УДК 519.7

В.Г. Ланских[1], Ю.В. Ланских[2]

[1]Вятский государственный технический университет,
Киров, Россия
[2]Пермский государственный национальный исследовательский университет,
Пермь, Россия

МЕТОДЫ ВЫБОРА ПАРАМЕТРОВ СТАНДАРТНОГО АЛГОРИТМА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Описывается стандартный алгоритм электронной цифровой подписи, основанный на операциях над эллиптической кривой в конечном поле. Описываются последовательность действий, выполняемых при формировании электронной цифровой подписи, и последовательность действий, выполняемых при ее верификации. Рассматриваются основные параметры алгоритма электронной цифровой подписи, представляющие собой большие простые числа. Стандарт определяет только математические формулы для операций над эллиптической кривой и предлагает нижние границы для некоторых параметров, не устанавливая каких-либо конкретных алгоритмов выполнения этих операций. Ставится задача выбора параметра алгоритма формирования и верификации электронной цифровой подписи как задача выбора псевдослучайного простого числа большой размерности из широкого диапазона с последующей проверкой того, что выбранное число является простым. Указывается на то, что верхние границы параметров определяются в основном тремя факторами, к которым относятся требуемый уровень безопасности, допустимое время формирования и верификации электронной цифровой подписи и используемая аппаратная платформа. Рассматриваются способы формирования простых чисел. Анализируются достоинства и недостатки различных алгоритмов проверки сформированных чисел на простоту, включая тест, основанный на малой теореме Ферма, тест Соловея–Штрассена и тест Миллера–Рабина. Из анализа делается вывод о том, что более предпочтительным для поиска больших простых чисел представляется использование теста Миллера–Рабина, который по сравнению с тестом Соловея–Штрассена имеет меньшую вычислительную сложность и большую точность, хотя и обладает недостатком, состоящим в том, что он пропускает числа Кармайкла, которые не являются простыми. Для практических приложений предлагается последовательность шагов формирования одного из параметров алгоритма электронной цифровой подписи. С помощью аналогичной процедуры предлагается осуществлять поиск и других параметров стандартного алгоритма формирования электронной цифровой подписи.

Ключевые слова: алгоритм электронной цифровой подписи, параметры алгоритма, псевдослучайные числа, большие простые числа, тесты простоты.

V.G. Lanskikh[1], Yu.V. Lanskikh[2]

[1]Vyatka state technical university, Kirov, Russian Federation
[2]Perm state national research university, Perm, Russian Federation

METHODS OF SELECTING ELECTRONIC DIGITAL SIGNATURE STANDARD ALGORITHM PARAMETERS

A standard algorithm, based on operations on an elliptic curve in a finite field, for electronic digital signature is described. Describes the sequence of actions performed in the formation of an electronic digital signature and the sequence of actions performed during its verification. The main parameters of the electronic digital signature algorithm, which are large prime numbers, are considered. The standard defines only mathematical formulas for operations on an elliptic curve and offers lower bounds for some parameters without establishing any specific algorithms for performing these operations. The task is to select the parameter of the algorithm for generating and verifying an electronic digital signature as a task of selecting a pseudorandom prime number of large dimension from a wide range with the subsequent verification that the chosen number is prime. It is pointed out that the upper limits of the parameters are determined mainly by three factors, which include the required level of security, the acceptable time of formation and verification of the electronic digital signature and the hardware platform used. Methods of forming prime numbers are considered. The advantages and disadvantages of various algorithms for checking formed numbers for simplicity are analyzed, including a test based on the small Fermat theorem, the Solovey-Strassen test, and the Miller-Rabin test. The analysis concludes that the use of the Miller-Rabin test is more preferable for the search for large prime numbers, which in comparison with the Solovey-Strassen test has less computational complexity and greater accuracy, although it has the disadvantage that it misses Carmichael numbers that are not prime. For practical applications, a sequence of steps is proposed for forming one of the parameters of an electronic digital signature algorithm. With the help of a similar procedure, it is suggested to search for other parameters of the standard algorithm for generating an electronic digital signature.

Keywords: algorithm of electronic digital signature, algorithm parameters, pseudo-random numbers, large prime numbers, simplicity tests.

Введение. Основной особенностью описанного в [1, 2] нового стандарта электронной цифровой подписи (ЭЦП) является максимальная преемственность по отношению к действовавшему стандарту. Во-первых, предлагаемая схема представляет собой тот же вариант асимметричного алгоритма, адаптированный для использования вместо операций умножения и возведения в степень в конечном поле из p элементов аналогичных операций на эллиптической кривой над этим же полем. Во-вторых, она позволяет использовать действующий стандарт функции хеширования. В-третьих, длина подписи остается без изменений. Все это существенно облегчает модификацию многочисленных существующих программных и аппаратных реализаций, определяемых действовавшим ранее стандартом.

Одним из основных параметров алгоритма ЭЦП является простое число p, представляющее собой модуль эллиптической кривой E и удовлетворяющее неравенству $p > 2^{255}$.

Следующим параметром служит упомянутая эллиптическая кривая E, задаваемая своим инвариантом $J(E)$ или коэффициентами a и b. Эллиптической кривой E, определенной над конечным простым полем $GF(p)$, называется множество пар чисел (x, y), принадлежащих этому полю и удовлетворяющих тождеству

$$y^2 = x^3 + ax + b \pmod{p}, \qquad (1)$$

где $a, b \in GF(p)$ и $4a^3 + 27b^3 \neq 0 \pmod{p}$

Инвариантом эллиптической кривой E называется величина $J(E)$, удовлетворяющая тождеству

$$J(E) = 1728\frac{4a^3}{4a^3 + 27b^3} \pmod{p}.$$

Коэффициенты a и b кривой E могут быть определены по известному инварианту $J(E)$ следующим образом:

$$a = 3k \pmod{p} \text{ и } b = 2k \pmod{p},$$

где $k = \dfrac{J(E)}{1728 - J(E)} \pmod{p}$, причем $J(E) \neq 0$ и $J(E) \neq 1728$.

Следующим параметром является целое число m, представляющее собой порядок группы точек кривой E. Пары (x, y), удовлетворяющие тождеству (1), называются точками кривой E, а x и y – координатами точки. Точки кривой E обозначим как $Q(x, y)$. Две точки равны, если равны их соответствующие координаты. На множестве точек кривой E введена операция сложения со следующими вариантами ее выполнения. Пусть координаты точек Q_1 и Q_2 удовлетворяют условию $x_1 \neq x_2$. Тогда суммой этих точек называется точка Q_3, координаты которой определяются соотношениями:

$$x_3 = \lambda^2 - x_1 - x_2 \pmod{p} \text{ и } y_3 = \lambda(x_1 - x_3) - y_1 \pmod{p},$$

где $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1} \pmod{p}$.

Если выполнены равенства $x_1 = x_2$ и $y_1 = y_2 \neq 0$, то координаты точки Q_3 определяются следующим образом: $x_3 = \lambda^2 - x_1 \pmod{p}$ и $y_3 = \lambda(x_1 - x_3) - y_1 \pmod{p}$, где

$$\lambda = \frac{3x^2 + a}{2y_1} \pmod{p}.$$

В случае, когда выполняется условие $x_1 = x_2$ и $y_1 = -y_2 \pmod{p}$, сумма точек Q_1 и Q_2 называется нулевой точкой, обозначаемой Θ, а точка Q_2 называется отрицанием точки Q_1. Относительно введенной операции сложения множество всех точек кривой E вместе с нулевой точкой Θ образует конечную коммутативную группу порядка m, для которого выполнено неравенство: $p+1-2\sqrt{p} \leq m \leq p+1+2\sqrt{p}$.

При выборе m должно быть выполнено условие: $m \neq p$.

Точка Q называется точкой кратности k для некоторой точки D, если выполняется равенство $Q = kD$.

Следующим параметром алгоритма является простое число q, представляющее собой порядок циклической подгруппы точек кривой E. При выборе q должны быть выполнены следующие условия: $m = nq$, $n \geq 1$, $2^{254} < q < 2^{256}$, $p^t \neq 1 \pmod{q}$ для всех целых $t = 1, 2, \ldots, B$ и $B \geq 31$.

Еще одним параметром алгоритма является точка $D \neq \Theta$ с координатами (x_D, y_D), удовлетворяющая равенству $qD = \Theta$..

В качестве одного из важнейших параметров алгоритма используется функция хеширования h по ГОСТ Р34.11 [3] и её возможные модификации [4, 5, 6, 7].

Каждый пользователь этой схемы ЭЦП должен обладать ключом подписи, который представляет собой целое число d, удовлетворяющее неравенству $0 < d < q$, и ключом проверки подписи, который представляет собой точку Q кривой E с координатами (x_q, y_q), удовлетворяющую равенству $Q = dD$.

Описанные параметры используются при реализации алгоритма формирования ЭЦП, который представляется в виде следующей последовательности действий:

1. С помощь функции h осуществить хеширование сообщения P и получить его хеш-значение $H = h(P)$.

2. Вычислить величину α, двоичным представлением которой является хеш-значение $H = h(P)$, и определить величину $e = \alpha \pmod q$. Если $e = 0$, то положить $e = 1$.

3. С помощью генератора псевдослучайных чисел выбрать число k, удовлетворяющее условию $0 < k < q$.

4. Вычислить точку C кривой E, удовлетворяющую условию $C = kD$. Определить величину $r = x_C \pmod q$, где x_C – x-координата точки C. Если $r = 0$, то следует выбрать новое значение k.

5. Вычислить значение $s = [rd + ke] \pmod q$. Если $s = 0$, то следует выбрать новое значение k.

6. Найти двоичные представления r и s, конкатенация которых и будет определять ЭЦП $\xi = (r \| s)$.

При наличии выбранных параметров исходными данным для алгоритма формирования ЭЦП являются подписываемое сообщение P и ключ подписи d.

Проверка или верификация ЭЦП осуществляется в следующем порядке:

1. Над принятой ЭЦП ξ^* выполнить деконкатенацию, найти числа r^* и s^*, определить выполнение условий $0 < r^* < q$ и $0 < s^* < q$. Если они не выполнены, то подпись отвергается.

2. С помощь функции h осуществить хеширование принятого сообщения P^* и получить его хеш-значение $H^* = h(P^*)$.

3. Вычислить величину α^*, двоичным представлением которой является хеш-значение H^*, и определить величину $e^* = \alpha^* \pmod q$.

4. Вычислить величину $\nu = [e^*]^{-1} \pmod q$.

5. Вычислить величины $z_1 = s\nu \pmod q$ и $z_2 = -r\nu \pmod q$.

6. Вычислить точку $C^* = z_1 D + z_2 Q$ и определить величину $R = x_{C^*} \pmod q$.

7. Если $R = r$, то подпись принимается, в противном случае она неверна.

Исходными данным для алгоритма верификации являются принятое подписанное сообщение P^*, ЭЦП ξ^* и ключ проверки Q.

Таким образом, стандарт определяет только математические формулы для операций на эллиптической кривой и предлагает нижние границы для некоторых параметров, не устанавливая каких-либо конкретных алгоритмов выполнения этих операций.

Выбор верхних границ параметров и конкретных вычислительных алгоритмов определяется в основном тремя взаимозависимыми факторами, к которым относятся требуемый уровень безопасности, допустимое время формирования и верификации ЭЦП и используемая аппаратная платформа. Так, например, нижней границей параметра p является $p > 2^{255}$. Из соображений безопасности в качестве минимальной верхней границы этого параметра целесообразно выбрать $2^{255} < p < 2^{511}$, если в указанном диапазоне разработанные вычислительные алгоритмы на применяемой аппаратной платформе выполняются за приемлемое время.

1. Постановка задачи. Анализ требований, предъявляемых стандартом к выбору параметров алгоритма формирования и верификации ЭЦП, позволяет сформулировать задачу выбора параметров в обобщенном виде как задачу выбора случайного (псевдослучайного) простого числа большой размерности из широкого диапазона. Простые числа встречаются довольно часто. Существует около 10^{151} простых чисел длиной от 1 до 512 бит включительно [8], а количество простых чисел, меньших 2^{512}, приблизительно равно 2^{503} [8].

2. Предлагаемое решение задачи. Один из способов формирования простых чисел базируется на следующей теореме [8, 9].

Пусть $p = fN + 1$, где f – нечетное простое число, N – четное число и $p < (2f + 1)^2$. Число p является простым, если выполняются два условия:

1) $2^{fN} = 1 \pmod p$;

2) $2^N \neq 1 \pmod p$.

Генерация простого числа с использованием этой теоремы осуществляется по несколько упрощенной в принятом стандарте схеме. Пусть требуется сформировать простое число p длиной $l \geq 17$ бит. С этой целью строится убывающая последовательность чисел $\{l_i\}$, где $i = 0,1,\ldots,s$, для которых $l_0 = l$, $l_i = \left[\frac{l_{i-1}}{2}\right]$. Далее последовательно

вырабатывается последовательность простых чисел $p_s, p_{s-1}, \ldots, p_0$, для всех $i = 1, \ldots, s$. Генерация простого числа p_{i-1} осуществляется с использованием следующей формулы: $p_{i-1} = p_i N + 1$, где число N удовлетворяет следующим условиям [12]: N – четное; N – такое, что длина числа $p_{i-1} = p_i N + 1$ в точности должна быть равна l_{i-1}. Число N получается с помощью генератора псевдослучайных чисел. Если полученное N нечетно, то полагают $N = N + 1$.

Число p_{i-1} считается полученным, если одновременно выполнены следующие два условия:

1) $2^{\phi} = 1 \bmod p_i$, где $\varphi = p_{i-1} N$;

2) $2^N \neq 1 \bmod p_i$.

Если хотя бы одно из условий не выполняется, то значение числа N увеличивается на 2, и вычисляется новое значение p_{i-1}, которое снова проверяется по тем же условиям. Данный процесс продолжается до тех пор, пока не будет получено простое число p_{i-1}, удовлетворяющее обоим условиям.

При выборе случайного числа из заданного диапазона предполагается, что число выбирается равновероятным образом из заданного множества чисел, если не указано другого вероятностного распределения.

Пусть η – число элементов множества, из которого требуется выбрать случайный элемент. Для того чтобы обеспечить отсутствие смещения результирующего распределения вероятностей, следует воспользоваться методом проб и ошибок, суть которого применительно к данному случаю состоит в следующем. Необходимо выбрать π, для которого $2^{\pi} \geq \eta$, и определить $\varepsilon = \left\lfloor {2^{\pi}}/{\eta} \right\rfloor$, где $\lfloor \cdots \rfloor$ – функция округления снизу, которая определяет ближайшее меньшее целое число. Далее следует выбрать ρ из множества, число элементов в котором равно $\eta\varepsilon$, и получить окончательный результат как $\rho \,(\mathrm{mod}\eta)$. Другими словами, этот метод предполагает, что для генерации равномерно распределенных случайных чисел, размер которых в битах не является степенью двух, необходимо отбросить от полученного результата несколько случайных бит, что при наличии современных генераторов псевдослучайных чисел не является проблемой.

Далее требуется определить, является ли выбранное число действительно простым.

Один из самых простых способов проверки числа p на простоту состоит в последовательном делении числа p на все нечетные числа, которые содержатся в интервале $\left[2, \sqrt{p}\right]$. Если в процессе деления получается целый результат, то число p – составное. Если же при переборе всех нечетных чисел из интервала $\left[2, \sqrt{p}\right]$ разделить число p на эти числа нацело нельзя, то число p – простое. Данный метод называется пробным делением [8]. Этот метод трудоемок по числу арифметических операций, и он используется в основном для проверки небольших простых чисел.

Другой метод, называемый решетом Эратосфена, также достаточно эффективен, но требует для реализации большого объема памяти ЭВМ, однако для составления таблиц простых чисел он является наилучшим [8]. Более того, разрабатываются специальные процессоры, на которых операции «просеивания» выполняются очень эффективно.

Малая теорема Ферма [10,11] утверждает, что если p простое число, то выполняется условие: при всех $u \in \{2,3,\ldots, p-1\}$ имеет место сравнение $u^{p-1} \equiv 1 \bmod p$. На основании этой теоремы построен вероятностный алгоритм проверки на простоту числа p.

Если для некоторого целого m из интервала [2, p] соотношение $u^{p-1} \equiv 1 \bmod p$ не выполняется, то число p – составное. Если же теорема выполняется, то вывод о том, что число p простое, сделать нельзя, так как теорема дает лишь необходимое условие. Поэтому, если для некоторого m имеет место соотношение $u^{p-1} \equiv 1 \bmod p$, то считают, что число p является псевдопростым по основанию u. Существует бесконечно много пар чисел u и p, где p – составное и псевдопростое. Вообще, для любого $m > 1$ существуют бесконечно много псевдопростых чисел по основанию m. Итак, справедливы следующие два утверждения:

– если пара (2, p) удовлетворяет сравнению $u^{p-1} \equiv 1 \bmod p$, то и пара чисел (2, $2^p - 1$) также ему удовлетворяет;

– для любого простого числа p и любого $u > 2$ такого, что $(u^2 - 1,\ p) = 1$, число $\dfrac{u^{2p}-1}{u^2-1}$ является псевдопростым по основанию u.

Составные числа p, для которых при всех основаниях выполняется сравнение $u^{p-1} \equiv 1 \bmod p$, называются числами Кармайкла [12].

Здесь уместно заметить [12], что числа Кармайкла достаточно редки. Так, существуют всего 2163 чисел Кармайкла, которые не превосходят 25 000 000 000, и всего 16 чисел, которые не превосходят числа 100 000.

Вероятностным тестом простоты, свободным от этого недостатка является тест Соловея–Штрассена [13]. Тест Соловея–Штрассена состоит из υ отдельных раундов. В каждом раунде выполняются следующие действия:

1. Случайным образом выбирается число $\omega < p$ и вычисляется $\psi = \text{Н.О.Д.}(\omega, p)$.

2. Если $\psi > 1$, то выносится решение о том, что p составное. В противном случае проверяется соотношение:

$$\omega^{\frac{p-1}{2}} \equiv \left(\frac{\omega}{p}\right) (\bmod p), \qquad (2)$$

где $\left(\dfrac{\omega}{p}\right)$ – символ Якоби.

Если соотношение (2) не выполнено, то p – составное. Если выполнено, то ω является свидетелем простоты числа p. Если после υ раундов найдено υ свидетелей простоты, то тест делает заключение о том, что p вероятно является простым числом.

В каждом раунде вероятность отсеять составное число больше 1/2, поэтому через υ раундов тест Соловея–Штрассена определяет простое число с вероятностью ошибки, меньшей $2^{-\upsilon}$. В этом отношении он проигрывает тесту Миллера–Рабина, который за υ раундов имеет ошибку, меньшую $4^{-\upsilon}$. Для определения простоты числа может быть использован тест Рабина–Миллера [14, 15, 16], в основе которого лежит малая теорема Ферма, утверждающая, что для любого простого числа p и для всех $1 \le \beta \le p$ справедливо соотношение $\beta^{p-1} \pmod p = 1 \pmod p$. Число β в этом случае называется базисом.

Можно представить $p-1=2^{\tau}\cdot\phi$, где φ – нечетное число. Если требуется вычислить $\beta^{p-1} \pmod p$, можно найти $\beta^{\varphi} \pmod p$ и возвести полученный результат в квадрат τ раз, т.е. получить $\beta^{p-1} \pmod p = \beta^{\varphi\cdot 2\cdot\tau} \pmod p$.

Если $\beta^{\varphi} \pmod p = 1 \pmod p$, то многократное возведение в квадрат не изменит результата и можно записать $\beta^{p-1} \pmod p = 1 \pmod p$.

Если $\beta^{\varphi} \pmod p \neq 1 \pmod p$, то необходимо вычислять и анализировать последовательность

$$\beta^{\varphi}, \beta^{\varphi\cdot 2}, \beta^{\varphi\cdot 2^2}, \beta^{\varphi\cdot 2^3}, \ldots, \beta^{\varphi\cdot 2^{\tau}}, \qquad (3)$$

каждый элемент которой берется по модулю p.

Если p является простым числом, то согласно малой теореме Ферма последним элементом последовательности (3) должна быть единица. Если хотя бы при одном случайно выбранном базисе β тест дает отрицательный результат, то принимается решение о том, что p является составным числом. Это свидетельствует о необходимости возврата к алгоритму проб и ошибок для выбора нового значения φ. Если φ успешно проходит тест при данном β, то следует повторить его, выбрав другой базис β, чем обеспечивается снижение вероятности получения неверного результата тестирования до приемлемой величины. Наиболее ресурсоемкой операцией в тесте Рабина–Миллера является операция $\beta^{\varphi} \pmod p$. Для ее реализации предлагается так называемый двоичный алгоритм, коротко формулируемый в виде следующей рекурсии. Если $\varphi=0$, то $\beta^{\varphi} \pmod p = 1$. Если $\varphi>0$ и является четным числом, то находится величина $\gamma=\beta^{\varphi/2} \pmod p$, и окончательный результат будет выглядеть $\beta^{\varphi} \pmod p = \gamma^2 \pmod p$.

Если $\varphi>0$ и является нечетным числом, то находится величина $\gamma=\beta^{(\varphi-1)/2} \pmod p$, и окончательный результат будет выглядеть так: $\beta^{\varphi} \pmod p = \beta\cdot\gamma^2 \pmod p$.

Если проанализировать описанные операции, то можно сделать вывод о том, что необходимый показатель степени формируется бит за битом, начиная от более значимой части двоичного представления

показателя степени к наименее значимой его части. Если обозначить σ – число бит значения φ, т.е. $2^{\sigma-1} \le \varphi < 2^{\sigma}$, то можно сказать, что данный алгоритм потребует не более 2σ операций умножения по модулю φ. Такой объем работы доступен вычислительным возможностям большинства стандартных персональных компьютеров.

Необходимость неоднократного тестирования с разными базисами объясняется существованием чисел Кармайкла, которые, будучи составными, успешно проходят тест Рабина–Миллера. Эксперты [17–21] рекомендуют ограничиться исследованием 5–10 базисов.

Выводы. Таким образом, если учесть, что числа Кармайкла в области больших чисел встречаются крайне редко, а также то обстоятельство, что тест Соловея–Штрассена имеет большую вычислительную сложность, то более предпочтительным для поиска больших простых чисел представляется использование теста Миллера–Рабина.

С учетом этого для практических приложений можно предложить следующую последовательность формирования параметра *p*:

1) сгенерировать псевдослучайное двоичное число *p* требуемой разрядности;

2) установить старший и младший биты полученного числа равными 1. Старший бит в этом случае гарантирует требуемую длину формируемого простого числа, а младший – его нечетность;

3) убедиться, что число *p* не делится на малые простые числа 3, 5, 7, 11 и т.д. Наиболее надежна проверка делимости на все простые числа, меньше 2000;

4) выполнить тест Рабина–Миллера для некоторого псевдослучайного числа φ. Если *p* проходит тест, то сгенерировать другое псевдослучайное число φ и повторить тест. Для практических приложений достаточно повторить тест Рабина–Миллера пять раз;

5) если *p* не проходит один из тестов, надо сгенерировать другое число *p* и повторить описанную последовательность действий. Другое число *p*, если оно оказалось непростым, можно получить, не генерируя новое, а последовательно перебирая все целые, начиная от $p + 1$, $p + 2$, и т.д., пока не найдется простое число.

С помощью аналогичной процедуры предлагается осуществлять поиск и других параметров (*b*, *m*, *q*, *y*) стандартного алгоритма формирования ЭЦП.

Библиографический список

1. ГОСТ Р34.10–2012. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи // Доступ из справ.-правовой системы КонсультантПлюс.

2. Щербаков А., Домашев А. Прикладная криптография. Использование и синтез криптографических интерфейсов. – М.: Русская редакция, 2002.

3. ГОСТ Р34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования // Доступ из справ.-правовой системы КонсультантПлюс.

4. Ланских В.Г., Ланских Ю.В. Использование блочного алгоритма шифрования для реализации функций хеширования // Научные тенденции: вопросы точных и технических наук: сб. науч. тр. по материалам VIII Междунар. науч. конф.; г. Москва, 12 июля 2017 г. – М., 2017. – С. 10–11.

5. Ланских В.Г., Ланских Ю.В. Повышение криптографической стойкости функций хеширования // Достижения и приложения современной информатики, математики и физики: материалы VI Всерос. науч.-практ. заочной конф.; г. Нефтекамск, 1 ноября 2017 г. – Нефтекамск, 2017. – С. 178–185.

6. Ланских В.Г., Ланских Ю.В. Применение блочных алгоритмов для формирования функций хеширования // Информационно-телекоммуникационные системы и технологии: материалы всерос. науч.-практ. конф.; Кемерово, 12–13 октября 2017 г. – Кемерово, 2017. – С. 316–318.

7. Реализация функций хеширования на основе стандартных симметричных криптографических алгоритмов / М.И. Красиков, В.Г. Ланских, Ю.В. Ланских, Л.В. Пешнина // Высокие технологии и модернизация экономики: достижения и новые векторы развития: сб. науч. тр. по материалам I Междунар. науч.-практ. конф.; 31 октября 2017 г. – М.: НОО «Профессиональная наука», 2017. – С. 57–62.

8. Уильямс Х. Проверка чисел на простоту с помощью вычислительных машин // Кибернетический сборник. – М.: Мир, 1986. – Вып. 23. – С. 51–99.

9. Василенко О.Н. Некоторые алгоритмы построения больших простых чисел // Вестник Моск. ун-та. Сер. 1: Математика. Механика. – 1997. – № 5. – С. 62–64.

10. Crandall R., Pomerance C. Prime numbers: a computational perspective. – Springer-Verlag, 2001.

11. Василенко О.Н. О некоторых свойствах чисел Ферма // Вестник Моск. ун-та. Сер. 1: Математика. Механика. – 1998. – № 5. – С. 56–58.

12. Alford W.R., Granville A., Pomerance C. There are infinitely many Carmichael numbers // Ann. Math. – 1994. – Vol. 140. – P. 703–722.

13. Solovay R., Strassen V. A fast monte-carlo test for primality // SIAM Journal on Computing. – 1977. – Vol. 6, no. 1. – P. 84–85.

14. Miller G.L. Riemann's hypothesis and tests for primality // J. Comput. and Syst. Sci. – 1976. – Vol. 13. – P. 300–317. [Перевод: Кибернетич. сборник. – М.: Мир, 1986. – Вып. 23. – С. 31–50].

15. Василенко О.Н. Об алгоритме Миллера–Рабина // Вестник Моск. ун-та. Сер. 1: Математика. Механика. – 2000. – № 2. – С. 41–42.

16. Гашков С.Б. Упрощенное обоснование вероятностного теста Миллера–Рабина для проверки простоты чисел // Дискретная математика. – 1998. – Т. 10(4). – С. 35–38.

17. Adleman L., Pomerance C., Rumely R.S. On distinguishing prime numbers from composite numbers // Ann. Math. – 1983. – Vol. 117. – P. 173–206.

18. Adleman L., Huang M.-D.A. Primality testing and abelian varietes over finite fields. – 1992. (Lect. Notes in Math.; Vol. 1512).

19. Adleman L., McCurley K. Open problems in number theoretic complexity // Proceedings of ANTS-I. – 1994. (Lect. Notes in Comput. Sci.; Vol. 877). – P. 291–322.

20. Adleman L.M., Manders K., Miller G.L. On taking roots in finite fields // Proc. 18th Ann. Symp. Found. Comput. Sci. – 1977. – P. 175–178.

21. Schoof R. Four primarity testing algorithms. Surveys in Algorithmic Number Theory / ed. J.B. Buchler, P. Stevenhagen // Math. Sci. Res. Inst. Publ. 44. – Cambridge Univ. Press, New York, 2008. – P. 101–126.

References

1. GOST R34.10–2012 Kriptograficheskaia zashchita informatsii. Protsessy formirovaniia i proverki elektronnoi tsifrovoi podpisi [Cryptographic protection of information. Processes of formation and verification of electronic digital signature]. Dostup iz spravochno-pravovoi sistemy Konsul'tantPlius.

2. Shcherbakov A., Domashev A. Prikladnaia kriptografiia. Ispol'zovanie i sintez kriptograficheskikh interfeisov [Applied cryptography. Use and synthesis of cryptographic interfaces]. Moscow: Russkaia redaktsiia, 2002.

3. GOST R34.11-94. Informatsionnaia tekhnologiia. Kriptograficheskaia zashchita informatsii. Funktsiia kheshirovaniia [Information technology. Cryptographic protection of information. Hash function]. Dostup iz spravochno-pravovoi sistemy Konsul'tantPlius.

4. Lanskikh V.G., Lanskikh Yu.V. Ispol'zovanie blochnogo algoritma shifrovaniia dlia realizatsii funktsii kheshirovaniia [Using a block encryption algorithm to implement hashing functions]. *Nauchnye tendentsii: voprosy tochnykh i tekhnicheskikh nauk: sbornik nauchnykh trudov po materialam VIII Mezhdunarodnoi nauchnoi konferentsii; Moscow, 12 July 2017*. Moscow, 2017, pp. 10-11.

5. Lanskikh V.G., Lanskikh Yu.V. Povyshenie kriptograficheskoi stoikosti funktsii kheshirovaniia [Increasing cryptographic stability of hashing functions]. *Dostizheniia i prilozheniia sovremennoi informatiki, matematiki i fiziki: materialy VI Vserossiiskoi nauchno-prakticheskoi zaochnoi konferentsii, Neftekamsk, 1 November 2017*. Neftekamsk, 2017, pp. 178-185.

6. Lanskikh V.G., Lanskikh Yu.V. Primenenie blochnykh algoritmov dlia formirovaniia funktsii kheshirovaniia [Application of block algorithms for the generation of hashing functions]. *Informatsionno-telekommunikatsionnye sistemy i tekhnologii: materialy Vserossiiskoi nauchno-prakticheskoi konferentsii Kemerovo, 12-13 October 2017*. Kemerovo, 2017, pp. 316-318.

7. Krasikov M.I., Lanskikh V.G., Lanskikh Yu.V., Peshnina L.V. Realizatsiia funktsii kheshirovaniia na osnove standartnykh simmetrichnykh kriptograficheskikh algoritmov [Implementing hashing functions based on standard symmetric cryptographic algorithms]. *Vysokie tekhnologii i modernizatsiia ekonomiki: dostizheniia i novye vektory razvitiia: sbornik nauchnykh trudov po materialam I Mezhdunarodnoi nauchno-prakticheskoi konferentsii, 31 October 2017*. Moscow: NOO “Professional'naia nauka”, 2017, pp. 57-62.

8. Williams H. Proverka chisel na prostotu s pomoshch'iu vychislitel'nykh mashin [Checking numbers for simplicity with the help of computers]. *Kiberneticheskii sbornik*. Moscow: Mir, 1986, iss. 23, pp. 51-99.

9. Vasilenko O.N. Nekotorye algoritmy postroeniia bol'shikh prostykh chisel [Some algorithms for constructing large primes]. *Vestnik Moskovskogo universiteta. Matematika. Mekhanika*, 1997, no. 5, pp. 62-64.

10. Crandall R., Pomerance C. Prime numbers: a computational perspective. Springer-Verlag, 2001.

11. Vasilenko O.N. O nekotorykh svoistvakh chisel Ferma [On some properties of Fermat numbers]. *Vestnik moskovskogo universiteta. Matematika. Mekhanika*, 1998, no. 5, pp. 56-58.

12. Alford W.R., Granville A., Pomerance C. There are infinitely many Carmichael numbers. *Annals of Mathematics*, 1994, vol. 140, pp. 703-722.

13. Solovay R., Strassen V. A fast monte-carlo test for primality. *SIAM Journal on Computing*, 1977, vol. 6, no. 1, pp. 84-85.

14. Miller G.L. Riemann's hypothesis and tests for primality. *J. Comput. and Syst. Sci*, 1976, vol. 13, pp. 300-317.

15. Vasilenko O.N. Ob algoritme Millera-Rabina [On the Miller-Rabin algorithm]. *Vestnik Moskovskogo universiteta. Matematika. Mekhanika*, 2000, no. 2, pp. 41-42.

16. Gashkov S.B. Uproshchennoe obosnovanie veroiatnostnogo testa Millera-Rabina dlia proverki prostoty chisel [Simplified justification of the Miller-Rabin probabilistic test for checking the simplicity of numbers]. *Diskretnaia matematika*, 1998, vol. 10(4), pp. 35-38.

17. Adleman L., Pomerance C., Rumely R. S. On distinguishing prime numbers from composite numbers. *Annals of Mathematics*, 1983, vol. 117, pp. 173-206.

18. Adleman L., Huang M.-D.A. Primality testing and abelian varietes over finite fields. 1992. (Lect. Notes in Math.; Vol. 1512).

19. Adleman L., McCurley K. Open problems in number theoretic complexity. Proceedings of ANTS-I. 1994. (Lect. Notes in Comput. Sci.; Vol. 877), pp. 291-322.

20. Adleman L.M., Manders K., Miller G.L. On taking roots in finite fields. *Proc. 18th Ann. Symp. Found. Comput. Sci*, 1977, pp. 175-178.

21. Schoof R. Four primarity testing algorithms. Surveys in Algorithmic Number Theory. Ed. J.B. Buchler, P. Stevenhagen. *Math. Sci. Res. Inst.* Publ. 44. Cambridge Univ. Press, New York, 2008, p.101-126.

Сведения об авторах

Ланских Владимир Георгиевич (Киров, Россия) – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Вятского государственного университета (610009, Киров, ул. Московская, 36, e-mail: usr00222@vyatsu.ru).

Ланских Юрий Владимирович (Пермь, Россия) – кандидат технических наук, доцент кафедры «Математические и естественно-научные дисциплины» Пермского государственного национального исследовательского университета (614990, Пермь, ул. Букирева, 15, e-mail: lyuv@inbox.ru).

About the authers

Lanskikh Vladimir Georgievich (Kirov, Russian Federation) is a Ph.D. in Technical Sciences, Associate Professor at the Department of Automation and Telemechanics Vyatka State University (610009, Kirov, 36, Moskovskaya st., e-mail: usr00222@vyatsu.ru).

Lanskikh Yury Vladimirovich (Perm, Russian Federation) is a Ph.D. in Technical Sciences, Associate Professor at the Department of Mathematical and Natural Science Disciplines Perm State National Research University (614990, Perm, 15, Bukirev st., e-mail: lyuv@inbox.ru).

Получено 25.04.2018