)$ – в обоих случаях имеем $t^2-4p\equiv 0(\mathrm{mod}\,l)$. В первом случае $\tau=1$, а во втором $-\tau=l$;
2. $(1,1,r,r,r...r)$ – в этом случае t^2-4p есть квадратный вычет по модулю l и r делит $l-1$;
3. $(r,r,r,r,r...r)$ – в этом случае t^2-4p не является квадратичным вычетом по модулю l, r делит $l+1$, отображение ϕ действует на $E[l]$ и удовлетворяет неприводимому на F_l многочлену $F_l=\phi^2-t_l\phi+p_l$, где $t_l\equiv t(\mathrm{mod}\,l)$, $p_i\equiv p(\mathrm{mod}\,l)$.

Для определения типа разложения необходимо вычислить значение $w=НОД(x^p-x,\Phi(x,j))$, w может принимать значения 0, 1, 2 или $l+1$. Если $\deg(w)$, то l – «простое число Аткина», в остальных случаях – «простое число Элкиса».

Если l является «простым Аткина», многочлен имеет два корня $\lambda,\mu\in F_{l^2}/F_l$. Тогда элемент $\frac{\lambda}{\mu}=\gamma$ поля F_{l^2} имеет порядок r, где r – степень неприводимых многочленов, полученных в результате разложения $\Phi_l(x,j)$. Первоначально вычислим образующий элемент g группы F_{l^2}. $\frac{i(l^2-1)}{r}$

Можно найти все $\gamma_r=g^{\ r}$, для которых $i\in\{1...r-1\}$ и числа i и r взаимно просты. Перечисляя все возможные γ_r, можно определить набор T возможных значений $t\,\mathrm{mod}\,l$, решив систему уравнений:

$$\begin{cases}\frac{\lambda}{\mu}=\gamma_r,\\ t=\lambda+\mu(\mathrm{mod}\,l),\\ p\equiv\lambda\mu(\mathrm{mod}\,l).\end{cases}$$

Число r может быть вычислено как наименьшее $i>1$, для которого выполняется следующее равенство: $\Phi_l(x,j)\,|\,x^{p^i}-x$.

Причем достаточно проверить $i\,|\,(l+1)$ и удовлетворяющее равенству $(-1)^{\frac{l+1}{i}}=\left(\frac{p}{l}\right)$.

В случае, если l – «простое Элкиса», то многочлен F_l имеет два корня λ, μ, которые являются собственными значениями эндоморфизма Фробениуса по модулю l. Если $\lambda=\mu$, то это случай второго этапа алгоритма Шуфа. Если $\lambda\neq\mu$, то нужно построить многочлен вида

$$F_l(x)=\prod_{\pm P\in C_1\setminus\{u\}}(x-(P)_x),$$

где $(P)_x-x$ координата точки P.

Его строят с помощью следующих фактов. Существуют ненулевые точки $P_1,P_2\in E[l]$, такие, что $\phi_p(P_1)=[\lambda]P$ и $\phi_p(P_2)=[\mu]P$. Пусть $C_1=\langle P_1\rangle$, $C_2=\langle P_2\rangle$ и $C_1\neq C_2$, где $C\langle P\rangle$ – циклическая подгруппа точек порядка l, такая, что $\phi(C)=C$; $\deg(F_l(x))=\frac{l-1}{2}$, а алгоритм построения многочлена приведен в [6].

Для нахождения $t(\mathrm{mod}\,l)$ с помощью метода, описанного в алгоритме Шуфа, достаточно вычислить только значения λ, удовлетворяющего уравнению $\phi_p(P)=[\lambda]P$, где $P=(x,y)\in C_1\setminus\{O\}$. Значение λ единственно, так как l – простое. Для такой точки P мы имеем $x^p=x-\frac{\psi_{\lambda-1}\psi_{\lambda+1}}{\psi_\lambda^2}$, где ψ_i – i-ый многочлен деления.

Пусть $h=\psi_\lambda^2(x^p-x)+\psi_{\lambda-1}\psi_{\lambda+1}$, приводя данный многочлен к виду $x-h_x$, заменяя переменную y выражения для рассматриваемой эллиптической кривой, необходимо найти такое значение λ, чтобы $НОД(h_x,F_l)\neq 1$. Тогда $t=\lambda+\frac{p}{\lambda}\,\mathrm{mod}\,l$.

Важно отметить, что в случае, если l – «простое Элкиса», мы получаем одно значение $t\,\mathrm{mod}\,l$, а если l – «простое Аткина», то множество воз-

можных значений $t \bmod l$. Для вычисления значения t используются методы, предложенные Аткиным [8], Же-Лерсье [9], и их модификации, приведенные в [10].

Преимущество обеспечивается за счет использования многочленов степени $\frac{l-1}{2}$, если l – «простое Элкиса» и $l+1$, если l – «простое Аткина», вместо используемых в алгоритме Шуфа многочленов степени $\frac{l^2-1}{2}$, таким образом, сложность алгоритма SEA составляет $O\left(\log_2^6 p\right)$.

Алгоритм 1. Алгоритм SEA вычисления количества точек эллиптической кривой, заданной над F_p.

Вход. Простое число p и $E\left(F_p\right)$.

Выход. N – количество точек эллиптической кривой $E\left(F_n\right)$.

1. $M=1$, $l=2$, $A=\{\}$, $El=\{\}$.

2. Если $M>4\sqrt{p}$, то перейти к шагу 15.

3. Если $\deg\left(НОД\left(x^p-x,\Phi_l(x,j)\right)\neq 0\right)$, то перейти к шагу 9.

4. Вычислить степень r для случая 3 утверждения.

5. Вычислить образующий элемент g группы $F_{l^2}^*$.

6. $S=\left\{\gamma_r=g^{\frac{i\left(l^2-1\right)}{r}} \mid НОД(i,r)=1\right\}$.

7. Для каждого $\gamma_i \in S$:

7.1. Решить систему уравнений:

$$\begin{cases}\dfrac{\lambda}{\mu}=\gamma_i,\\ t=\lambda+\mu\left(\bmod l\right),\\ p=\lambda\mu\left(\bmod l\right).\end{cases}$$

7.2. $A=A\cup(t,l)$.

8. Перейти к шагу 12.

9. Вычислить многочлен $F_l(x)$.

10. Вычислить λ такое, что $НОД\left(\psi_\lambda^2\left(x^p-x\right)+\psi_{\lambda-1}\psi_{\lambda+1},F_l\right)\neq 1$.

11. Вычислить $t=\lambda+\frac{p}{\lambda}\bmod l$, $EL=El\cup(t,l)$.

12. $M=l\ M$.

13. Сгенерировать следующее простое число.

14. Перейти к шагу 2.

15. Вычислить t – след эндоморфизма Фробениуса.

16. Вернуть $p+1-t$.

Пример. Пусть t – след эндоморфизма Фробениуса для эллиптической кривой $E\left(F_7\right): y^2=x^3+2x+6$. Найти:

1. $t \bmod 3$;

2. $t \bmod 5$.

Решение.

Вычислим $j(E)$:

$$j(E)=1728\frac{4\cdot 2^3}{4\cdot 2^3+27\cdot 6^2}=1728\frac{4}{4+27}=1728\frac{4}{3}=1.$$

1. Для модуля 3 используем классический модулярный многочлен $\Phi_3(X,Y)$:

$$\Phi_3(X,1)=X^4-X^3+1+2232\left(X^3+X^2\right)-$$
$$1069956\left(X^3+X\right)+36864000\left(X^3+1\right)+$$
$$+2587918086X^2+8900222976000\left(X^2+X\right)+$$
$$452984832000000\left(X^2+1\right)-$$
$$770845966336000000X+$$
$$1855425871872000000000(X+1)=$$
$$=X^4+35796275X^3+461887642896318X^2$$
$$+1854655034805885906044X+$$
$$+1855426324856868864001.$$

Так как $НОД\left(x^7-x,\Phi_3(X,1)\right)=1$, то $l=3$ является «простым Аткина».

Вычисляем степень r для случая 3 утверждения.

Так как i должно удовлетворять трем условиям:

1. $(-1)^{\frac{4}{i}}=\left(\frac{1}{3}\right)$,

2. $i \mid 4$,

3. $i>1$,

то может быть равно только $i=2$.

Проверим $\Phi_3(X,1) \mid x^{49}-x$, для этого достаточно вычислить $\left(x^{49}-x\right)\bmod\Phi_3(x,1)$.

Получим $\left(x^{49}-x\right)\bmod\Phi_3(x,1)=0$ и $r=2$, где $\Phi_3(X,1)$ представляется в виде $\Phi_3(X,1)=(X^2+2X+2)(X^2+2X+3)$.

Для построения $F_{7^2}^*$ воспользуемся неприводимым многочленом x^2+1. Обратим внимание на свойство квадратичного поля Галуа:

$$(ax+b)^8=(ax+b)^{7+1}=(ax+b)^7(ax+b)=$$
$$\left(ax^7+b\right)(ax+b)=a^2x^8+abx^7+abx+b^2=a^2+b.^2$$

Так как $5\in F_7^*$ является образующим элементом в F_7^* и $5=1^2+2^2$, то проверим, является ли элемент $x+2\in F_{7^2}^*$ образующим элементом $F_{7^2}^*$,

для этого проверим следующие два условия: $(x+2)^{16} \neq 1$ и $(x+2)^{24} \neq 1$.

$$(x+2)^{16} = \left((x+2)^8\right)^2 = 5^2 = 4 \neq 1,$$
$$(x+2)^{24} = \left((x+2)^8\right)^3 = 5^3 = 6 \neq 1,$$

значит, $(x+2) \in F_{7^2}^*$ – образующий элемент, $g = x+2$.

Так как i может быть равно только $i=1$, то решим систему

$$\begin{cases} \dfrac{\lambda}{\mu} = g^{24}, \\ \lambda\mu = 1 (\bmod 3), \\ t = \lambda + \mu (\bmod 3); \end{cases} \Leftrightarrow \begin{cases} \dfrac{\lambda^2}{\lambda\mu} = g^{24}, \\ \lambda\mu = 1 (\bmod 3), \\ t = \lambda + \mu (\bmod 3); \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} \lambda^2 = g^{24}, \\ \lambda\mu = 1 (\bmod 3), \\ t = \lambda + \mu (\bmod 3); \end{cases} \Leftrightarrow \left[\begin{array}{l} \begin{cases} \lambda = g^{12}, \\ \lambda\mu = 1 (\bmod 3), \\ t = \lambda + \mu (\bmod 3); \end{cases} \\ \begin{cases} \lambda = -g^{12}, \\ \lambda\mu = 1 (\bmod 3), \\ t = \lambda + \mu (\bmod 3). \end{cases} \end{array}\right.$$

Вычислим

$$g^{12} = g^8 g^4 = 5(x+2)^4 = 5\left((x+2)^2\right)^2 =$$
$$5\left(x^2+4x+4\right)^2 = 5(4x+3)^2 = 5\left(16x^2+24x+9\right) = x.$$

Получим, что

$$\left[\begin{array}{l} \begin{cases} \lambda = g^{12}, \\ \lambda\mu = 1 (\bmod 3), \\ t = \lambda + \mu (\bmod 3); \end{cases} \\ \begin{cases} \lambda = -g^{12}, \\ \lambda\mu = 1 (\bmod 3), \\ t = \lambda + \mu (\bmod 3); \end{cases} \end{array}\right. \Leftrightarrow \left[\begin{array}{l} \begin{cases} \lambda = x, \\ \lambda\mu = 1 (\bmod 3), \\ t = \lambda + \mu (\bmod 3); \end{cases} \\ \begin{cases} \lambda = -x, \\ \lambda\mu = 1 (\bmod 3), \\ t = \lambda + \mu (\bmod 3); \end{cases} \end{array}\right. \Leftrightarrow$$

$$\Leftrightarrow \left[\begin{array}{l} \begin{cases} \lambda = x, \\ \mu = -x (\bmod\ 3), \\ t = 0 (\bmod\ 3); \end{cases} \\ \begin{cases} \lambda = -x, \\ \mu = x (\bmod\ 3), \\ t = 0 (\bmod\ 3), \end{cases} \end{array}\right.$$

значит, $t \bmod 3 = 0$.

Найдем $t \bmod 5$, для этого воспользуемся каноническим многочленом:

$$\Phi_5^c(X,Y) = X^6 + 30X^5 + 315X^4 + 1300X^3 + $$
$$+ 1575X^2 + (-Y + 750)X + 125.$$

Вычислим $\Phi_5^c(X,1)$:

$$\Phi_5^c(X,1) = X^6 + 30X^5 + 315X^4 + 1300X^3 + $$
$$+ 1575X^2 + 749X + 125.$$

Так как $НОД\left(x^7 - x, \Phi_5^c(X,1)\right) = X^2 + 6$, то $l = 5$ – «простое число Элкиса». Заметим, что

$$\Phi_5^c(X,1) = (X+1)(X+6)\left(X^4 + 2X^3 + X^2 + 1\right).$$

Вычислим многочлен $F_5(x) = x^2 + x$:

$$НОД\left(\psi_\lambda^2\left(x^p - x\right) + \psi_{\lambda-1}\psi_{\lambda+1}, F_l\right) \neq 1.$$

При $\lambda = \{1,2,3\}$, тогда

$$НОД\left(\psi_\lambda^2\left(x^p - x\right) + \psi_{\lambda-1}\psi_{\lambda+1}, F_l\right) = 1.$$

При $\lambda = 4$ получим

$$НОД\left(\psi_\lambda^2\left(x^p - x\right) + \psi_{\lambda-1}\psi_{\lambda+1}, F_l\right) = x^2 + x,$$

следовательно, $\lambda = 4$. Найдем

$$t \bmod 5 = 4 + \frac{2}{4} \bmod 5 = 4 + \frac{1}{2} \bmod 5 =$$
$$= 4 + 3 \bmod 5 = 2.$$

В случае, когда l – «простое Аткина», нужно строить квадратичные поля Галуа. Удобно использовать квадратичные поля Галуа, построенные на неприводимых двучленах $x^2 + \alpha$ в $F_p[x]$. Для них справедливо следующее утверждение.

Утверждение 2. Пусть

$$(ax+b) \in F_{p^2}^* = \left\{ ax+b \mid x^2 + \alpha = 0, a, b, \alpha \in F_p \right\},$$

где p – простое число и $(p-a)$ – квадратичный невычет в F_p^*, тогда $(ax+b)^{p+1} = a^2\alpha + b^2$.

Доказательство. Так как $(a+b)^p = a^p + b^p$,

$$(ax+b)^{p+1} = (ax+b)^p (ax+b) =$$
$$= \left(ax^p + b\right)(ax+b) = a^2 x^{p+1} + ab\left(x^p + x\right) + b^2.$$

Так как $(p-\alpha)$ – квадратичный невычет в F_p^*, то из свойств символа Лежандра следует, что $(p-\alpha)^{\frac{p-1}{2}} = -1$.

Значит, $x^{p-1} = \left(x^2\right)^{\frac{p-1}{2}} = (p-\alpha)^{\frac{p-1}{2}} = -1$, подставив вместо x^{p-1} значение -1, получим: $a^2 x^{p+1} + ab\left(x^p + x\right) + b^2 = -a^2 x^2 + b^2 = a^2\alpha + b^2$.

Утверждение доказано. Из него следует, что $(ax+b)^{p+1} \in F_p$.

Для вычислений удобно использовать следующие квадратичные поля Галуа.

1. Если $p \bmod 4 = 3$, то неприводим многочлен в x^2+1 в $F_p[x]$ и для любого элемента

$$(ax+b) \in F^*_{p^2} = \left\{ ax+b \mid x^2+1=0, a,b \in F_p \right\}$$

выполняется соотношение $(ax+b)^{p+1} = a^2+b^2$.

2. Если $p \bmod 8 = 5$, то неприводим многочлен x^2+2 в $F_p[x]$ и для любого элемента

$$(ax+b) \in F^*_{p^2} = \left\{ ax+b \mid x^2+2=0, a,b \in F_p \right\}$$

выполняется соотношение $(ax+b)^{p+1} = 2a^2+b^2$.

3. Если $p \bmod 6 = 5$, то неприводим многочлен x^2+3 в $F_p[x]$ и для любого элемента

$$(ax+b) \in F^*_{p^2} = \left\{ ax+b \mid x^2+3=0, a,b \in F_p \right\}$$

выполняется соотношение

$$(ax+b)^{p+1} = 3a^2+b^2,$$

и для нахождения образующего элемента $g \in F^*_{l^2}$ справедливо следующее утверждение.

Утверждение 3. Если образующий элемент $g \in F^*_{p^2} = \left\{ ax+b \mid x^2+\alpha=0, a,b \in F_p \right\}$ и $\gamma = g^{p+1}$, где p – простое число, а $(p-\alpha)$ – квадратичный невычет в F^*_p, то γ – образующий элемент в F^*_p.

Утверждение 4. Элемент $g \in F^*_{p^2} = \left\{ ax+b \mid x^2+\alpha=0, a,b \in F_p \right\}$, где p – простое число и $(p-\alpha)$ – квадратичный невычет в F^*_p, является образующим элементом в $F^*_{p^2}$, если выполняются следующие два условия:

1. Элемент $\gamma = g^{p+1} \in F_p$ – образующий элемент в F^*_p;

2. Для всех $t \mid (p+1)$ и $t < p+1$ выполняется $g^{2t} \notin F_p$.

Доказательства. Необходимость следует из утверждения 3. Докажем достаточность. Пусть $p-1 = 2^{n_0} p_1^{n_1} p_2^{n_2} \cdot \ldots \cdot p_{s-1}^{n_{s-1}}$ и $p+1 = 2^{n_s} p_{s+1}^{n_{s+1}} p_{s+2}^{n_{s+2}} \cdot \ldots \cdot p_{s+m}^{n_{s+m}}$, где $n_0, n_s \geq 1$ и p_i – попарно различные простые числа.

Для доказательства утверждения достаточно доказать, что выполняются следующие соотношения:

$$g^{\frac{p^2-1}{2}} \neq 1, \quad g^{\frac{p^2-1}{p_i}} \neq 1 \qquad (2)$$

для всех $i = 1 \ldots s+m$. Вычислим $g^{\frac{p^2-1}{2}}$, получим $g^{\frac{p^2-1}{2}} = \left(g^{p+1}\right)^{\frac{p-1}{2}} = \gamma^{\frac{p+1}{2}} = -1 \neq 1$, так как γ – образующий элемент в F^*_p.

Пусть i принимает одно из значений в отрезке $[1 \ldots s-1]$, тогда

$$g^{\frac{p^2-1}{p_i}} = \left(g^{p+1}\right)^{\frac{p-1}{p_i}} = \gamma^{\frac{p-1}{p_i}} \neq 1,$$

так как γ – образующий элемент в F^*_p.

Пусть i принимает одно из значений в отрезке $[s+1 \ldots s+m]$, тогда

$$g^{\frac{p^2-1}{p_i}} = \left(g^{p-1}\right)^{\frac{p+1}{p_i}} = \left(\frac{g^{p+1}}{g^2}\right)^{\frac{p+1}{p_i}} =$$

$$= \left(\frac{\gamma}{g^2}\right)^{\frac{p+1}{p_i}} = \gamma g^{-2\frac{p+1}{p_i}},$$

откуда следует

$$g^{2\frac{p+1}{p_i}} \notin F_p,$$

значит, $g^{\frac{p^2-1}{p_i}} \neq 1$.

Показано, что выполняются условия (2), утверждение доказано. Использование простых чисел специального вида позволяет упростить условия утверждения 4.

Следствие. Элемент

$$g \in F^*_{p^2} = \left\{ ax+b \mid x^2+\alpha=0, a,b \in F_p \right\},$$

где p – простое число вида $p = 4k+1$ и $q = 2k+1$ – простое число, $(p-\alpha)$ – квадратичный невычет в F^*_p, является образующим элементом в $F^*_{p^2}$, если $\gamma = g^{p+1}$ – образующий элемент в F^*_p, и $g^4 \notin F^*_p$.

Доказательство. Выполняется первое условие утверждения 4. Покажем, что выполняется и второе условие: так как $(p+1) = 2(2k+1)$ и $g^4 \notin F^*_p$.

Следствие доказано.

Числами, удовлетворяющими условию следствия и меньшими ста, являются 5, 13, 37, 61, 73.

Предложим метод нахождения образующего элемента в $F^*_{p^2}$ на базе утверждения 4.

Метод. Нахождение образующего элемента $g \in F^*_{p^2}$ производится следующим образом.

1. Находим образующий элемент $\gamma \in F^*_p$.

2. Находим пару (a,b), удовлетворяющую условию $\gamma = a^2\alpha + b^2$.

2.1. Для найденной пары (a,b) и всех значений p_i проверяем: если $(ax+b)^{2\frac{p+1}{p_i}} \in F^*_p$, то переходим на шаг 2 к поиску следующей подходящей пары, где $p+1 = 2^{n_0} p_1^{n_1} p_2^{n_2} \cdot \ldots \cdot p_s^{n_s}$.

3. Возвращаем элемент (a,b).

Выводы

В статье проведен анализ алгоритма SEA для нахождения количества точек эллиптической кривой, заданной над простым полем. В случае, когда простое число является «простым числом Аткина», предложено для построения квадратичных полей использовать неприводимые двучлены. Для ускорения операций в квадратичном поле Галуа доказан ряд утверждений. Предложен метод нахождения образующих элементов в квадратичном поле Галуа.

Литература

1. Menezes A., van Oorchot P., Vanstone S. Handbook of applied cryptography. CRC Press, 1997. – 816 p.
2. Ростовцев А. Г., Маховенко Е. Б. Два подхода к логарифмированию на эллиптической кривой. http://www.ssl.stu.neva.ru/ssl/archieve/lift1.pdf
3. Atkin A.O.L., Morain F., Elliptic curves and primality proving // Math. Comp. 61, 203, 1993. – P. 339-405.
4. Elkies N.D. Elliptic and modular curves over finite fields and related computaional issues // Computational perspectives in number theory: Proc. of a Conf. in Honor of A.O. L.Atkin, J. T. Teitelbaum and D.A.Buell, editors. 1998. – P. 21-76.
5. Elkies N.D. Explicit isogenies, manuscript // Boston, MA, 1992.
6. Csirik J. A. An exposition of the SEA algorithm // Preprint, 2000. www.csirik.net/sch-survey.pdf
7. Menezes A., van Oorchot P., Vanstone S. Handbook of applied cryptography. CRC press, 1997. – 816 p.
8. Blake I.F., Seroussi G., Smart N.P. Elliptic curves in cryptography. Cambridge Univ. Press, 1999. – 228 p.
9. Joux A, Lercier R. «Chinese&Match», an alternative to Atkin's «Match and Sort» method used in the SEA algorithm // Mathematics of Computation. 70(234), 2001. – P. 827-836.
10. Василенко О.Н. К вопросу о вычислении порядка группы точек эллиптической кривой над конечным простым полем // Труды по дискретной математике. Вып. 9. М.: Гелиос АРВ, 2006. – С. 32-50.

ABOUT THE CHOICE OF THE IRREDUCIBLE POLYNOMIALS FOR THE SEA ALGORITHM

Babenko M.G., Chervaykov N.I.

The SEA algorithm for finding the number of points of an elliptic curve defined over a prime field is analyzed in the article. In the case of «prime Atkin» is proposed to construct quadratic fields, the authors recommend the use of irreducible binomials, which allow the most efficient to implement arithmetic in quadratic Galois field.

Keywords: *elliptic curve, algorithm SEA, modular polynomials, polynomials division, quadratic Galois field, irreducible binomials, primitive elements of a quadratic Galois field.*

Бабенко Михаил Григорьевич, аспирант Кафедры «Высшая алгебра и геометрия» Ставропольского государственного университета (СГУ). Тел (8-8652) 38-80-84. E-mail: whbear@yandex.ru

Червяков Николай Иванович, д.т.н., профессор, заведующий Кафедрой «Прикладная математика и информатика» СГУ. Тел. (8-8652) 35-68-32, доб. 1154; 8 (8652) 35-48-61.

Поздравляем!

Всех авторов, издателей и читателей журнала ИКТ с наступающим Новым Годом! Пусть сбудутся ваши заветные мечты и желания, а в год Кролика, знаменующего творческую плодовитость и неиссякаемую внутреннюю энергию, пусть хватит времени, здоровья и сил, чтобы воплотить их в жизнь. Ждем от вас содержательных научно-информационных материалов, которые мы будем рады публиковать на страницах ИКТ.

Еще раз с Новым, 2011 Годом и удачи во всем!

Редакционный совет и редколлегия журнала ИКТ