УДК 003.26.09
doi:10.15217/issn1684-8853.2016.3.79

ШИФРОВАНИЕ ПРИ ПОМОЩИ СПАРИВАНИЯ

А. Ю. Абрамов[a, 1], *аспирант*
Е. С. Востокова[б, 1], *аспирант*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ*
[б]*Санкт-Петербургский государственный университет, Санкт-Петербург, РФ*

Постановка проблемы: *исследование математических задач, лежащих в основе современных криптосистем с открытым ключом, привело к значительному увеличению длин ключей и, как следствие, повышению вычислительной сложности операций шифрования и расшифрования.* ***Цель:*** *создание криптосистем, основанных на новых математических задачах, вычислительная эффективность процедур шифрования и расшифрования, а также криптографическая стойкость которых были бы выше, чем у существующих систем.* ***Результаты:*** *доказана возможность создания криптосистем на основе билинейного спаривания и приведены примеры таких систем, построенных на задачах факторизации больших чисел и дискретного логарифмирования. Сущность данного подхода состоит в увеличении скорости шифрования и расшифрования сообщений с использованием спаривания в локальных полях и в надежности полученных систем. Криптоанализ систем показал, что обе системы устойчивы к прямым атакам, а именно к поиску простых сомножителей для разложения (факторизации) при использовании достаточно больших ключей, длиной не менее 2048.* ***Практическая значимость:*** *разработанные криптографические системы могут быть использованы в приложениях, для защиты программного обеспечения и в системах электронной подписи.*

Ключевые слова *— криптография с открытым ключом, билинейное спаривание, числа Вифериха.*

Введение

После появления работы Диффи и Хеллмана, в которой были сформулированы основные принципы криптографии с открытым ключом, начался поиск так называемых «функций с закрытыми дверями», при помощи которых можно было бы строить асимметричные криптосистемы. Пусть C — некоторое функциональное преобразование, ставящее в соответствие сообщению m из множества допустимых сообщений шифротекст $u=C(m)$, тогда если не существует обратной функции к C (т. е., имея u, невозможно восстановить m), то такая функция C называется односторонней. Однако понятно, что использовать такую функцию для шифрования невозможно, так как даже легальный пользователь не сможет восстановить исходное сообщение по шифротексту. Допустим, что C^{-1} существует, но для его нахождения требуется знать дополнительный параметр k. Функция, обладающая таким свойством, называется функцией с закрытыми дверями, и с ее использованием становится возможным строить криптосистемы с открытым ключом. Легальный пользователь, используя секретный ключ k, может вычислить $m=C^{-1}(u, k)$ и таким образом восстановить исходное сообщение, а нелегальный должен найти неизвестный ему ключ k. Таким образом, появилась задача поиска функции с закрытыми дверями, которая бы обеспечивала наиболее вычислительно «простое» шифрование и расшифрование информации и наибольшую криптографическую стойкость при заданном размере ключа.

На данный момент сформулировано два основных подхода к построению таких функций: один основан на задачах из области теории чисел (криптосистемы RSA [1], El-Gamal [2], Koblitz [3], Miller [4]), а другой — на задаче декодирования кода, исправляющего ошибки (McEliece [5], Krouk [6]).

Появление каждой системы асимметричной криптографии приводило к развитию техник решения той «сложной» задачи, которая лежала в ее основе. В результате появились новые алгоритмы факторизации чисел и поиска дискретного логарифма: ρ- и χ-методы Полларда, общий метод решения числового поля, новые алгоритмы декодирования линейных кодов [7–9]. Однако ни про задачу дискретного логарифмирования, ни про задачу факторизации не доказано, что они принадлежат классу NP-полных задач, т. е. тех задач, которые принято считать вычислительно трудными. Кроме того, существуют алгоритмы решения этих задач для квантовых компьютеров, имеющие полиномиальную сложность.

Совокупность вышеозначенных соображений приводит к необходимости продолжать поиск новых трудноразрешимых задач в области теории чисел, на основе которых можно строить системы шифрования.

[1] Научный руководитель — профессор, доктор технических наук, проректор по науке, директор Института информационных систем и защиты информации, заведующий кафедрой безопасности информационных систем Санкт-Петербургского государственного университета аэрокосмического приборостроения *Е. А. Крук*.

Общие принципы спаривания

В данной статье рассматривается математический аппарат билинейного спаривания и описывается подход, позволяющий использовать его для построения систем асимметричного шифрования. В последнее десятилетие этот подход применяли для построения протоколов аутентификациии обмена ключами, цифровой подписи с использованием пользовательской информации [10–14] и др. Для построения криптосистемы на спаривании в общем случае требуется построить две группы и шифрующее отображение из пары элементов одной группы в элемент другой. Тогда элементами одной группы являются сообщения, другой — шифротексты, а закрытым ключом является обратное преобразование. Опишем предложенный подход более формально. Пусть заданы две группы G_1 и G_2, имеющие простой порядок q, и имеется отображение

$$e: G_1 \times G_1 \to G_2.$$

Будем обозначать элементы G_1как P, Q и считать, что $aP = \underbrace{P + P + \ldots + P}_{a}$. Тогда отображениям, которые могут быть эффективно использованы для построения криптосистем, присущи следующие свойства:

1) билинейность: $\forall P, Q \in G_1, \ \forall a,$

$$b \in \mathbb{Z}_q^* \ e(aP, bQ) = e(P, Q)^{ab};$$

2) невырожденность: $P \neq 0 \Rightarrow e(P, P) \neq 1$;

3) вычислимость — должен существовать эффективный алгоритм вычисления e.

Известны примеры отображений, которые удовлетворяют вышеперечисленным свойствам, — спаривания Вейля и Тейта, и на их основе построены криптосистемы, перечисленные выше. Очевидно, что для взлома такой системы злоумышленнику придется решать задачу нахождения дискретного логарифма, когда $Q = aP$ и требуется найти a при известных P и Q. При определенном выборе групп G_1, G_2 для решения этой задачи может не оказаться известных алгоритмов, которые были бы быстрее полного перебора. Понятно, что решить задачу дискретного логарифма в G_1 не сложнее, чем в G_2. Пусть

$$e(P, Q) = e(P, aP) = e(P, P)^a,$$

тогда

$$P' = e(P, P), \ Q' = e(P, Q)$$

и a может быть найдено в группе G_2 как $\log_p(Q')$. А сама задача Диффи — Хеллмана в группе решается вычислительно просто. Она заключается в различении двух наборов

$$<P, aP, bP, C = cP> \text{ и } <P, aP, bP, C = abP>$$

при неизвестных a, b. Действительно, если вычислить

$$v_1 = <aP, bP>, \ v_2 = <P, C>$$

и окажется, что $v_1 = v_2$, то заданный набор принадлежит типу $<P, aP, bP, abP>$:

$$e(aP, bP) = e(P, P)^{ab} = e(P, abP) = e(P, C).$$

Таким образом, если известно отображение e, то решение данной задачи требует меньшей сложности.

Настоящая статья описывает новый подход, состоящий в использовании спаривания для построения криптосистем асимметричного шифрования. Это становится возможным благодаря применению аппарата чисел Вифериха.

Билинейное спаривание и числа Вифериха

Опишем необходимую для построения криптосистем теоретическую информацию об аппарате спариваний и числах Вифериха. Пусть p — простое нечетное число, N^+ — полугруппа натуральных чисел по сложению, а $Z^{(p)}$ — полугруппа целых взаимно простых с p чисел по умножению. Рассмотрим функцию, обратную к функции Артина — Хассе:

$$l(a) = \frac{1}{p}\log a^{p-1}, \ a \in \mathbb{Z}^{(p)}.$$

Тогда из свойств логарифма следует, что

$$l(ab) = \frac{1}{p}\log(ab)^{p-1} = \frac{1}{p}\log a^{p-1} + \frac{1}{p}\log b^{p-1} = l(a) + l(b), a, b \in \mathbb{Z}^{(p)}. \quad (1)$$

Определение. Пусть p — простое число. Число a, взаимно простое с p, будем называть числом Вифериха, если выполнено условие

$$a^{p-1} \equiv 1 \bmod p^2. \quad (2)$$

В противном случае число a будем называть антивифериховым, т. е. выполняется

$$a^{p-1} \neq 1 \bmod p^2. \quad (3)$$

Лемма 1. Если $a \equiv b \bmod p^2$, то $l(a) \equiv l(b) \bmod p$.

Доказательство: Пусть $a = b + p^2k$, тогда

$$l(a) = l\left(b + p^2k\right) = \frac{1}{p}\log\left(\left(b + p^2k\right)^{p-1}\right) = \frac{1}{p}\log\left(1 + \frac{\left(b + p^2k\right)^{p-1} - 1}{p}p\right) \equiv \frac{\left(b + p^2k\right)^{p-1} - 1}{p} \equiv \frac{b^{p-1} - 1}{p} \equiv l(b) \bmod p.$$

Определение. Будем называть спариванием отображение следующего вида:

$$<,>_p : \mathbb{Z}^{(p)} \times \mathbb{N}^+ \to \mathbb{Z}/p\mathbb{Z},$$
$$<a, n>_p = l(a)n \bmod p.$$

Лемма 2. Спаривание $<,>_p$ билинейно и невырождено по первому аргументу для антивифериховых чисел.

Доказательство:

1. Линейность по первому аргументу следует из равенства (1). Линейность по второму аргументу очевидна.

2. Невырожденность. Проверим сначала, что если a не является числом Вифериха, то

$$l(a) \neq 0 \bmod p.$$

Действительно:

$$l(a) = \frac{1}{p}\log a^{p-1} = \frac{1}{p}\log\left(1 + \frac{a^{p-1}-1}{p}\right) =$$
$$= \frac{1}{p}\left(\frac{a^{p-1}-1}{p}p - \left(\frac{a^{p-1}-1}{p}p\right)^2 + \ldots\right) \equiv \frac{a^{p-1}-1}{p} \not\equiv 0 \bmod p,$$

поэтому разрешимо сравнение

$$l(a)n = 1 \bmod p,$$

откуда следует, что

$$<a, n>_p = 1. \quad (4)$$

Лемма 3. Если $a \equiv b \bmod p^2$, то

$$<a, n>_p = <b, n>_p . \quad (5)$$

Доказательство: Из леммы 1 следует, что $l(a) \equiv l(b) \bmod p$. Тогда равенство (5) получается непосредственно из определения.

Лемма 4. Пусть p, q_1, q_2, ..., q_r — различные простые числа. Тогда найдется целое число c, которое будет антивифериховым для числа p и вифериховым для q_1, q_2, ..., q_r.

Доказательство: Построим сначала антивифериково число a для простого p. Если a является таковым, то процесс построения окончен, иначе возьмем $a' = a + p$. Тогда $a^{p-1} \equiv 1 \bmod p^2$ и

$$(a')^{p-1} - 1 = (a+p)^{p-1} - 1 \equiv$$
$$\equiv (a^{p-1} - 1) + (p-1)a^{p-2}p \equiv -a^{p-2}p \neq 0 \bmod p^2,$$

и значит a' будет антивифериховым для p.

Построим теперь, исходя из числа a', число c, которое будет вифериховым для q_1, q_2, ..., q_r и останется антивифериховым для p.

Шаг 1. Если a' является вифериховым для q_1, то $c = a'$, и переходим к следующему шагу. В противном случае рассмотрим

$$c_1 = a' + p^2 q_1 x$$

и будем искать x такое, чтобы

$$c_1^{p-1} \equiv 1 \bmod q_1^2.$$

Для этого получим относительно x сравнение первой степени по модулю q_1:

$$c_1^{q_1-1} - 1 \equiv (a')^{q_1-1} - 1 + (q_1 - 1)(a')^{q_1-2}p^2 q_1 x \equiv$$
$$\equiv (a')^{q_1-1} - 1 - (a')q_1 - 2p^2 q_1 x \bmod q_1^2.$$

Отсюда получаем сравнение для x:

$$(a')^{q_1-2}p^2 x \equiv \frac{(a')^{q_1-1}-1}{q_1} \bmod q_1,$$

решая которое получаем искомое число c_1.

Заметим, что $c_1 \equiv a' \bmod p^2$, поэтому оно останется антивифериховым для p.

Шаг 2. Если c_1 будет вифериховым для q_2, то переходим к следующему шагу и далее. В противном случае рассмотрим

$$c_2 = c_1 + p^2 q_1^2 q_2 x.$$

Здесь $c_2 \equiv c_1 \bmod p^2$ и $c_2 \equiv c_1 \bmod q_1^2$, следовательно, c_2 будет антивифериховым для p и вифериховым для q_1. Чтобы c_2 стало вифериховым для q_2, решаем сравнение

$$c_2^{q_2-1} - 1 \equiv \left(c_2^{q_2-1} - 1\right) + (q_2 - 1)c_2^{q_2-2}p^2 q_1^2 q_2 x \equiv$$
$$\equiv \left(c_2^{q_2-1} - 1\right) + c_2^{q_2-2}p^2 q_1^2 q_2 x \bmod q_2^2.$$

Отсюда получаем сравнение для x:

$$bx \equiv \frac{c_2^{q_2-1}-1}{q_2} \bmod q_2,$$

где $b = c_2^{q_2-2}p^2 q_1^2$ — взаимно простое с q_2 число.

Решая последнее сравнение, получим c_2. Продолжая процесс, получим искомое число c, удовлетворяющее условию леммы.

Из формулы (1) и определения спаривания можно получить

$$<a, n> = l(a)n \equiv \frac{a^{p-1}-1}{p} n \bmod p.$$

Поскольку $\frac{a^{p-1}-1}{p} \not\equiv 0 \bmod p$, то это сравнение имеет единственное решение, равное n. Докажем теперь еще одно свойство, которое используется в построении криптосистемы и является ключевым в расшифровании информации.

Лемма 5. Если $a \equiv b \bmod p^2$, то $l(a) \equiv l(b) \bmod p$.

Доказательство: По условию, $b = a + p^2 c$, следовательно:

$$l(b) \equiv \frac{b^{p-1}-1}{p} \equiv \frac{(a+p^2c)^{p-1}-1}{p} \equiv \frac{a^{p-1}-1}{p} \equiv$$
$$\equiv l(a) \bmod p.$$

На основании представленных доказательств построены две новые криптографические системы с открытым ключом, использующие билинейное спаривание и числа Вифериха.

Примеры криптосистем на спаривании

Криптосистема 1. В этом случае в качестве групп G_1 и G_2 рассматриваем, соответственно, группы $Z^{(p)} \times N^+$ и Z/pZ.

1. *Генерация ключей.* Пусть p, $q < p$ — простые числа и $m = pq$. Возьмем число $a \in Z$, удовлетворяющее условию

$$\frac{a^{p-1}-1}{p} \not\equiv 0 \bmod p.$$

Найдем натуральное число n, решая сравнение

$$\frac{a^{p-1}-1}{p} n \equiv 1 \bmod p.$$

Закрытый ключ: (p, q, n).

Открытый ключ: (a, m).

2. *Шифрование.* Пусть число M — информационное сообщение, и $M < \sqrt{m}$. Тогда шифротекст r может быть получен следующим образом:

$$r \equiv a^M \bmod m^2.$$

3. *Расшифрование.* Чтобы восстановить сообщение M, требуется вычислить

$$M = \frac{r^{p-1}-1}{p} n \bmod p.$$

4. *Корректность.* Из того, как осуществляется шифрование, и того, что $p|m$, следует, что $r \equiv a^M \bmod p^2$. Тогда по лемме 3 и равенству (5) получаем

$$<r, n>_p = <a^M, n>_p = M<a, n>_p = M.$$

При расшифровании мы решаем задачу во второй группе с уже известными нам из закрытого ключа числами n и p, в то время как злоумышленнику они неизвестны. Найти число n без знания p не представляется возможным, а поиск числа p является трудноразрешимой задачей факторизации. Однако, зная p, получить n можно довольно просто путем решения соответствующего сравнения.

Криптосистема 2. Здесь в роли групп G_1 и G_2 выступают те же самые группы, что и в предыдущем примере, а именно $Z^{(p)} \times N^+$ и Z/pZ.

1. *Генерация ключей.* Зафиксируем некоторое число m и выберем произвольное s: $2 \le s \le m$. Выберем $N = pq_1 \ldots q_{s-1}$, a — число Вифериха для всех q_i и антивиферихово для p, т. е.

$$a^{p-1} \not\equiv 1 \bmod p^2, a^{q_i-1} \equiv 1 \bmod q_i^2.$$

Обозначим $b = \frac{a^{p-1}-1}{p}$ и найдем n как решение сравнения

$$b(1 + pb + p^2b^2 + \ldots + p^{s-1}b^{s-1})n \equiv 1 \bmod p^2.$$

Открытый ключ: (m, N, a).

Закрытый ключ: $(n, p, q_1, \ldots, q_{s-1})$.

2. *Шифрование.* Пусть число M — информационное сообщение, и $M < N$. Тогда шифротекст r может быть получен следующим образом:

$$r \equiv a^M \bmod N^m.$$

3. *Расшифрование.* Пусть $c = \frac{r^{p-1}-1}{p}$, тогда

$$c(1 + pc + \ldots + p^{s-1}c^{s-1}) \equiv M \bmod p^s.$$

Помимо задачи факторизации числа N возникает вопрос о количестве простых чисел в его разложении, т. е. необходимо после каждой итерации алгоритма факторизации проверять каждое число в полученном разложении на простоту. Также появляется дополнительная трудность в выборе из полученного набора простых чисел того числа, для которого a является антивифериховым.

Заключение

В данной работе предложен подход, позволяющий строить асимметричные системы шифрования при помощи операции спаривания на билинейных группах. Вычислительно сложной задачей в таких системах является задача дискретного логарифмирования — это несложно увидеть, опираясь на то, как осуществляется шифрование и дешифрование в системах, описанных выше. Пусть задан шифротекст r, полученный в результате шифрования информации M в системах 1 и 2:

$$r = a^M \bmod m^2 \text{ либо } r = a^M \bmod N^m.$$

Тогда атакой первого рода на эти системы будет являться поиск M как решение задачи дискретного логарифма:

$$M = \log_a r.$$

Как следствие есть основания полагать, что при выборе тех групп, между которыми определена операция спаривания таким образом, что в группе G_2 не будет существовать эффективных алгоритмов для нахождения дискретного логарифма, окажется, что такие криптосистемы в смысле размера ключей будут эффективнее, чем RSA или ElGamal. Поиск таких групп представляет значительный интерес для исследования.

Литература

1. **Rivest R., Shamir A., Adleman L.** A Method for Obtaining Digital Signatures and Public-Key Cryptosystems // Communications of the ACM. 1978. N 21(2). P. 120–126.
2. **ElGamal T.** A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Transactions on Information Theory. 1985. N 31(4). P. 469–472.
3. **Koblitz N.** Elliptic Curve Cryptosystems//Mathematics of Computation. 1987. Vol. 48. N 177. P. 203–209.
4. **Miller V.** Use of Elliptic Curves in Cryptography // Advances in Cryptology — CRYPTO'85. 1985. N 85. P. 417–426.
5. **McEliece R. J.** A Public-Key Cryptosystem Based on Algebraic Coding Theory // DSN Progress Report. 1978. N 114. P. 42–44.
6. **Krouk E.** A New Public Key Cryptosystem//Proc. of Sixth Joint Swedish-Russian International Workshop on Information Theory, Moelle, Sweden. 1993. P. 285–286.
7. **Barg A., Krouk E. A.** and **van Tilborg H. C. A.** On the Complexity of Minimum Distance Decoding of Long Linear Codes // IEEE Transactions on Information Theory. 1999. N 45. P. 1392–1405.
8. **Finiasz M., Sendrier N.** Security Bounds for the Design of Code-based Cryptosystems // Cryptology ePrint Archive. IACR. 2009. P. 414.
9. **Becker A., Joux A., May A., Meurer A.** Decoding Random Binary Linear Codes in $2^{n/20}$: How $1 + 1 = 0$ Improves Information Set Decoding // Advances in Cryptology — Eurocrypt 2012. Lecture Notes in Computer Science. Springer-Verlag, 2012.
10. **Yuan Q., Li S.** A New Efficient ID-based Authenticated Key Agreement Protocol // Cryptology ePrint Archive. Report. 2005. P. 309.
11. **Shim K.** Effient ID-based Authenticated Key Agreement Protocol Based on the Weil Pairing // Electronics Letters. 2003. N 39(8). P. 653–654.
12. **Chen L., Kudla C.** Identity Based Authenticated Key Agreement Protocols from Pairings // Cryptology ePrint Archive. 2002. P. 184.
13. **Boneh D.** and **Franklin M.** Identity-based Encryption from the Weil Pairing // Lecture Notes in Computer Science. 2001. N 2139. P. 213–229.
14. **Hess F.** Efficient Identity Based Signature Schemes Based on Pairings // Proc. of 9th Annual Intern. Workshop of SAC 2002, Newfoundland, Canada, Aug. 15–16. 2003. N 2595. P. 310–324.

UDC 003.26.09
doi:10.15217/issn1684-8853.2016.3.79

Encryption by Paring

Abramov A. Y.[a], Post-Graduate Student, hexxyg@gmail.com
E. S. Vostokova[b], Post-Graduate Student, lizk.vostokova@gmail.com
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation
[b]Saint-Petersburg State University, 7/9, Universitetskaya Nab., 199034, Saint-Petersburg, Russian Federation

Introduction: Studying the mathematical problems which underlie modern public-key cryptosystems has led to a significant increase in the lengths of the keys and, consequently, to an increase in the computational complexity of encryption and decryption. **Purpose:** The goal is to create cryptosystems based on new mathematical challenges which would have more computationally efficient encryption and decryption, and cryptographic resistance higher than that of the existing systems. **Results:** We proved that it is possible to create cryptosystems based on bilinear pairing, and gave examples of such systems based on large integer factorization and on discrete logarithms. The essence of this approach is to increase the speed of encryption and decryption of messages using pairing in local fields, with a high reliability of the obtained systems. Cryptanalysis of the proposed systems showed that the complexity of compromising either of them is equivalent to the complexity of compromising RSA cryptosystem as these systems are based on the same computationally hard problem. **Practical relevance:** The developed cryptographic systems can be used in applications for protecting software or in electronic signature systems.

Keywords — Public-Key Cryptography, Bilinear Pairing, Wieferich Prime.

References

1. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 1978, no. 21(2), pp. 120–126.
2. ElGamal T. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, 1985, no. 31(4), pp. 469–472.
3. Koblitz N. Elliptic Curve Cryptosystems. *Mathematics of Computation*, 1987, vol. 48, no. 177, pp. 203–209.
4. Miller V. Use of Elliptic Curves in Cryptography. *Advances in Cryptology. CRYPTO*, 1985, no. 85, pp. 417–426.
5. McEliece R. J. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *DSN Progress Report*, 1978, no. 114, pp. 42–44.
6. Krouk E. A New Public Key Cryptosystem. *Proc. of Sixth Joint Swedish-Russian Inter. Workshop on Information Theory*, Moelle, Sweden, 1993, pp. 285–286.
7. Barg A., Krouk E. A. and van Tilborg H. C. A. On the Complexity of Minimum Distance Decoding of Long Linear Codes. *IEEE Transactions on Information Theory*, 1999, no. 45, pp. 1392–1405.

8. Finiasz M., Sendrier N. Security Bounds for the Design of Code-based Cryptosystems. *Cryptology ePrint Archive. IACR*, 2009, p. 414.
9. Becker A., Joux A., May A., Meurer A. Decoding Random Binary Linear Codes in $2^{n/20}$: How 1+1=0 Improves Information Set Decoding. *Advances in Cryptology — Eurocrypt 2012. Lecture Notes in Computer Science*, Springer-Verlag, 2012.
10. Yuan Q., Li S. A New Efficient ID-based Authenticated Key Agreement Protocol. *Cryptology ePrint Archive. Report*, 2005, p. 309.
11. Shim K. Effient ID-based Authenticated Key Agreement Protocol Based on the Weil Pairing. *Electronics Letters*, 2003, no. 39(8), pp. 653–654.
12. Chen L., Kudla C. Identity Based Authenticated Key Agreement Protocols from Pairings. *Cryptology ePrint Archive*, 2002, p. 184.
13. Boneh D. and Franklin M. Identity-based Encryption from the Weil Pairing. *Lecture Notes in Computer Science*, 2001, no. 2139, pp. 213–229.
14. Hess F. Efficient Identity Based Signature Schemes Based on Pairings. *Proc. of 9th Annual Intern. Workshop of SAC 2002*, 2003, no. 2595, pp. 310–324.

ПАМЯТКА ДЛЯ АВТОРОВ

Поступающие в редакцию статьи проходят обязательное рецензирование.

При наличии положительной рецензии статья рассматривается редакционной коллегией. Принятая в печать статья направляется автору для согласования редакторских правок. После согласования автор представляет в редакцию окончательный вариант текста статьи.

Процедуры согласования текста статьи могут осуществляться как непосредственно в редакции, так и по e-mail (ius.spb@gmail.com).

При отклонении статьи редакция представляет автору мотивированное заключение и рецензию, при необходимости доработать статью — рецензию. Рукописи не возвращаются.

Редакция журнала напоминает, что ответственность за достоверность и точность рекламных материалов несут рекламодатели.