УДК 681.3.06:519.248.681

*А. А. ПОЛЯКОВ*

# МЕТОД НАХОЖДЕНИЯ СЛУЧАЙНОЙ КРИПТОГРАФИЧЕСКИ СТОЙКОЙ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ НА РАСШИРЕННЫХ ПОЛЯХ ХАРАКТЕРИСТИКИ 2

Безопасность криптосистем, использующих группу точек эллиптической кривой, по сегодняшним взглядам, существенно зависит от сложности решения задачи эллиптического дискретного логарифма. Основными алгоритмами решения задачи дискретного логарифма в абелевых группах являются алгоритм Шанкса «больших и маленьких шагов», $\rho$-метод Полларда [1], алгоритм Полинга-Хелмана [2]. Для защиты от этой атаки необходимо выбирать группу, порядок которой кратен большому простому числу.

Известно, что существует множество слабых кривых, имеющих особые свойства, прежде всего это – суперсингулярные и аномальные кривые. На такие кривые известна атака Menezes-Okamoto-Vanstone (MOV),позволяющая перевести задачу эллиптического дискретного логарифма в задачу дискретного логарифма в мультипликативном поле $F_{q^B}$.

Учитывая требования по уровню прочности, предложенные в стандартах, рекомендуется, чтобы эллиптическая кривая была случайной, т.е. ее параметры были сгенерированы случайным образом. Случайная кривая, порядок которой делится на простое число как минимум длиной 160 бит, обеспечивает безопасность, сопоставимую с симметричными системами с длиной ключа 80 бит или системой RSA с длиной ключа 1024 бита. Эллиптические кривые, соответствующие данному требованию, а также требованию MOV ($B \geq 25$) и аномальности ($\# E \neq q$), будем называть криптографически стойкими. Для случайной кривой вероятность того, что будет сгенерирована слабая кривая, относительно мала. В приложениях, требующих более высокий уровень безопасности, необходимо увеличивать длину модуля преобразования.

В данной работе приведены и проанализированы основные методы вычисления порядка случайной эллиптической кривой (алгоритмы Сато и SEA). Ставится задача нахождения случайных криптографически стойких кривых, имеющих порядок эллиптической кривой, кратный 2 или 4.

Напомним основные сведения об эллиптических кривых на расширенном поле.

Эллиптическая кривая $E$ с ненулевыми $j$-инвариантами на расширенном поле $F_q$, где $q = 2^m$, задается в следующем виде [6-7]:

$$E : y^2 + xy = x^3 + ax^2 + b, \text{ где } b \in F_q^*,$$

где $a$ – некоторый фиксированный элемент из поля $F_q$ следа 1.

$j$-инвариант, определяющий изоморфные кривые, вычисляется $j(E) = 1/b$. Следует заметить, что данные кривые несуперсингулярные и также необходимо выполнение следующего дополнительного условия: $j(E) \notin F_{2^2}$.

Множество точек кривой $E(F_q)$, описывающее абелевую группу, определяется как:

$$E(F_{2^m}) = \{(x, y) \in F_q \mid E\} \cup (O_E),$$

где $O_E$ – точка бесконечности.

Эндоморфизм Фробениуса $\phi$ и мультипликативный эндоморфизм на кривой $E$ определяются следующими отображениями точек:

$$\phi : E(\mathrm{F}_q) \to E(\mathrm{F}_q), \quad (x,y) \mapsto (x^q, y^q), \quad \text{и} \quad [m] : E(\mathrm{F}_q) \to E(\mathrm{F}_q), \quad (x,y) \mapsto m(x,y).$$

Характеристическое уравнение эндоморфизма Фробениуса на эллиптической кривой имеет вид:

$$\phi^2 - t\phi + q = 0.$$

По теореме Хассе число точек кривой $E$ ограничено и равно:

$$u = q + 1 - t, \text{ где } |t| \le 2\sqrt{q},$$

где $t$ – след эндоморфизма Фробениуса на кривой $E$.

Заметим, что на кривой $E$ всегда существует точка $(0, \sqrt{b})$ порядка 2 и, следовательно, порядок кривой кратен 2, $2 \mid u$. Если на кривой существует точка $(\sqrt[4]{b}, \sqrt{b})$ порядка 4, то соответствующий порядок кривой будет кратен 4.

Маленький автоморфизм Фробениуса $\sigma$ задает отображение $x \mapsto x^2$, которое может быть расширено для изогении кривой $E$, сопряженной кривой $E^\sigma : y^2 + xy = x^3 + b^2$, следовательно:

$$\sigma : E(\mathrm{F}_q) \to E^\sigma(\mathrm{F}_q), \quad (x,y) \mapsto (x^2, y^2).$$

**1 Основные методы вычисления порядка случайной эллиптической кривой на поле $\mathrm{F}_q$**

К основным методам вычисления порядка случайной эллиптической кривой необходимо отнести полиномиальные методы Скуфа, SEA, Сато.

В 1985 году Скуф [8] предложил первый полиномиальный алгоритм, основанный на эндоморфизме Фробениуса $\phi$ в подгруппах точек $\ell$-кручения. Данный алгоритм позволяет вычислить количество точек на эллиптической кривой $E$ на конечном поле $\mathrm{F}_q$.

Аткин и Елкис [9] предложили некоторые уточнения по использованию сомножителей *полиномов деления,* полученных из вычисления некоторых *изогений* на поле характеристики $char(\mathrm{F}_q) > 3$. Лерсье и Ковергенц [10] построили эллиптические кривые на расширенных полях малой характеристики и получили изогении для характеристики $char(\mathrm{F}_q) = 2$ и 3.

Совокупность данных исследований позволила вычислить порядок эллиптической кривой на простом поле $\mathrm{F}_p$, где $p = 10^{499} + 15$, и на расширенном поле $\mathrm{F}_{2^{1999}}$, используя алгоритм Schoof-Atkin-Elkies (SEA)[11].

Основной идеей алгоритма Скуфа является нахождение следа кривой по модулю маленьких простых чисел $\ell$, используя свойства эндоморфизма Фробениуса $\phi$ в точках $\ell$-кручения на кривой $E$.

Обозначим $\bar{\phi}$ сокращение $\phi$ в некоторой подгруппе $E[\ell]$ точек $\ell$-кручения на кривой $E$. В результате получаем уравнение:

$$\bar{\phi}^2 - [t \bmod \ell^n]\phi + [q \bmod \ell^n] = 0.$$

Находим значение $\tau$. Для этого выполняем поиск по всем значениям $\tau$ из интервала $[0, \ell-1]$, удовлетворяющее тождеству $[\tau]\bar{\phi} \equiv \bar{\phi}^2 + [q \bmod \ell]$.

Согласно следствию из теоремы Хассе, что порядок кривой ограничен $|t| \le 2\sqrt{q}$, достаточно подсчитать значения $t$ по модулю $\ell_i$, где количество маленьких простых чисел $\ell_i$ ограничено следующим уравнением:

$$\prod \ell_i > 4\sqrt{q}.$$

Используя остатки $\tau_i$, можно вычислить значение следа Фробениуса $t$, воспользовавшись китайской теоремой об остатках, и тем самым получить порядок кривой.

Для вычисления точки $[q](X,Y)$ необходимо найти многочлены деления $f_\ell(X)$ степени $O(\ell^2)$. Решение этой задачи, а также вычисление значений $X^q$ и $Y^q$ составляют основную вычислительную сложность метода Скуфа. Все вычисления выполняются в кольце $F[X,Y]/(f_\ell(X),E)$. При этом размер элементов поля равняется $\ell^2 \log q$. Вычислительная сложность метода Скуфа с использованием быстрой арифметики равна $O(\log^{5+\tau} q)$ и с обычной арифметикой – $O(\log^8 q)$. Использование данного алгоритма при значениях простого $\ell$, большего 61, является неэффективным, потому что требует больших вычислительных затрат.

В основе алгоритма SEA [9, 11, 12] лежит базовый алгоритм Скуфа. Отличие алгоритма SEA заключается в том, что Аткин и Елкиес попытались уменьшить степени многочленов деления $f_\ell(X)$, используя только некоторый сомножитель степени $\frac{\ell-1}{2}$. Они рассмотрели подгруппу $E[\ell]$, образованную двумя точками $P$ и $Q$, содержащую $\ell+1$ подгрупп. В этом случае изогении I описывают мультипликативный эндоморфизм $[\ell]$, который представлен следующей диаграммой:

$$\begin{tikzcd} E \arrow[rr, "[\ell]"] \arrow[dr, "\mathrm{I}_j"'] & & E \\ & E/C_j \arrow[ur, "\hat{\mathrm{I}}_j"'] & \end{tikzcd}$$

Следовательно,

$$\mathrm{Ker}(\mathrm{I}_j) \subset \mathrm{Ker}([\ell]),$$

где $\#\mathrm{Ker}(\mathrm{I}_j) = \ell$.

Построив изогении $\mathrm{I}_j$ и $\hat{\mathrm{I}}_j$, можно вычислить сомножитель $h(X)$ многочлена деления $f_\ell(X)$. Использование модулярного уравнения $\Phi_\ell(j(E_\ell), j(E)) = 0$ позволяет эффективным образом определять существование изогении I .

Как и в алгоритме Скуфа, вычисления производятся в кольце $F[X,Y]/(h_\ell(X),E)$ при использовании полинома $h_\ell(X)$ степени $\frac{\ell-1}{2}$. Поэтому вычислительная сложность алгоритма SEA меньше за счет использования полиномов степени $O(\ell)$ и равна $\log^5 p$.

Например: используя алгоритм SEA, Морейн смог вычислить порядок кривой, определенной на простом поле размера $10^{499} + 153$ [10].

*Алгоритм Сато* [13,14] коренным образом отличается от алгоритмов SEA и Скуфа и реализуется двумя этапами. Первый этап – поднятие цикла изогений и коэффициентов кривых на $\mathbf{Z}_q$ с требуемой точностью, второй – вычисление следа эндоморфизма Фробениуса. Алгоритм Сато имеет следующий вид:

**Задано:** Эллиптическая кривая $E$, определенная на поле $\mathrm{F}_q$, $j$-инвариант, который удовлетворяет условию $j \notin \mathrm{F}_{p^2}$.

**Получаем:** След эндоморфизма Фробениуса на эллиптической кривой $E$. При этом выполняется:

1. Поднятие $j$-инвариантов, коэффициентов кривых и их подгрупп $p$-кручения, при этом предварительно вичислив цикл $d$ кривых $E_i$ и их $j$-инвариантов $j_i$;
2. Подсчет следа на $\mathbf{Z}_q$.

Рассматривая маленький эндоморфизм Фробениуса $\sigma$ в поле $\mathrm{F}_q$, строятся циклы $j$-инвариантов.

При использовании многомерной итерации Ньютона производится их одновременное поднятие. Таким образом, не вычисляя эндоморфизма Фробениуса $\Sigma$ в $\mathbf{Z}_q$, можно получить сопряженные $j$-инварианты $J$ в $\mathbf{Z}_q$. Поднимаются коэффициенты кривых, используя одномерную итерацию Ньютона, последовательно поднимаются сами кривые.

Изогении $\hat{\sigma}_i$ и $\hat{\Sigma}_i$ сепарабельны в степени $p$, они определяются своим ядром порядка $p$. Следовательно, поднятие $\hat{\sigma}_i$ к $\hat{\Sigma}_i$ осуществляется поднятием их ядра, которое является подгруппой $p$-кручения.

Можно поднимать каждую подгруппу $p$-кручения или поднимать единственную точку, используя итерацию Ньютона, когда $p=2$ и $p=3$. В случае характеристики $p \geq 5$ необходимо поднимать коэффициент многочлена $p$-деления с помощью поднятия Хэнселя. Схематично первый этап можно представить следующим образом:

**Задано:** Цикл эллиптических кривых $E_i$, определенных на поле $\mathrm{F}_q$.

**Получаем:** Цикл эллиптических кривых $\mathbf{Z}_q : \mathrm{E} \to \mathrm{E}_1 \to \ldots \to \mathrm{E}_{d-1} \to \mathrm{E}_0$ и их подгруппы $p$-кручения. При этом производится:

1. Подсчет цикла $d$ кривых $E_i$ и их $j$-инварианта $j_i$;
2. Поднятие всех $j_i$, которые нам дает $J_i$;
3. Поднятие каждой кривой при поднятии ее коэффициентов;
4. Поднятие подгруппы $p$-кручения для каждой кривой.

Задачей второго этапа алгоритма Сато является вычисление следа эндоморфизма Фробениуса $F : E \to E$. Предположим, что получено каноническое поднятие $\mathrm{E}$ кривой $E$, которая имеет свойство, $\mathrm{Tr}\, F = \mathrm{Tr}\, \mathrm{F}$, где $\mathrm{F}$ – эндоморфизм Фробениуса кривой $\mathrm{E}$ на $\mathbf{Z}_q$. След эндоморфизма равен следу дуального эндоморфизма:

$$\mathrm{Tr}\, F = \mathrm{Tr}\, \mathrm{F} = \mathrm{Tr}\, \hat{\mathrm{F}}.$$

Эндоморфизм Фробениуса $F$ можно разложить на произведение малых эндоморфизмов Фробениуса, которые проходят через цикл $d$ кривых $E$. Такое разложение применимо и для сопряженных кривых $\mathrm{E}$. Получаем:

$$\mathrm{Tr}\, F = \mathrm{Tr}\left(\hat{\Sigma}_{d-1} \circ \hat{\Sigma}_{d-2} \circ \ldots \circ \hat{\Sigma}_0\right).$$

Следующий шаг описывает переход в формальные группы кривой E и ее сопряжений. Обозначим через $\tau$ локальный параметр $-X/Y$ кривой E и $\tau_i$ – локальный параметр кривых $E_i$. Выражая действие $\hat{F}$ через этот параметр, получаем:

$$\hat{F}(\tau) = \sum_{k \geq 1} c_k \tau^k .$$

Далее, используя утверждение Сато, что уравнение $\phi^2 - \mathrm{Tr}(\hat{F})\phi + q = 0$, след эндоморфизма Фробениуса равен:

$$\mathrm{Tr}\, F = \mathrm{Tr}\left(\hat{F}(\tau)\right) = c_1 + \frac{q}{c_1}.$$

Таким образом, подсчета первого коэффициента достаточно для нахождения следа Фробениуса. Так как $\hat{F}$ является композицией морфизмов, то можно вычислить $c_1$ как произведение первых коэффициентов в разложении дуального эндоморфизма Фробениуса $\hat{F}$. Представим эндоморфизм $\hat{\Sigma}_i : E_i \to E_{i+1}$ в формальных группах как:

$$\hat{\Sigma}_i(\tau_i) = g_i \tau_i + O(\tau_i^2).$$

Тогда имеем:

$$c_1 = \prod_{0 \leq i \leq d} g_i .$$

Произведение $g_i$ есть норма элемента $g_0$ из $\mathbf{Z}_q$ на $\mathbf{Z}_p$, а также это след $F$ с точностью $O(p^d)$. Для увеличения точности необходимо добавить слагаемое $\frac{q}{c_1}$.

На втором этапе алгоритма Сато вычисляем $g_i$ из кривых $E_i$ и $E_{i+1}$, и ядра $\hat{\Sigma}_i$. Используя формулы Велу, получаем след эндоморфизма Фробениуса.

Рассмотрим алгебраическое расширение степени $d$ поля $F_q$ с $p$-адической точностью $O\left(p^{O(d)}\right)$. Каждый элемент $\mathbf{Z}_q$ требует для своего представления $O(d^2 \log p)$ памяти. При вычислении для каждой сопряженной кривой необходимо хранить его в памяти и при этом хранить $d$ сопряженных кривых. Значит, общий объем памяти будет не менее $O(d^3 \log p)$. Сложность вычислений с использованием быстрой арифметики можно оценить как $O(d^3 \log d \log\log d)$ или с использованием обычной – $O(d^5)$, для фиксированной характеристики $p$.

Применение алгоритма Сато позволило вычислить эллиптическую кривую на поле $2^{8001}$ за 313 часов, при этом использовался объем памяти около 16 GB.

**2 Сравнение алгоритмов Сато и SEA**

При вычислении порядка кривой необходимо выбрать, какой из алгоритмов SEA или Сато использовать для вычисления порядка кривой. Поэтому необходимо рассмотреть ограничения алгоритма.

Применение алгоритма Сато ограничено характеристикой базового поля. Вычислительная сложность алгоритма Сато сильно зависимост от характеристики $p$ базового поля, что вытекает из вычисления модулярного уравнения $\Phi_p$ для поднятия кривых, имеющего

$O(p^2)$ коэффициентов. При больших значениях характеристики $p$ базового поля применение алгоритма Сато становится неэффективным, в то время как алгоритм SEA полиномиально зависит от $p$.

Алгоритм Сато более эффективен, по сравнению с алгоритмом SEA, для небольшой характеристики базового поля, особенно для характеристики 2. В таблице 1 приведены численные характеристики сложности алгоритмов SEA и Сато для расширенного поля $F_{2^m}$.

Таблица 1

| Размер поля | 155 | 196 | 300 |
|---|---|---|---|
| SEA (сек) | 86,5 | 308 | 2434 |
| Сато(сек) | 41 | 78 | 445,4 |
| SEA/Сато | 2 | 4 | 5,4 |

Сравнительный анализ результатов вычисления алгоритмов Сато и SEA показывает, что при увеличении размера поля применения алгоритма Сато предпочтительнее по сравнению с алгоритмом SEA. Этот связано с зависимостью степеней изогении от маленького простого числа $\ell$ в алгоритме SEA.

Основной сложностью подсчета кривой для криптографических приложений является подсчет числа точек многочисленных кривых до момента нахождения требуемой, криптографически стойкой, кривой. Данную задачу оптимально решает алгоритм SEA. Например, для анализа 1000 случайных кривых на поле $F_{2^m}$ алгоритмом SEA при поиске «правильных» кривых потребовалось 14112 сек. В то время, как алгоритм Сато вычисляет одну кривую за 41 сек., на поиск правильных кривых потребуется около 41000 сек.

Для поиска криптографически стойкой кривой в связи с эффективностью вычисления порядка одной эллиптической кривой алгоритмом Сато предлагается использовать выявленную особенность по вычислению большого количества кривых алгоритмом SEA.

### 3 Нахождение криптографически стойких эллиптических кривых

Пусть кривая $E$ определена над полем $F_q$. Будем называть кривую $E$ «хорошей», если ее порядок при маленьких простых числах $\ell_i$ удовлетворяет условию $НОД(\#E, \ell_i) = 1$, и соответственно «плохой» кривой, если $НОД(\#E, \ell_i) \neq 1$.

Таким образом, попытаемся отбросить кривые, чей порядок кратен маленьким простым числам $\ell$, данное действие назовем «решетом». Отсюда вытекает задача, как, не вычисляя порядка кривой, определить ее кратность числу $\ell$.

**Теорема** *Если для некоторого простого числа $\ell$, модулярное уравнение $\Phi_\ell(X, j(E))$ в своем разложении по модулю $q$ не содержит простых корней, то порядок эллиптической кривой $\#E$ не кратен простому числу $\ell$, $НОД(\#E, \ell_i) = 1$.*

Из теоремы получаем алгоритм «решета».

*Алгоритм «решета»:*

1. Для каждого маленького простого числа $\ell$ и эллиптической кривой строим модулярные уравнения $\Phi_\ell$;
2. Вычисляем корни модулярного уравнения $\Phi_\ell(X, j(E))$;
3. Если корней не существует, то кривая $E$ – «хорошая»;

4. Если корни $\Phi_\ell$ существуют, то для каждого из них необходимо построить соответствующий сомножитель многочлена деления $h_\ell(x)$ и найти его корень. В случае существования корня полинома $h_\ell(x)$ кривая $E$ считается «плохой»;
5. Если ни один из корней $\Phi_\ell$ не принадлежит кривой, то кривая $E$ является «хорошей».

Использование данного алгоритма позволяет проанализировать порядок эллиптической кривой на кратность маленькому простому числу, не вычисляя порядка кривой. Таким образом, попробуем скомбинировать алгоритм «решета» с быстрым алгоритмом Сато:

1. Вначале исключим значительное число кривых алгоритмом «решета».
2. Затем, используя алгоритм Сато, вычислим порядки оставшихся кривых и тем самым найдем стойкие кривые.

Наиболее вычислительно трудоемкой операцией в алгоритме «решета» является вычисление $X^q$ по модулю модулярного уравнения $\Phi_\ell(X, j(E))$, имеющего степень $\ell+1$. Для ускорения вычислений можно заменить $\Phi_\ell$ на канонический модулярный полином $\Phi_\ell^c$.

Также необходимо найти такое максимальное значение $\ell$, которое бы позволило сбалансировать вычислительные затраты между $\ell$ – проверками кривой и вычислением порядка кривой. Экспериментально было получено, что уже для $\ell \le 19$ эффективность применения этого комбинированного метода превосходит алгоритм SEA. В таблице 2 приведены вычисления модулярных полиномов для различных $\ell$.

Таблица 2

| | $\ell$ | 3 | 5 | 7 | 11 | 13 | 17 | 19 |
|---|---|---|---|---|---|---|---|---|
| Вычисление корня $\Phi_\ell$ (мс) | $q = 2^{161}$ | 0,25 | 0,33 | 1,37 | 4,38 | 6,65 | 12,7 | 15,9 |
| | $q = 2^{257}$ | 0,41 | 1,08 | 2,18 | 13,1 | 15,36 | 27,9 | 33,5 |

Таблица 2 может быть расширена вследствие увеличения размера базового поля. Поэтому для каждого значения базового поля будет соответствовать свое максимальное значение маленького простого числа $\ell$.

Объединение алгоритмов «решета» и Сато позволило получить более эффективное решение, чем с алгоритм SEA. Нахождение криптографических кривых из 1000 случайных кривых в расширенном поле $F_{2^{155}}$, используя алгоритм Сато с алгоритмом «решета», потребовало 5218 сек., что в 8 раз быстрее, чем просто использовать алгоритм Сато.

В табл. 3 показан анализ 10000 кривых и приведено количество «хороших» кривых, оставшихся после выполнения алгоритма «решета», а также время вычисления алгоритма Сато для поиска криптографических кривых из оставшихся «хороших» кривых.

Таблица 3

| Поле | Хорошие кривые | Крипт. кривые | Время работы (мин) |
|---|---|---|---|
| 163 | 457 | 56 | 23,3 |
| 193 | 434 | 38 | 31,5 |
| 239 | 487 | 34 | 58,3 |
| 283 | 398 | 22 | 180 |
| 512 | 507 | 11 | 1460 |

Из табл. 3 видно, что использование алгоритма «решета» позволяет с ростом размера поля существенно уменьшить вычислительные затраты. Так, при использовании алгоритма Сато потребовалось 713 час, что в 27 раз больше, чем при использовании алгоритма Сато с алгоритмом «решета».

**Выводы**

Применение алгоритма Сато для вычисления порядка одной эллиптической кривой, определенной на расширенном поле характеристики 2, эффективно. Но, несмотря на это, алгоритм Сато не позволяет вычислить порядок кривой на простом поле большой характеристики, и в этом случае лучшим алгоритмом остается алгоритм SEA. Для увеличения эффективности нахождения криптографически стойкой кривой алгоритмом Сато был применен алгоритм «решета».

При совместном применении двух данных алгоритмов появилась возможность отказаться от использования предварительно вычисленных кривых, так как построение новой кривой будет проходить за несколько секунд. Таким образом, в криптографии получен эффективный метод для нахождения криптографически стойких кривых, используя при вычислении порядка эллиптической кривой комбинированный алгоритм Сато с алгоритмом «решета» для полей характеристики 2.

**Список литературы:** 1. *И.Д. Горбенко, С.И. Збитнев, А.А. Поляков* Криптоанализ криптографических преобразований в группах точек эллиптических кривых методом полларда // Радиотехника: Всеукр. межвед. науч-тех. сб 2001. Вып. 119. С. 43 – 50. 2. *S. Pohlig, M. Hellman* An improved algorithm for computing logarithm over *GF (p)* and its cryptographic significance, IEEE Translation on Information Theory, vol. 24, pp. 106 – 110, 1978. 3. *FIPS 186-2,* Digital signature standard, National Institute of Standards and Technology, 2000. 4. *ANSI X9.62-1999*, Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1999. 5. *IEEE P1363* / D9 (Draft Version 9). Standard Specifications for Public Key Cryptography. Number-Theoretic Background. 1999. 6. *J. Silverman*, Advanced Topic in the Arithmetic of Elliptic Curves, Graduate Text in Math., Vol. 151, Springer-Verlag, Berlin and New York, 1994. 8. *R. Schoof* Elliptic curves over finite fields and the computation o square roots mod $p$, Mathematics of Computation, 55 (1990), 745 – 763. 7. *J.H. Silverman*. The arithmetic of elliptic curve, volume 106 of Graduate Texts in Mathematics. Springer, 1986. 9. *R. Lercier*. Finding good random elliptic curves for cryptosystems defined over $F_{2^n}$. In W. Fumy, editor, Advanced in Cryptology – EUROCRYPT '97, Vol. 1233 of Lecture Notes in Comput. Sci., pages 379 – 392. Springer-Verlag, 1997. International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 1997, Proceeding. 10. *Schoof R.* Counting points on elliptic curve over finite fields, Journal de Theories des Nombres de Bordeaux, Vol. 7, pp. 219 – 254, 1995. 11. *R. Lercier and A. Morain*. Counting the number of points on elliptic curves over finite fields: Strategies end performances. In L. C. Guillou and J.-J. Quisquater, Editors, Advanced in Cryptology – EUROCRYPT '95, Vol. 921 of Lecture Notes in Comput. Sci., pp. 79 – 94. Springer-Verlag, 1995. International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 1995, Proceeding. 12. *L. Dewaghe.* Remarks on the Schoof-Elkies-Atkin algorithm. Math. Comp., 67(233): 1247 – 1252, July 1998. 13. *B. Skiernaa.* Satoh's algorithm in characteristic 2. 14. *T. Satoh.* The canonical lift of an ordinary elliptic curve over a finite field and its point counting. J. Ramanujan Math. Soc., 15: 247 – 270, 2000.

*Харьковский национальный*

*университет радиоэлектроники*

*Поступила в редколлегию 12.05.2003*