УДК 519.719.2

ОБ ОДНОЙ СХЕМЕ ГИБРИДНОГО ШИФРОВАНИЯ

А. Ю. Нестеренко*, А. В. Пугачев**

**Национальный исследовательский университет «Высшая школа экономики»,*
***Московский государственный университет информационных технологий, радиотехники и электроники,*
г. Москва, Россия

Предлагается гибридная схема шифрования, которая базируется на схеме асимметричного шифрования Эль-Гамаля и использует предварительно распределённые секретные ключи для защиты от навязывания сообщений. Стойкость схемы основывается на высокой трудоёмкости решения задачи дискретного логарифмирования в группе точек эллиптической кривой. Основная особенность предлагаемой схемы заключается в том, что шифруемое сообщение не представляется в виде точки эллиптической кривой, что позволяет зашифровывать длинные сообщения. Приводится обоснование стойкости предложенной схемы, а также описание её возможных модификаций, направленных на выполнение дополнительных криптографических свойств, например аутентификации отправителя сообщения. Приводятся также результаты практической реализации схемы.

Ключевые слова: *асимметричное шифрование, схема Эль-Гамаля, эллиптические кривые, аутентификация отправителя сообщений.*

DOI 10.17223/20710410/30/5

A NEW HYBRID ENCRYPTION SCHEME

A. Yu. Nesterenko*, A. V. Pugachev**

**National Research University Higher School of Economics,*
***Moscow State University of Information Technologies, Radio Engineering and Electronics, Moscow, Russia*

E-mail: nesterenko_a_y@mail.ru, a_pugachev@mirea.ru

A new hybrid encryption scheme based on ElGamal asymmetric encryption scheme with distributed secret keys is presented. The keys are used for defence against unauthorised intrusion of encrypted messages. The security of the scheme is based on elliptic curve discrete logarithm problem. The main feature of the scheme is the fact that plain message is not represented as a point of elliptic curve, hence, we can encrypt a long messages. We validate the cryptographic properties of the scheme and give some examples of its practical evaluations.

Keywords: *asymmetric encryption, authentication, ElGamal scheme, elliptic curves.*

Введение

В настоящее время известно много схем асимметричного шифрования, позволяющих обеспечить процесс передачи зашифрованного сообщения от одного абонента

к другому. К таким схемам можно отнести схемы RSA, Эль-Гамаля, Рабина, Голдвассер — Микали и т. д. [1, гл. 8]. Стойкость каждой из перечисленных схем основывается на трудоёмкости решения некоторой теоретико-числовой задачи, например разложения больших чисел на множители или дискретного логарифмирования.

Основным недостатком асимметричных схем шифрования является тот факт, что они позволяют эффективно зашифровывать и расшифровывать только сообщения малой длины, например криптографические ключи. В связи с этим для шифрования длинных сообщений применяются так называемые «гибридные» схемы, в которых сообщение шифруется при помощи симметричного алгоритма шифрования, а ключ — при помощи асимметричной схемы [2].

В настоящей работе предлагается новый вариант схемы гибридного шифрования, основывающийся на схеме асимметричного шифрования Эль-Гамаля и использующий предварительно распределённые секретные ключи для защиты от навязывания сообщений. Кроме того, представлены несколько модификаций схемы, позволяющих её участникам:

— эффективно зашифровывать сообщения большой длины;
— использовать цифровую подпись для аутентификации отправителя сообщений.

В п. 1 приводится подробное описание предложенного нового варианта схемы асимметричного шифрования, определяется ключевая система, а также процедуры зашифрования и расшифрования сообщений. В п. 2 дан краткий анализ предложенной схемы: определены возможности нарушителя и перечень целей компрометации; рассмотрены основные атаки и показано, что при выполнении ряда предположений схема является стойкой.

В п. 3 приведены несколько модификаций предложенной схемы. Каждая модификация позволяет обеспечить дополнительные криптографические свойства, например обеспечить аутентификацию отправителя сообщений или увеличить длину шифруемого сообщения. В заключение приводятся результаты практической реализации схемы с конкретными значениями параметров и используемыми криптографическими примитивами.

1. Описание базовой схемы

1.1. Параметры схемы и её ключевая система

1) Пусть $p > 3$ — простое число. Рассмотрим эллиптическую кривую $\mathcal{E}$, заданную над конечным простым полем $\mathbb{F}_p$ сравнением

$$y^2 \equiv x^3 + ax + b \pmod{p}, \tag{1}$$

где $a, b \in \mathbb{F}_p$ удовлетворяют условию $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$.
2) Рассмотрим простое число $q > 2$, делящее порядок группы точек эллиптической кривой $\mathcal{E}$, и выберем точку $P = (x_P, y_P) \in \mathcal{E}$, которая порождает циклическую подгруппу $\langle P \rangle \subset \mathcal{E}$ порядка q.
3) Рассмотрим целое число m, такое, что $p < m < 2p^2$. Каждое сообщение s будем представлять в виде вычета по модулю m: $s \in \mathbb{Z}_m$.
4) Введём два простых отображения

$$f : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{Z}_m, \quad h : \mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{Z}_m,$$

которые будут использованы при зашифровании и расшифровании сообщений. В п. 1.3 мы дадим корректное определение этих отображений.

5) Пусть r — натуральное число. Будем использовать отображение

$$\mathrm{mac} : \mathbb{F}_q \times \mathbb{Z}_m \to \mathbb{Z}_r,$$

позволяющее вычислить код целостности или, другими словами, имитовставку сообщения $s \in \mathbb{Z}_m$, зависящую от некоторого секретного ключа из $\mathbb{F}_q$. В качестве такого отображения может выступать алгоритм HMAC [3] или отечественный алгоритм выработки имитовставки [4].

6) Для генерации ключа, используемого при выработке имитовставки, будем использовать функцию выработки ключа

$$\mathrm{kdf} : \mathbb{F}_p \times \mathcal{E} \to \mathbb{F}_q.$$

Примером функции выработки ключа может служить алгоритм, описанный в рекомендациях [5].

Далее будем считать, что все перечисленные параметры (целые числа p, a, b, q, m, r; точка эллиптической кривой $P = (x_P, y_P)$; отображения f, h, mac() и kdf()) известны как отправителю и получателю сообщения, так и нарушителю.

Теперь рассмотрим ключевую систему. Абонент Б, являющийся получателем сообщений, должен обладать следующими параметрами:

1) секретным ключом d — целым числом, удовлетворяющим неравенствам $0<d<q$;
2) открытым ключом Y — точкой эллиптической кривой $\mathcal{E}$, заданной парой координат (x_Y, y_Y) и определяемой равенством

$$Y = [d]P = \underbrace{P + \cdots + P}_{d \text{ раз}}.$$

Кроме того, будем считать, что абоненты А и Б обладают общим долговременным секретным ключом S — точкой эллиптической кривой $\mathcal{E}$, заданной парой своих координат (x_S, y_S) и удовлетворяющей сравнению (1). Дополнительно будем считать, что координата x_S выбрана таким образом, что величина $(ax_S + b)^2 + 4bx_S^3$ является квадратичным невычетом по модулю p.

1.2. Процедуры зашифрования и расшифрования

Для зашифрования сообщения $s \in \mathbb{Z}_m$ абонент А (отправитель сообщения) выполняет следующие шаги:

1) Вычисляет случайное целое число k, удовлетворяющее неравенствам $0 < k < q$.
2) Вычисляет точку $U = [k]Y$, $U = (x_U, y_U)$, эллиптической кривой $\mathcal{E}$ и определяет $\alpha, \beta \in \mathbb{F}_p$, где

$$\begin{cases} \alpha \equiv \dfrac{y_U - y_S}{x_U - x_S} \pmod p, \\ \beta \equiv \dfrac{y_S x_U - x_S y_U}{x_U - x_S} \pmod p. \end{cases} \tag{2}$$

3) Вычисляет точку $W = [k]P$, $W = (x_W, y_W)$, и определяет

$$t \equiv f(\alpha, y_U)s + h(\alpha, \beta, y_U) \pmod m. \tag{3}$$

4) Определяет ключ $d_U = \mathrm{kdf}(x_U, S)$. Затем вычисляет код целостности $\mathrm{mac}(d_U, s)$ и формирует сообщение

$$M = t||(x_W, y_W)||\,\mathrm{mac}(d_U, s). \tag{4}$$

Сообщение M является шифртекстом, который отправляется абоненту Б.

Легко видеть, что длина открытого текста s равна $\log_2 m$ бит, а длина соответствующего ему шифртекста M равна $\log_2 m + 2\log_2 p + \log_2 r$ бит.

В случае, когда преобразования f и h имеют вид

$$f(\alpha, y_U) \equiv \alpha \pmod m, \quad h(\alpha, \beta, y_U) \equiv \beta \pmod m,$$

предложенный способ зашифрования сообщения s имеет красивую геометрическую интерпретацию. Действительно, рассмотрим координаты точек S, U эллиптической кривой $\mathcal{E}$ как пары целых неотрицательных чисел. Расположим эти точки на действительной плоскости и проведём через них прямую линию. Рассмотрим открытый текст s как целое неотрицательное число, определяющее абсциссу некоторой точки T на данной прямой. Тогда шифртекст t есть ордината точки T, взятая по модулю m (рис. 1).

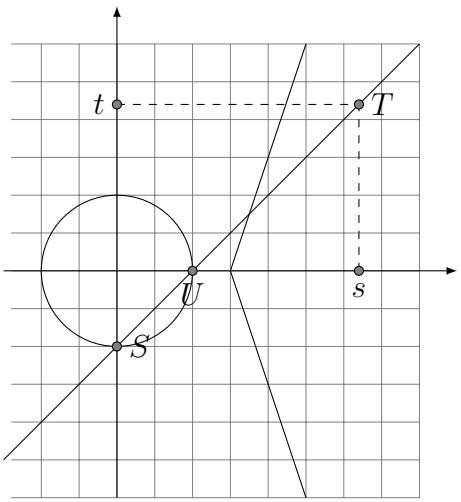

Рис. 1. Геометрическая интерпретация в простейшем случае

Поскольку абонент А при зашифровании сообщения s выбирает значение k случайным образом, вырабатываемая им точка $U = [k]P$, а следовательно, и прямая $t = f(\alpha, y_U)s + h(\alpha, \beta, y_U)$ также являются случайными.

Для расшифрования полученного сообщения M абонент Б представляет его в виде тройки $t \in \mathbb{Z}_m$, $W = (x_W, y_W) \in \mathcal{E}$ и кода целостности $\xi \in \mathbb{Z}_r$. Далее абонент Б выполняет следующие шаги:

1) Проверяет, что точка W принадлежит эллиптической кривой $\mathcal{E}$. В противном случае сообщение t не принимается.
2) Вычисляет точку $U = [d]W$, где $U = (x_U, y_U)$.
3) Используя сравнения (2), вычисляет значения $\alpha, \beta \in \mathbb{F}_p$ и определяет открытый текст s сравнением

$$s \equiv (t - h(\alpha, \beta, y_U))f^{-1}(\alpha, y_U) \pmod m. \tag{5}$$

4) Вычисляет ключ $d_U = \mathrm{kdf}(x_U, S)$ и код целостности $\mathrm{mac}(d_U, s)$. Если $\mathrm{mac}(d_U, s) = \xi$, то сообщение принимается и считается корректно расшифрованным. В противном случае сообщение не принимается.

1.3. Некоторые замечания о выборе параметров схемы

Сделаем несколько замечаний по выбору параметров схемы, влияющих как на корректность её работы, так и на её эксплуатационные качества.

Выбор долговременного ключа S

Для корректной работы предложенной схемы асимметричного шифрования должно выполняться условие

$$U \neq \pm S. \tag{6}$$

В противном случае выполнено сравнение $x_S \equiv x_U \pmod p$, и величины $\alpha, \beta \in \mathbb{F}_p$, удовлетворяющие равенствам (2), не могут быть корректно определены.

Выполнение условия (6) может быть обеспечено двумя способами. В первом случае можно выбрать эллиптическую кривую $\mathcal{E}$ таким образом, чтобы порядок её группы $|\mathcal{E}|$ удовлетворял равенству

$$|\mathcal{E}| = cqq_1,$$

где $q_1 > 2$ — некоторое большое простое число и $q_1 \neq q$; $c \geqslant 1$ — произвольное натуральное число. Тогда, выбирая в качестве S точку порядка q_1, получим, что для любого целого k, такого, что $0 < k < q$, выполнено условие

$$S \neq \pm U = \pm [k]P.$$

Во втором случае, когда порядок кривой $\mathcal{E}$ удовлетворяет равенству $|\mathcal{E}| = cq$ для некоторого натурального числа $c \geqslant 1$, можно модифицировать процедуру зашифрования сообщения s и проверять выполнение условия $U \neq \pm S$ на первом шаге алгоритма зашифрования. В случае невыполнения этого условия необходимо выбрать новое значение k.

Следует отметить, что если k выбирается случайно равновероятно из интервала $0 < k < q$, то вероятность получить равенство $U = \pm S$ мала и равна $2/(q-1)$.

Выбор значения параметра m и отображений f и h

Отметим, что выполнение условия $U \neq \pm S$ влечёт за собой выполнение условия $y_S \neq y_U$. В этом случае из (2) следует, что $\alpha \not\equiv 0 \pmod p$. Аналогично, для величины β выполнено следующее утверждение.

Лемма 1. Пусть величина $\beta \in \mathbb{F}_p$ определена сравнением (2). Пусть x-координата точки $S = (x_S, y_S) \in \mathbb{E}$ удовлетворяет условию

$$\left(\frac{(ax_S + b)^2 + 4bx_S^3}{p}\right) = -1,$$

где $\left(\frac{\cdot}{\cdot}\right)$ есть символ Лежандра. Тогда $\beta \not\equiv 0 \pmod p$.

Доказательство. Из (2) следует, что выполнение условия $\beta \equiv 0 \pmod p$ эквивалентно выполнению сравнения

$$y_S x_U \equiv y_U x_S \pmod p. \tag{7}$$

В силу выбора параметров схемы порядки точек U и S больше двух, поэтому их y-координаты отличны от нуля. Далее, если одна из x-координат, скажем x_U, сравнима с нулем по модулю p, то из (7) следует, что и вторая x-координата x_S также сравнима с нулем, что невозможно в силу (6). Таким образом, выполнение сравнения $\beta \equiv 0 \pmod p$ влечёт за собой сравнение

$$y_U \equiv \frac{y_S}{x_S} x_U \pmod p, \quad x_S \not\equiv 0 \pmod p.$$

Поскольку $(x_U, y_U) \in \mathcal{E}$, из последнего сравнения следует, что величина x_U должна являться корнем многочлена

$$\varphi(x) = x^3 - \left(\frac{y_S}{x_S}\right)^2 x^2 + ax + b$$

по модулю простого числа p. Легко проверить, что $\varphi(x_S) \equiv 0 \pmod{p}$; тогда можно записать сравнение

$$\varphi(x) \equiv (x - x_S)\left(x^2 - \frac{(ax_S + b)}{x_S^2}x - \frac{b}{x_S}\right) \pmod{p}. \tag{8}$$

В силу утверждения леммы, многочлен второй степени, входящий в произведение в правой части сравнения (8), не имеет корней в поле $\mathbb{F}_p$, поскольку его дискриминант

$$D \equiv \left(\frac{ax_S + b}{x_S^2}\right)^2 + \frac{4b}{x_S} \equiv \frac{(ax_S + b)^2 + 4bx_S^3}{x_S^4} \pmod{p}$$

является квадратичным невычетом по модулю p. ■

Теперь можно дать точное определение введённых ранее отображений f и h. Ввиду того, что значение $f(\alpha, y_U) \in \mathbb{Z}_m$ должно быть обратимо по модулю m, отображения f и h должны зависеть от значений параметра m, задающего длину шифруемого сообщения s.

Рассмотрим несколько вариантов.

1) Пусть m есть простое число или $m = p_1p_2$ есть произведение двух нечётных простых чисел, для которых выполнены неравенства $p < p_1 < p_2$. Поскольку вырабатываемая в алгоритме зашифрования величина α удовлетворяет соотношению $\alpha \not\equiv 0 \pmod{p}$, можно определить

$$f(\alpha, y_U) \equiv \alpha y_U \pmod{m}. \tag{9}$$

Порядок точки U равен q, поэтому $y_U \not\equiv 0 \pmod{p}$,

$$0 < \alpha y_U < m, \quad (\alpha, m) = 1.$$

Следовательно, значение $f(\alpha, y_U) = \alpha y_U$ обратимо по модулю m. Поскольку должно выполняться неравенство $m = p_1p_2 < 2p^2$, можно предъявить следующие оценки на величины p_1, p_2. Определим действительные величины γ_1, γ_2 неравенством $p_i < p + p^{\gamma_i}$, где $i = 1, 2$, и будем считать, что выполнено неравенство

$$0 < \gamma_1 < \gamma_2 < 1 - \log_p 3. \tag{10}$$

Тогда, учитывая, что из (10) следует неравенство $1 + \gamma_2 > 2\gamma_2$, получим

$$m = p_1p_2 < p^2 + p(p^{\gamma_1} + p^{\gamma_2}) + p^{\gamma_1+\gamma_2} < p^2 + 2p^{1+\gamma_2} + p^{2\gamma_2} < p^2 + 3p^{1-\log_p 3} = 2p^2.$$

2) Пусть $m = 2^n$ для некоторого натурального n и $m > 4p + 1$. Тогда можно определить

$$f(\alpha, y_U) \equiv 2(\alpha + y_U) + 1 \pmod{m}. \tag{11}$$

Поскольку $0 < \alpha < p$, $0 < y_U < p$, то получаем, что выполнено неравенство $1 < < f(\alpha, y_U) < 4p + 1 < m$; значение $f(\alpha, y_U)$ нечётно, следовательно, $f(\alpha, y_U)$ обратимо по модулю m.

Легко видеть, что отображение h действует в (3) как аддитивная маска. Следовательно, можно определить

$$h(\alpha, \beta, y_U) \equiv f^{-1}(\alpha, y_U)\beta \pmod{m}.$$

Отметим, что из леммы 1 вытекает, что значение $h(\alpha, \beta, y_U)$ отлично от нуля.

2. Краткий анализ предложенной схемы

Далее рассмотрим несколько атак на предложенную схему асимметричного шифрования и покажем, что при некоторых допущениях схема может считаться стойкой. Будем считать, что у желающего скомпрометировать схему нарушителя могут быть следующие цели:

— определение секретного ключа абонента Б;
— дешифрование переданного сообщения;
— навязывание абоненту Б ложного сообщения.

Предполагаем, что нарушитель обладает открытыми параметрами схемы, может перехватывать все передаваемые сообщения и проводить так называемый «пассивный» анализ. Более того, предполагаем, что нарушитель может активно воздействовать на канал связи и использовать абонента Б в качестве «оракула» для расшифрования специально подобранных сообщений [6]. Данные возможности нарушителя в англоязычной литературе принято называть возможностями, используемыми при проведении CCA и CCA2 атак.

Будем считать, что нарушитель может получать расшифрованные сообщения только в том случае, если сообщение расшифровано абонентом Б корректно, в частности, содержит корректный код целостности. Кроме того, упростим задачу нарушителю и будем предполагать, что ему известны координаты точки S, рассматривавшейся ранее как долговременный ключ.

2.1. Сведение задачи определения секретного ключа к задаче дискретного логарифмирования

Легко видеть, что сложность определения секретного ключа d абонента Б основывается на трудоёмкости решения задачи дискретного логарифмирования в группе точек эллиптической кривой $\mathcal{E}$. Действительно, поскольку нарушителю известны все открытые параметры схемы, в частности точка P порядка q и открытый ключ Y абонента Б, то секретный ключ может быть найден из уравнения

$$Y = [d]P, \quad d \in \mathbb{Z}_q^*.$$

Аналогично, если нарушителю каким-либо образом удалось определить точку U, используемую для зашифрования и расшифрования сообщений, то он может найти секретный ключ d из уравнения

$$U = [d]W, \quad d \in \mathbb{Z}_q^*.$$

Известно, что решение задачи дискретного логарифмирования в группе точек эллиптической кривой, определённой над конечным простым полем $\mathbb{F}_p$, является сложной задачей, трудоёмкость которой оценивается величиной $\mathrm{O}(\sqrt{q})$ [7, 8]. Это не позволяет, при больших значениях q, на практике найти значение d.

2.2. Сведение к задаче Диффи — Хеллмана

Перейдём к рассмотрению вопросов о дешифровании передаваемого сообщения. Предположим, что нарушитель умеет находить решение задачи Диффи — Хеллмана

в группе точек эллиптической кривой $\mathcal{E}$. Другими словами, по заданным точкам P, $W = [k]P$, $Y = [d]P$, $P, W, Y \in \mathcal{E}$, нарушитель может определить точку $U \in \mathcal{E}$, удовлетворяющую равенству

$$U = [kd]P.$$

Поскольку мы предполагаем, что нарушителю известна точка S, он может воспользоваться сравнениями (2), определить значения $\alpha, \beta \in \mathbb{F}_p$ и расшифровать передаваемое сообщение с использованием сравнения (5). Таким образом, нарушитель, который умеет решать задачу Диффи — Хеллмана в группе точек эллиптической кривой $\mathcal{E}$, может дешифровывать передаваемые сообщения. Следует отметить, что в настоящее время задача Диффи — Хеллмана в группе точек эллиптической кривой считается трудноразрешимой, а наиболее эффективный способ её решения заключается в сведении к задаче дискретного логарифмирования [8].

В случае, когда нарушитель умеет решать задачу Диффи — Хеллмана, но не знает точного значения координат точки S, он может предложить атаку для их определения. Действительно, пусть $l \geqslant 2$ — натуральное число, тогда, воспользовавшись абонентом Б как «оракулом» расшифрования, нарушитель может получить значения открытых текстов $s_1, \ldots, s_l \in \mathbb{Z}_m$ для некоторых произвольных корректно расшифрованных абонентом Б шифртекстов $M_1, \ldots, M_l$ вида (4). После этого нарушитель может составить систему уравнений

$$\begin{cases} \alpha_i \equiv \dfrac{y_{U_i} - y_S}{x_{U_i} - x_S} \pmod p, \\ \beta_i \equiv \dfrac{y_S x_{U_i} - x_S y_{U_i}}{x_{U_i} - x_S} \pmod p, \\ t_i \equiv f(\alpha_i, y_{U_i}) s_i + h(\alpha_i, \beta_i, y_{U_i}) \pmod m, \quad i = 1, \ldots, l. \end{cases} \tag{12}$$

Данная система состоит из $3l$ уравнений и зависит от $2l + 2$ неизвестных $\alpha_1, \ldots, \alpha_l, \beta_1, \ldots, \beta_l, x_S, y_S$ (значения $x_{U_1}, \ldots, x_{U_l}, y_{U_1}, \ldots, y_{U_l}$ известны нарушителю). В силу построения решение системы (12) существует, следовательно, нарушитель может найти это решение и определить неизвестные ему значения x_S, y_S.

2.3. Понятие разового ключа

Можно считать, что величина $k \in \mathbb{Z}_q^*$, вырабатываемая на первом шаге алгоритма зашифрования, является *разовым* ключом, поскольку её раскрытие приводит к эффективному дешифрованию.

Действительно, пусть $M = t||W||\operatorname{mac}(d_U, s)$ — шифртекст, выработанный под сообщением $s \in \mathbb{Z}_m$ с использованием величины k. Тогда нарушитель, зная величину k и открытый ключ Y абонента Б, может вычислить точку $U = [k]Y$. Далее, используя (2) и зная долговременный ключ S, нарушитель может определить параметры $\alpha, \beta \in \mathbb{F}_p$ и расшифровать передаваемое сообщение с использованием сравнения (5).

Добавим, что если нарушитель имеет доступ к $l \geqslant 2$ различным разовым ключам $k_1, \ldots, k_l$, а также может использовать абонента Б в качестве «оракула» расшифрования, вычисляющего по шифртекстам M_1, …, M_l, выработанным с использованием указанных разовых ключей, соответствующие корректно расшифрованные открытые тексты $s_1, \ldots, s_l$, то он может определить точное значение долговременного ключа S. Для этого нарушителю достаточно решить систему сравнений (12).

2.4. Атака при шифровании на одинаковых разовых ключах

Рассмотрим ситуацию, при которой нарушитель перехватывает $l \geqslant 2$ шифртекстов $M_1, \ldots, M_l$, выработанных с использованием одного и того же неизвестного нарушите-

лю разового ключа k. Для этого нарушителю достаточно отобрать из множества всех перехваченных шифртекстов те, у которых совпадают координаты точки W.

В этом случае, если нарушитель может использовать абонента Б как «оракула» для корректного расшифрования двух открытых текстов, скажем s_1 и s_2, он может при $l \geqslant 3$ эффективно дешифровать оставшиеся сообщения $s_3, \ldots, s_l$.

Действительно, параметры $\alpha, \beta \in \mathbb{F}_p$, определяемые равенствами (2) при одинаковых значениях $k \in \mathbb{Z}_q^*$, точка U и, следовательно, значения $f(\alpha, y_U)$, $h(\alpha, \beta, y_U)$ одинаковы для всех перехваченных сообщений $M_1, \ldots, M_l$. Тогда значения $f(\alpha, y_U)$, $h(\alpha, \beta, y_U)$ могут быть эффективно вычислены нарушителем. Пусть $t_1, t_2 \in \mathbb{Z}_m$ — фрагменты шифртекстов M_1 и M_2 соответственно. Тогда нарушитель может решить систему сравнений

$$\begin{cases} t_1 \equiv f(\alpha, y_U)s_1 + h(\alpha, \beta, y_U) \pmod m, \\ t_2 \equiv f(\alpha, y_U)s_2 + h(\alpha, \beta, y_U) \pmod m \end{cases} \tag{13}$$

относительно неизвестных значений $f(\alpha, y_U)$ и $h(\alpha, \beta, y_U)$, после чего воспользоваться равенствами (5) и дешифровать открытые тексты $s_3, \ldots, s_l$.

2.5. Атака на основе адаптивно подобранных шифртекстов

Известно [9], что классическая схема Эль-Гамаля является уязвимой относительно атаки с адаптивно подобранным шифртекстом. Рассмотрим возможность применения данной атаки к нашей схеме.

Будем считать, что нарушитель хочет дешифровать шифртекст

$$M = t||(x_W, y_W)||\operatorname{mac}(d_U, s)$$

и определить сообщение s. Для этого он пользуется абонентом Б как «оракулом» расшифрования и направляет ему на расшифрование два шифртекста специального вида

$$M_1 = 0||(x_W, y_W)||\operatorname{mac}(d_U, s), \quad M_2 = 1||(x_W, y_W)||\operatorname{mac}(d_U, s).$$

Легко видеть, что шифртексты M, M_1, M_2 выработаны с одним и тем же значением разового ключа k. Используя рассуждения выше и соответствующие шифртекстам M_1 и M_2 открытые тексты s_1, s_2, нарушитель может определить значения величин $f(\alpha, y_U)$ и $h(\alpha, \beta, y_U)$ из равенств (13):

$$f(\alpha, y_U) \equiv \frac{1}{s_2 - s_1} \pmod m, \quad h(\alpha, \beta, y_U) \equiv \frac{s_1}{s_1 - s_2} \pmod m. \tag{14}$$

Теперь величина s определяется из сравнения (3). Отметим, что для проведения атаки значения t_1 и t_2 могут принимать произвольные отличные друг от друга значения. Значения $t_1 = 0$ и $t_2 = 1$ выбраны для минимизации формул (14).

Однако возможность осуществления приведённой атаки возникает только в том случае, когда абонент Б при расшифровании шифртекстов M_1, M_2 не проверяет код целостности сообщения. Действительно, направляемый в шифртекстах M_1, M_2 код целостности $\operatorname{mac}(d_U, s)$ соответствует сообщению s и для корректного расшифрования должен изменяться при замене фрагмента t на t_1 или t_2. Таким образом, данная атака осуществима нарушителем в одном из двух случаев:

1) Для двух произвольных отличных друг от друга заранее заданных значений t_0, t_1 нарушитель может вычислить значения

$$\operatorname{mac}(d_U, s_i), \quad s_i \equiv (t_i - h(\alpha, \beta, y_U))f^{-1}(\alpha, y_U) \pmod m, \quad i = 1, 2,$$

при неизвестных значениях $f(\alpha, y_U)$, $h(\alpha, \beta, y_U)$ и ключа d_U.

2) Для двух произвольных отличных друг от друга заранее заданных значений ξ_1, ξ_2 нарушитель может определить два значения t_1 и t_2, такие, что

$$\mathrm{mac}(d_U, s_i) = \xi_i,\ s_i \equiv (t_i - h(\alpha, \beta, y_U))f^{-1}(\alpha, y_U) \pmod m,\ i = 1, 2,$$

при неизвестных значениях $f(\alpha, y_U)$, $h(\alpha, \beta, y_U)$ и ключа d_U.

Если для функции mac перечисленные предположения не выполняются, то предложенная схема может считаться стойкой относительно атаки с адаптивно подобранными шифртекстами (CCA2).

2.6. Использование геометрических особенностей схемы для её компрометации

Легко заметить, что предложенная схема обладает одной геометрической особенностью, которая может быть использована нарушителем для достижения целей компрометации. Действительно, из закона сложения на эллиптической кривой $\mathcal{E}$ вытекает, что в простейшем случае, когда $f(\alpha, y_U) \equiv \alpha \pmod m$ и $h(\alpha, \beta, y_U) \equiv \beta \pmod m$, прямая $t \equiv \alpha s + \beta$, используемая для зашифрования сообщения s, содержит в себе не только точки $U, S \in \mathcal{E}$, но и точку $-(U+S) \in \mathcal{E}$ (здесь, как и ранее, мы рассматриваем координаты точек как целые неотрицательные числа). Геометрически это изображено на рис. 2.

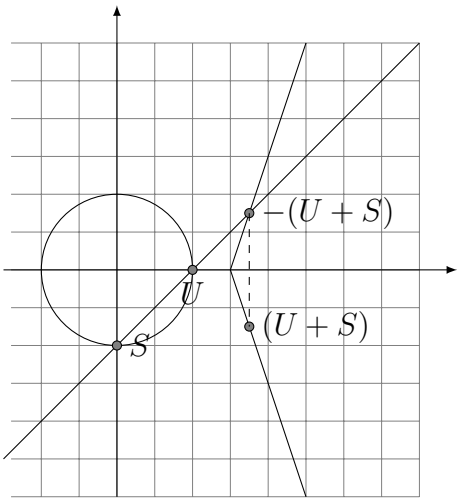

Рис. 2. Точки U, S и $-(U+S)$ на эллиптической кривой $\mathcal{E}$

Этот факт позволяет выразить значения параметров α и β через координаты точек U и $-(S+U)$. Более того, если $S, U \in \langle P \rangle$, то и $-(S+U) \in \langle P \rangle$, следовательно, найдется целое число k_0, такое, что $0 < k_0 < q$ и $-(U+S) = [k_0]P$. Если выполнено условие $S \neq [-2]U$, то $k_0 \neq k$ и получаем, что в схеме существуют два различных значения k, k_0, для которых будет выработано одно и то же значение параметров α и β.

Согласно (9) и (11), значение функции $f(\alpha, y_U)$ зависит не только от α, но и от x-координаты точки U, следовательно, значения $f(\alpha, y_U)$ и $f(\alpha, y_{-(U+S)})$, выработанные для точек U и $-(U+S)$ соответственно, различаются.

2.7. Навязывание сообщений

Высказанное ранее предположение о том, что нарушителю известен долговременный ключ S, позволяет предъявить простой алгоритм подделки передаваемого сообще-

ния. Действительно, для любого открытого текста $s_1 \in \mathbb{Z}_m$, $s_1 \not\equiv s \pmod m$, нарушитель может воспользоваться алгоритмом зашифрования и сформировать шифртекст

$$M_1 = t_1 || (x_W, y_W) || \operatorname{mac}(d_U, s_1),$$

который будет корректно расшифрован абонентом Б.

Поскольку $d_U = \operatorname{kdf}(x_U, S)$ и вычисление кода целостности $\operatorname{mac}(d_U, s_1)$ невозможно без знания долговременного ключа S, то навязывание абоненту Б ложного сообщения возможно только в двух случаях:

1) при компрометации долговременного ключа S;
2) если для заданных значений s и $\operatorname{mac}(d_U, s)$ нарушитель может определить секретный ключ d_U.

Для навязывания ложного сообщения при наличии второй уязвимости может быть применён вариант изложенной ранее атаки на одинаковых разовых ключах. Используя абонента Б в качестве «оракула расшифрования», нарушитель может получить для двух перехваченных шифртекстов M_1, M_2, выработанных на одном и том же разовом ключе k, соответствующие им открытые тексты s_1, s_2. Решая систему сравнений (13), нарушитель может найти значения $f(\alpha, y_U)$ и $h(\alpha, \beta, ty_U)$.

Теперь, используя уязвимость функции mac(), нарушитель может определить секретный ключ d_U, на котором был выработан код целостности сообщений s_1, s_2, и вычислить корректный шифртекст для произвольного сообщения s. Заметим, что в таком шифртексте будет присутствовать точка W, содержащаяся также в сообщениях M_1, M_2.

Легко заметить, что данная атака невозможна, если в распоряжении нарушителя не имеется двух шифртекстов M_1, M_2, выработанных на одном и том же разовом ключе.

Суммируем изложенные результаты в виде следующей теоремы.

Теорема 1. Предложенная схема асимметричного шифрования может считаться стойкой относительно угроз раскрытия секретного ключа, дешифрования и навязывания сообщений в случае, когда выполнены следующие условия:

1) для нарушителя являются трудоёмкими задачи дискретного логарифмирования и Диффи — Хеллмана в группе точек эллиптической кривой $\mathcal{E}$;
2) долговременный ключ S не известен нарушителю;
3) каждое сообщение шифруется с помощью уникального разового ключа k;
4) для функции выработки кода целостности mac() нарушитель не может решить задач, поставленных в п. 2.5 и 2.7;
5) расшифрованные сообщения, для которых неверен код целостности, не являются доступными нарушителю.

3. Обобщения базовой схемы

Изложенная базовая схема допускает несколько различных модификаций, позволяющих изменить её функциональные особенности без изменения стойкости. Далее рассмотрим несколько вариантов, приведя, для краткости, лишь алгоритм зашифрования сообщений.

3.1. Вариант с зашифрованием кода целостности

Передаваемый абоненту Б шифртекст M содержит в себе три составляющих: зашифрованное сообщение t, точку эллиптической кривой W и код целостности открытого текста s. При этом код целостности может рассматриваться как некоторая информация о передаваемом сообщении. Эта информация может привести к появлению

атак на функцию выработки кода целостности с целью определения сообщения s по его коду целостности.

Для предотвращения подобного рода атак схема может быть модифицирована следующим образом. Определим целое число c_m равенством

$$c_m = \lfloor \log_2 m \rfloor - \lceil \log_2 r \rceil.$$

Будем шифровать сообщения $s \in \mathbb{Z}_{2^{c_m}}$. Для этого абонент А выполняет сначала шаги 1, 2 базовой схемы (см. п. 1.1), затем следующие шаги:

3) Определяет ключ $d_U = \mathrm{kdf}(x_U, S)$, затем вычисляет код целостности $\mathrm{mac}(d_U, s)$ и формирует сообщение $s' = s || \mathrm{mac}(d_U, s)$.
4) Вычисляет точку $W = [k]P$, $W = (x_W, y_W)$, определяет

$$t \equiv f(\alpha, y_U)s' + h(\alpha, \beta, y_U) \pmod{m}$$

и направляет абоненту Б шифртекст $M = t||(x_W, y_W)$.

В данном варианте схемы шифрования длина открытого текста s равна c_m бит, а длина соответствующего ему шифртекста M равна $\log_2 m + 2\log_2 p$ бит.

Легко видеть, что мы зашифровываем код целостности сообщения вместе с самим сообщением. Это позволяет скрыть от нарушителя информацию об открытом тексте s. Взамен мы уменьшаем размер открытого текста на $\lceil \log_2 r \rceil$ бит.

3.2. Вариант с аутентификацией отправителя

Изложенная базовая схема, в общем случае, не обеспечивает аутентификацию отправляющего сообщения абонента А. Действительно, точка S может являться долговременным ключом, известным нескольким абонентам, скажем $\mathrm{A}_1, \ldots, \mathrm{A}_l$, отправляющим сообщения абоненту Б. В этом случае абонент Б не может произвести различия между абонентами $\mathrm{A}_1, \ldots, \mathrm{A}_l$. Кроме того, это позволяет им навязывать от имени друг друга сообщения абоненту Б.

В случае, когда подобная ситуация является недопустимой, можно воспользоваться механизмом аутентификации отправляемых сообщений на основе цифровой подписи. Идея схемы асимметричного шифрования с аутентификацией отправителя была ранее высказана первым автором в [10].

Для реализации механизма аутентификации отправителя сообщения абонент А должен обладать парой персональных ключей — открытым ключом e_A и секретным ключом d_A цифровой подписи. Для выработки и проверки цифровой подписи может быть использована схема, регламентируемая национальным стандартом РФ ГОСТ Р 34.10-2012 [11].

В связи с использованием механизма цифровой подписи алгоритмы mac() и kdf() не используются. Кроме того, мы можем считать точку S общеизвестным открытым параметром схемы.

Как и для базовой схемы, будем считать, что абонент А зашифровывает сообщение $s \in \mathbb{Z}_m$. Для зашифрования абонент А выполняет шаги 1–3 базовой схемы (см. п. 1.1), а последний шаг выполняется следующим образом:

4) С использованием секретного ключа цифровой подписи d_A абонент А вычисляет цифровую подпись $\mathrm{sign}(d_A, s)$ под сообщением s и формирует сообщение

$$M = t||(x_W, y_W)||\,\mathrm{sign}(d_A, s).$$

Сообщение M является шифртекстом, который отправляется абоненту Б.

Длина открытого текста s равна $\log_2 m$ бит, а длина соответствующего ему шифртекста M равна $\log_2 m + 2\log_2 p + z$ бит, где z — размер цифровой подписи.

При получении шифртекста абонент Б должен расшифровать сообщение s и, используя открытый ключ e_A абонента А, проверить цифровую подпись. Если подпись верна, то абонент Б принимает решение о корректном расшифровании сообщения s.

В заключение отметим, что при неизвестном нарушителю значении S схема с аутентификацией отправителя сообщения может быть модифицирована для передачи цифровой подписи в зашифрованном виде так, как это было сделано в предыдущем пункте.

3.3. Вариант с шифрованием длинных сообщений

Изложенная базовая схема, а также два её варианта предназначены для шифрования сообщений короткой длины. Следующий вариант позволяет зашифровывать более длинные сообщения. Для его реализации отправитель и получатель сообщения, помимо определённых в п. 1.1 открытых параметров, должны иметь отображение $g : \mathbb{F}_q^* \to \mathbb{F}_q^*$, которое также может быть известно нарушителю.

Пусть абонент А хочет зашифровать сообщение, представленное в виде конечной последовательности $s_1, \ldots, s_l \in \mathbb{Z}_m$ при $l \geqslant 2$. Для его зашифрования абонент выполняет следующие шаги:

1. Вычисляет случайное целое число k_0, удовлетворяющее неравенствам $0<k_0<q$.
2. Вычисляет точку $W = [k_0]P$, где $W = (x_W, y_W)$.
3. Для всех индексов i от 1 до l:
   а) вычисляет значение $k_i = g(k_{i-1}) \in \mathbb{F}_q^*$;
   б) вычисляет точку $U_i = [k_i]Y$, $U_i = (x_{U_i}, y_{U_i})$ и, используя (2), определяет параметры $\alpha, \beta \in \mathbb{F}_p$;
   в) определяет $t_i \equiv f(\alpha, y_{U_i})s_i + h(\alpha, \beta, y_{U_i}) \pmod m$.
4. Определяет ключ $d_U = \mathrm{kdf}(x_{U_1}, S)$, затем вычисляет код целостности $\mathrm{mac}(d_U, s_1||\cdots||s_l)$ и формирует сообщение

$$M = t_1||\cdots||t_l||(x_W, y_W)||\,\mathrm{mac}(d_U, s_1||\cdots||s_l).$$

Сообщение M является шифртекстом, который отправляется абоненту Б.

В данном варианте длина открытого текста s равна $l\log_2 m$ бит, а длина соответствующего ему шифртекста M равна $l\log_2 m + 2\log_2 p + \log_2 r$ бит.

Легко видеть, что этот вариант схемы асимметричного шифрования представляет собой последовательность из l зашифрований в соответствии с базовой схемой; мы лишь минимизировали объём передаваемых данных за счёт использования отображения g, порождающего последовательность разовых ключей.

Надо добавить, что допустимый объём данных, зашифровываемый изложенным вариантом схемы, существенно зависит от свойств отображения g. Поскольку оно действует на конечном множестве из $q-1$ элементов, то оно порождает циклические последовательности разовых ключей, что, как говорилось в п. 2.4, является небезопасным.

Пусть τ — минимальная длина цикла последовательности, порождаемой отображением g, а λ — минимальная длина подхода к циклу. Тогда для каждого уникального значения k количество блоков открытого текста l должно удовлетворять неравенству $l < \lambda + \tau$.

3.4. Вариант со случайным многочленом

Базовая схема асимметричного шифрования допускает ещё одно обобщение, использующее геометрические особенности схемы и позволяющее зашифровывать более

длинные сообщения. Действительно, в базовой схеме для зашифрования используется случайная прямая, задаваемая сравнением (3). Однако можно использовать для зашифрования случайный многочлен некоторой заранее фиксированной степени l.

Рассмотрим этот процесс более детально. Будем считать, что абонентам А и Б известна не одна общая точка S, а некоторый набор точек $S_1, \ldots, S_l \in \mathcal{E}$, для которых выполнено условие

$$S_i \neq [\pm]S_j, \quad 1 \leqslant i < j \leqslant l, \quad l \geqslant 2.$$

Будем предполагать, что данный набор точек является известным не только абонентам, участвующим в передаче сообщения, но и нарушителю.

Будем считать, что абонент А, как и в схеме, описанной в п. 3.2, обладает парой персональных ключей — открытым ключом e_A и секретным ключом d_A цифровой подписи. Тогда для зашифрования последовательности сообщений $s_1, \ldots, s_l \in \mathbb{Z}_m$ абонент А выполняет следующие шаги:

1) Вычисляет случайное целое число k, удовлетворяющее неравенствам $0 < k < q$.
2) Вычисляет точку $S_{l+1} = [k]Y$ эллиптической кривой $\mathcal{E}$. Если найдётся индекс $i \in \{1, \ldots, l\}$, такой, что $S_{l+1} = [\pm]S_i$, то абонент возвращается на шаг 1.
3) Строит интерполяционный многочлен [12]

$$g(x) \equiv \sum_{i=1}^{l+1} y_{S_i} \prod_{j \neq i} \frac{x - x_{S_j}}{x_{S_i} - x_{S_j}} \pmod m, \ \deg g(x) = l, \ g(x) \in \mathbb{Z}_m[x].$$

   Если коэффициент при старшем мономе многочлена $g(x)$ не взаимно прост с модулем m, то абонент возвращается на шаг 1.
4) Для каждого $i = 1, \ldots, l$ вычисляет произвольный вычет $t_i \in \mathbb{Z}_m$, удовлетворяющий сравнению

$$g(t_i) \equiv s_i \pmod m.$$

5) Вычисляет точку $W = [k]P$, где $W = (x_W, y_W)$.
6) Используя свой секретный ключ d_A, вычисляет цифровую подпись $\operatorname{sign}(d_A, s_1 || \cdots || s_l)$ и формирует сообщение

$$M = t_1 || \cdots || t_l || (x_W, y_W) || \operatorname{sign}(d_A, s_1 || \cdots || s_l).$$

   Сообщение M является шифртекстом, который отправляется абоненту Б.

Длина открытого текста равна $l \log_2 m$ бит, а длина соответствующего ему шифртекста M равна $l \log_2 m + 2 \log_2 p + z$ бит, где z — размер цифровой подписи.

Легко видеть, что на 3-м шаге алгоритма зашифрования абонент А вычисляет случайный многочлен $g(x) \in \mathbb{Z}_m[x]$ степени l, коэффициенты которого определяются по $l + 1$ точкам эллиптической кривой $\mathcal{E}$. При этом, как и в базовой схеме, открытый текст s_i есть абсцисса некоторой точки, принадлежащей многочлену $g(x)$, а шифртекст t_i — ордината этой точки.

Основная алгоритмическая сложность при реализации данной схемы на практике заключается в вычислении на 4-м шаге алгоритма зашифрования значений шифртекстов $t_1, \ldots, t_l$ — корней многочленов вида $g(x) - s_i \in \mathbb{Z}_m[x]$, $i = 1, \ldots, l$. Для нахождения корней можно использовать вероятностный алгоритм [13, § 6.6].

4. Результаты практической реализации

Для оценки возможности эффективной реализации предложенной базовой схемы написана программа на языке C++. Эксперименты проводились на персональной ЭВМ

с процессором AMD A6-3410MX с тактовой частотой 1,6 МГц. Результаты вычислений сведены в таблицу.

Размер p	512	1024	2048	4096	8192
Величина n	1024	2048	4096	8192	16384
Скорость, байт/с	5418	1809	628	204	80

Размеры простых чисел p приведены в битах, параметр n определяет длину блока шифруемых данных $m = 2^n$, скорость зашифрования — среднее значение объёма информации (в байтах), зашифрованной в течение одной секунды.

Из приведённых результатов видно, что максимальная скорость шифрования предложенной базовой схемой существенно ниже скорости шифрования симметричными алгоритмами шифрования. Кроме того, увеличение длины блока шифруемых данных приводит к снижению скорости шифрования.

ЛИТЕРАТУРА

1. *Menezes A. J., van Oorschot P. C., and Vanstone S. A.* Handbook of Applied Cryptography. CRC Press, 1996. 816 p.
2. ISO/IEC 18033-2:2006. Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers. 2006.
3. ISO/IEC 9797-2:2011. Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function. 2011.
4. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. М.: Стандартинформ, 2015.
5. Рекомендации по стандартизации. Использование криптографических алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012. М.: Технический комитет 26 «Криптографическая защита информации», 2014.
6. *Bellare M., Desai A., Pointcheval D., and Rogaway P.* Relations among notions of security for public-key encryption schemes // Crypto'98. LNCS. 1998. V. 1462. P. 26–46.
7. *Nesterenko A. Yu.* Cycle detection algorithms and their applications // J. Math. Sci. 2012. V. 182. No. 4. P. 518–526.
8. *Blake I., Seroussi G., and Smart N.* Elliptic Curves in Cryptography. Cambridge University Press, 1999.
9. *Mao W.* Modern Cryptography: Theory and Practice. Prentice Hall PTR, 2003. 648 p.
10. *Аносов В. Д., Нестеренко А. Ю.* Схема асимметричного шифрования, основанная на отечественных криптографических примитивах // Материалы IX Междунар. конф. «Интеллектуальные системы и компьютерные науки» (23–27 окт. 2006 г.). Т. 1. Ч. 1. М.: МГУ, 2006. С. 45–47.
11. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Стандартинформ, 2013.
12. *Бахвалов Н. С., Жидков Н. П., Кобельков Г. М.* Численные методы. М.: Наука, 1987.
13. *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003. 328 с.

REFERENCES

1. *Menezes A. J., van Oorschot P. C., and Vanstone S. A.* Handbook of Applied Cryptography. CRC Press, 1996. 816 p.

2. ISO/IEC 18033-2:2006. Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers. 2006.
3. ISO/IEC 9797-2:2011. Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function. 2011.
4. GOST R 34.13-2015. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Rezhimy raboty blochnykh shifrov [Information technology. Cryptographic protection of information. Operating modes of block ciphers]. Moscow, Standartinform, 2015. (in Russian)
5. Rekomendatsii po standartizatsii. Ispol'zovanie kriptograficheskikh algoritmov, soputstvuyushchikh primeneniyu standartov GOST R 34.10-2012 i GOST R 34.11-2012 [Recommendations for standardization. The use of cryptographic algorithms, concomitant use of GOST R 34.10-2012 and GOST R 34.11-2012]. Moscow, Technical Committee 26, 2014. (in Russian)
6. *Bellare M., Desai A., Pointcheval D., and Rogaway P.* Relations among notions of security for public-key encryption schemes. Crypto'98, LNCS, 1998, vol. 1462, pp. 26–46.
7. *Nesterenko A. Yu.* Cycle detection algorithms and their applications. J. Math. Sci., 2012, vol. 182, no. 4, pp. 518–526.
8. *Blake I., Seroussi G., and Smart N.* Elliptic Curves in Cryptography. Cambridge University Press, 1999.
9. *Mao W.* Modern Cryptography: Theory and Practice. Prentice Hall PTR, 2003. 648 p.
10. *Anosov V. D., Nesterenko A. Yu.* Skhema asimmetrichnogo shifrovaniya, osnovannaya na otechestvennykh kriptograficheskikh primitivakh [Asymmetric encryption scheme based on domestic cryptographic primitives]. Proc. IX Mezhdunar. konf. «Intellektual'nye sistemy i komp'yuternye nauki», vol. 1, part 1. Moscow, MSU Publ., 2006, pp. 45–47. (in Russian)
11. GOST R 34.10-2012. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Protsessy formirovaniya i proverki elektronnoy tsifrovoy podpisi [Information technology. Cryptographic protection of information. The formation and checking of digital signature]. Moscow, Standartinform, 2013. (in Russian)
12. *Bakhvalov N. S., Zhidkov N. P., Kobel'kov G. M.* Chislennye metody [Numerical Methods]. Moscow, Nauka Publ., 1987. (in Russian)
13. *Vasilenko O. N.* Teoretiko-chislovye algoritmy v kriptografii [Number-Theoretical Algorithms in Cryptography]. Moscow, MCCME Publ., 2003. 328 p. (in Russian)