PCT

ВСЕМИРНАЯ ОРГАНИЗАЦИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ
Международное бюро

МЕЖДУНАРОДНАЯ ЗАЯВКА, ОПУБЛИКОВАННАЯ В СООТВЕТСТВИИ С ДОГОВОРОМ О ПАТЕНТНОЙ КООПЕРАЦИИ (PCT)

(51) Международная классификация изобретения [7]: **H04L 9/32**	**A1**	(11) Номер международной публикации: **WO 00/19658** (43) Дата международной публикации: 6 апреля 2000 (06.04.00)

(21) **Номер международной заявки:** PCT/RU99/00197

(22) **Дата международной подачи:** 16 июня 1999 (16.06.99)

(30) **Данные о приоритете:**
98117706 29 сентября 1998 (29.09.98) RU

(71) (72) **Заявители и изобретатели:** ЗОЛОТАРЁВ Олег Анатольевич [RU/RU]; 188537 Ленинградская обл., Сосновый Бор, ул. Молодёжная, д. 25, кв. 20 (RU) [ZOLOTAREV, Oleg Anatolievich, Sosnovy Bor (RU)]. КУЗНЕЦОВ Иван Владимирович [RU/RU]; 191123 Санкт-Петербург, ул. Салтыкова-Щедрина, д. 48, кв. 56 (RU) [KUZNETSOV, Ivan Vladimirovich, St. Petersburg (RU)]. МОШОНКИН Андрей Геннадьевич [RU/RU]; 191123 Санкт-Петербург, ул. Шпалерная, д. 44а, кв. 5 (RU) [MOSHONKIN, Andrei Genna-dievich, St.Petersburg (RU)]. СМИРНОВ Александр Леонидович [RU/RU]; 191126 Санкт-Петербург, ул. Достоевского, д. 36, кв. 8 (RU) [SMIRNOV, Alexandr Leonidovich, St.Petersburg (RU)]. ХАМИТОВ Ильдар Магафурович [RU/RU]; 193029 Санкт-Петербург, ул., Бабушкина, д. 29, корп. 2, кв. 45 (RU) [KHAMITOV, Ildar Magafurovich, St.Petersburg (RU)]

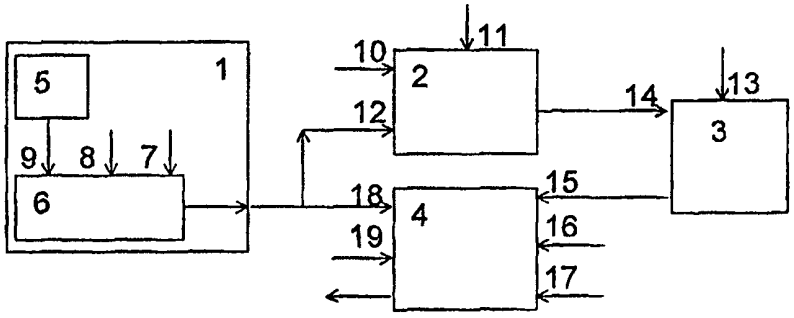
(74) **Агент:** МАТВЕЕВА Татьяна Ивановна; 199034 Санкт-Петербург, Университетская наб., д. 7/9, Университет, Департамент патентов и лицензий (RU) [MATVEEVA, Tatiyana Ivanovna, St.Petersburg (RU)].

(81) **Указанные государства:** US, европейский патент (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Опубликована
С отчётом о международном поиске.

(54) **Title:** METHOD FOR THE BLIND GENERATION OF A DIGITAL RSA SIGNATURE AND DEVICE FOR REALISING THE SAME

(54) **Название изобретения:** СПОСОБ ИЗГОТОВЛЕНИЯ ВСЛЕПУЮ ЦИФРОВОЙ RSA-ПОДПИСИ И УСТРОЙСТВО ДЛЯ ЕГО РЕАЛИЗАЦИИ (ВАРИАНТЫ)



(57) Abstract

The present invention essentially relates to a new method for generating blindly a digital RSA signature, wherein said method involves masking the starting data by performing an RSA encryption. This invention also relates to a corresponding method for unmasking the masked and signed data. This invention allows for the use of an unlimited number of signature types in global-service electronic systems. Intraceability is ensured by the corresponding selection of a randomised exponent R and of an RSA key used during the RSA encryption of the starting data, and also by the characteristics of an open module N which are checked at a random moment in time. According to this invention, N = P.Q in which P and Q are secret simple factors, while R is a multiple of N-1. In other embodiments of the present invention, the diversity of the signature types is determined by limiters of the open exponent multiplicities, said limiters being selected before masking the starting data. The device for realising the method for the blind generation of a digital RSA signature includes a masking unit based on a modular exponentiating operator, as well as corresponding unmasking unit.

(54) Реферат

Сущность изобретения состоит в том, что при изготовлении вслепую цифровой RSA-подписи применяют новый метод маскировки исходных данных посредством их RSA-шифрования, и соответствующий ему метод демаскировки подписанных замаскированных данных, что дает возможность использовать в электронных системах массового обслуживания неограниченное число видов подписи. Непрослеживаемость обеспечивается соответствующим выбором рандомизированной экспоненты R, используемого при RSA-шифровании исходных данных RSA-ключа, и свойствами открытого модуля N, проверяемыми в произвольный момент времени. При этом $N = P \cdot Q$, где P и Q секретные простые множители, а R кратна N-1. В других вариантах изобретения многообразие видов подписи задается выбираемыми перед маскировкой исходных данных ограничениями для кратностей открытых экспонент. Устройство для реализации способа изготовления вслепую цифровой RSA-подписи содержит блок маскировки, основанный на модулярном экспоненциаторе, и соответствующий блок демаскировки.

СПОСОБ ИЗГОТОВЛЕНИЯ ВСЛЕПУЮ ЦИФРОВОЙ RSA-ПОДПИСИ И УСТРОЙСТВО ДЛЯ ЕГО РЕАЛИЗАЦИИ (варианты)

Область техники

Изобретение относится к области криптографических систем, а более точно, к области систем, использующих цифровую подпись.

Предшествующий уровень техники

Цифровая подпись широко используется на практике и играет роль, аналогичную роли обычной рукописной подписи. Преимущества цифровой подписи состоят в том, что ее достоверность легко проверяема, ее подделка весьма затруднительна, и, кроме того, цифровая подпись легко может быть передана по телекоммуникационным каналам. В системах, использующих цифровую подпись, имеют дело с данными, которые располагаются на подходящих материальных носителях и могут быть представлены цифровым образом.

В схеме RSA, называемой так по именам ее изобретателей (R. L. Rivest, A. Shamir, L. M. Adleman, Cryptographic Communications System and Method, U.S. Patent 4,405,829, 20 Sep 1983), используют представление данных целыми числами из некоторой системы вычетов по модулю целого числа N, называемого RSA-модулем. В качестве системы вычетов обычно используют целые числа от 0 до N-1. Понятия, связанные со схемой RSA (A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997, p. 285, 433), могут быть снабжены, для определенности, префиксом RSA, например, RSA-подпись, RSA-шифрование, RSA-ключ, RSA-экспонента и т.п.

Данные S удовлетворяет свойству цифровой RSA-подписи для данных M по отношению к RSA-ключу с модулем N и экспонентой E, или, иными словами, являются цифровой RSA-подписью для данных M, если $M \equiv S^E \pmod N$, где под RSA-ключом имеются в виду произвольные данные, определяющие модуль и экспоненту, а запись $A \equiv B \pmod N$ означает, что A и B сравнимы по модулю N, то есть, что целое число (A - B) делится нацело на N.

Цифровая RSA-подпись для данных M может быть изготовлена RSA-шифрованием данных M, при котором в качестве шифровального ключа используют секретный RSA-ключ подписывающей стороны, соответствующий открытому RSA-ключу с модулем N и экспонентой E. При этом под RSA-шифрованием имеется в виду обработка данных X, в результате которой получают данные Y, удовлетворяющие соотношению $Y \equiv X^C \pmod N$, где C и N, соответственно, экспонента и модуль шифровального RSA-ключа. Под соответствием двух RSA-ключей имеется в виду возможность проверки цифровой RSA-подписи, изготовленной одним RSA-ключом, с помощью другого RSA-ключа, или, что то же самое, возможность расшифровки данных, зашифрованных одним ключом, посредством другого ключа. Соответствие RSA-ключей с экспонентами A и B и модулем N обеспечено условием $A \cdot B \equiv 1 \bmod \varphi(N)$, где $\varphi(N)$ число вычетов, взаимно простых с N.

Однако, изготовление цифровой RSA-подписи для исходных данных M непосредственным RSA-шифрованием исходных данных секретным RSA-ключом подписывающей стороны не обеспечивает приватности подателей, так как предназначенные для подписания исходные данные доступны подписывающей стороне при изготов-

лении подписи. Это пояснено в статье D. Chaum, Blind signatures for untraceable payments, Advanced in Cryptology - Proceedings of Crypto 82, 1983, p. 199-203, где введена концепция изготовления цифровой подписи вслепую, предназначенная для преодоления этого недостатка.

Известен способ изготовления вслепую цифровой RSA-подписи (D. Chaum, Blind Signature Systems, U.S. Patent 4,759,063, 19 Jul 1988), в котором податель, желающий получить цифровую RSA-подпись для исходных данных M, выбирает рандомизированный маскировочный ключ R и создает замаскированные данные M' в соответствии с формулой $M' \equiv R^E \cdot M \pmod N$, где E экспонента, а N модуль открытого RSA-ключа. Замаскированные данные предоставляются подписывающей стороне, которая возвращает подателю цифровую RSA-подпись S' для замаскированных данных. Податель завершает изготовление цифровой RSA-подписи S для исходных данных демаскировкой полученной цифровой RSA-подписи для замаскированных данных, которую проводит в соответствии с формулой $S \equiv S' \cdot R^{-1} \pmod N$. Известный способ обеспечивает непрослеживаемость, то есть практическую невозможность для подписывающей стороны, получившей впоследствии подписи многих исходных данных, установить соответствие между этими подписями и обработанными замаскированными данными. Однако известный способ не позволяет изготовить вслепую цифровую RSA-подпись без предварительного знания вида подписи, так как экспонента E открытого ключа, определяющая вид подписи, используется при создании замаскированных данных.

Известен способ изготовления вслепую неожидаемой цифровой RSA-подписи (D. Chaum, Blind Unanticipated Signature Systems, U.S. Patent 4,759,064, 19 Jul 1988), который является наиболее близким аналогом к предлагаемому изобретению и выбран заявителем в качестве прототипа. В этом способе используют набор допустимых открытых RSA-экспонент $E_1,\ldots, E_k$ и набор данных $(g_1, \ldots, g_u)$, названных генераторами. Для каждого генератора g_j публикуют цифровые RSA-подписи $S_{i,j}$, соответствующие каждой допустимой открытой RSA-экспоненте E_i. Податель выбирает в качестве рандомизированного маскировочного ключа R набор $(k_1,\ldots,k_u)$ и создает замаскированные данные M' в соответствии с формулой $M' = M \cdot g_1^{k1} \cdot \ldots \cdot g_u^{ku} \pmod N$, где N модуль открытого RSA-ключа. Замаскированные данные M' предоставляют подписывающей стороне, которая выбирает вид подписи, то есть выбирает ту допустимую открытую RSA-экспоненту E_i, которой будет соответствовать изготавливаемая цифровая RSA-подпись. Цифровую RSA-подпись S' для замаскированных данных, соответствующую выбранной открытой RSA-экспоненте E_i, вместе с информацией о выбранной открытой RSA-экспоненте E_i, предоставляют подателю. Податель получает цифровую RSA-подпись S для исходных данных демаскировкой S', которую проводят в соответствии с формулой $S \equiv S' \cdot S_{i,1}^{-k1} \cdot \ldots \cdot S_{i,u}^{-ku} \pmod N$.

Непрослеживаемость в известном способе изготовления вслепую неожидаемой цифровой RSA-подписи определенными свойствами генераторов по отношению к секретным RSA-ключам, в связи с чем используется тестирование пригодности генераторов методом "cut and choose". Подпись в известном способе называется неожидаемой, так как податель, в момент предоставления подписывающей стороне замаскированных данных, не знает вида изготавливаемой подписи, то есть той откры-

той RSA-экспоненты, которой будет соответствовать изготавливаемая подпись.

Недостатки известного способа состоят в ограничении количества видов изготавливаемой RSA-подписи, что снижает ее неожидаемость, в росте вероятности ошибок при изготовлении подписи и в замедляющем воздействии количества видов подписи на скорость ее изготовления. Указанные недостатки обусловлены необходимостью осуществлять демаскировку с помощью растущего пропорционально количеству видов подписи объема данных, которые, в свою очередь, требуют дополнительных ресурсов и времени для их хранения и обработки. Кроме того, известный способ имеет недостаточную достоверность непрослеживаемости, так как проверка пригодности сообщенных подписывающей стороной данных, в частности генераторов, производится третьей стороной, а не подателем непосредственно.

Известно устройство для изготовления вслепую цифровой RSA-подписи (D. Chaum, Blind Signature Systems, U.S. Patent 4,759,063, 19 Jul 1988). Однако этого устройства не достаточно для изготовления вслепую неожидаемой цифровой RSA-подписи.

Известно устройство для изготовления вслепую неожидаемой цифровой RSA-подписи (D. Chaum, Blind Unanticipated Signature Systems, U.S. Patent 4,759,064, 19 Jul 1988), наиболее близкое к заявляемому устройству и выбранное заявителем в качестве прототипа. Известное устройство состоит из блока выбора маскировочного ключа, включающего датчик случайных чисел, блока маскировки, блока подписи и блока демаскировки. Блок маскировки имеет входы исходных данных и маскировочного ключа и содержит модулярный экспоненциатор, к модульному входу которого подсоединен модульный вход блока маскировки, а к экспонентному входу которого подсоединен вход маскировочного ключа блока маскировки. Блок подписи имеет вход секретного ключа и вход данных подписи, соединенный с выходом блока маскировки. Блок демаскировки имеет модульный вход, экспонентный вход, вход маскировочного ключа, вход данных демаскировки, соединенный с выходом блока подписи, и выход для вывода цифровой RSA-подписи для исходных данных.

Недостатки известного устройства состоят в том, что оно не позволяет при изготовлении вслепую цифровой RSA-подписи использовать неограниченное количество видов подписи, что снижает неожидаемость изготавливаемой цифровой RSA-подписи, его использование приводит к росту вероятности ошибок при изготовлении подписи и к замедляющему воздействию количества видов подписи на скорость ее изготовления, что обусловлено необходимостью вводить в демаскирующий блок данные, поиск которых требует времени, растущего пропорционально количеству видов подписи.

Раскрытие изобретения

Основной задачей, решаемой вариантами заявленного изобретения, является создание таких способа изготовления вслепую цифровой RSA-подписи и устройства для его реализации, которые обеспечивают непрослеживаемость и высокую неожидаемость при изготовления цифровой RSA-подписи, а также допускают быстрое изготовление вслепую цифровой RSA-подписи при сравнительно небольших ресурсах.

Единый для всех предложенных вариантов заявленного изобретения технический результат, достигаемый при их реализации, состоит в том, что при изготовлении

вслепую неожидаемой цифровой RSA-подписи возможно использование неограниченного количества видов подписи, не требуются растущие в зависимости от количества возможных видов подписи технические ресурсы, хранилища больших объемов данных и поиск в них, что приводит к ускорению и повышению надежности изготовления вслепую цифровой RSA-подписи. Помимо этого, повышается достоверность непрослеживаемости за счет того, что свойства данных, обеспечивающих непрослеживаемость, могут быть, в некоторых из заявленных вариантов, протестированы непосредственно самим подателем.

Заявленный способ изготовления вслепую цифровой RSA-подписи предназначен исключительно для аппаратной или компьютерной реализации, так как сама цифровая RSA-подпись реализуется только на аппаратной или компьютерной основе (R.L. Rivest, A. Shamir, L.M. Adleman, Cryptographic Communications System and Method, U.S. Patent 4,405,829, 20 Sep 1983).

В описании изобретения используются известные устройства, реализующие основные арифметические функции и основные функции модулярной арифметики. Такие устройства могут работать с данными, представляющими целые числа подходящей разрядности. Для уточнения терминологии далее описана функциональность используемых устройств. Под модулярным умножителем имеется в виду устройство с модульным и двумя аргументными входами, причем если на модульный вход подано целое число N, а на аргументные входы поданы целые числа X, Y, то на выходе появляется целое число Z такое, что $Z \equiv X \cdot Y \pmod{N}$. Под модулярным инвертором имеется в виду устройство с модульным и аргументным входами, причем если на модульный вход подано целое число N, а на аргументный вход подано целое число X, взаимно простое с N, то на выходе появляется целое число Y такое, что $X \cdot Y \equiv 1 \pmod{N}$. Под модулярным вычислителем частного имеется в виду устройство с модульным входом и входами делимого и делителя, причем если на модульный вход подано целое число N, на вход делимого подано целое число X, а на вход делителя подано целое число Y, взаимно простое с N, то на выходе появляется целое число Z такое, что $Z \cdot Y \equiv X \pmod{N}$. Под модулярным экспоненциатором имеется в виду устройство с модульным, базовым и экспонентным входами, причем если на модульный вход подано целое число N, на базовый вход подано целое число X, а на экспонентный вход подано целое число E, то на выходе появляется целое число Z такое, что $Z \equiv X^E \bmod N$. Под тестером взаимной простоты имеется в виду устройство с двумя входами, причем если на входы поданы целые числа A и B, то на выходе появляется логическое значение «Истина», если наибольший общий делитель A и B равен единице, и логическое значение «Ложь» в ином случае.

Предложено несколько вариантов способа изготовления вслепую цифровой RSA-подписи.

Ниже дано описание способа изготовления вслепую цифровой RSA-подписи по первому варианту. Это описание предназначено для раскрытия способа изготовления вслепую цифровой RSA-подписи по первому варианту и не ограничивает рамки заявленного изобретения, описанного более полно где-либо еще в настоящей заявке.

В качестве секретных множителей RSA-модуля N подписывающая сторона выбирает простые числа подходящего размера, причем в наилучшем варианте выбирают

два секретных множителя. Кроме того, выбирают, по меньшей мере, одну допустимую открытую RSA-экспоненту. Допустимые открытые RSA-экспоненты, то есть такие открытые RSA-экспоненты, что при изготовлении цифровой RSA-подписи допускается использование секретного RSA-ключа, соответствующего каждой из них, могут быть выбраны подписывающей стороной, подателем, совместно подателем и подписывающей стороной, и вообще произвольным способом.

При изготовлении цифровой RSA-подписи для исходных данных M податель выбирает в качестве рандомизированного маскировочного ключа целое число R, кратное произвольно выбранному маскирующему множителю G и взаимно простое с каждой допустимой открытой RSA-экспонентой. Рандомизация R, то есть внесение элемента случайности в выбор R, может быть осуществлена, например, с помощью датчика случайных чисел или иным способом.

Под датчиком случайных чисел заявитель имеет в виду устройство, на выходе которого появляются данные подходящей разрядности, предпочтительно непредсказуемые для стороны, не контролирующей работу такого устройства. Такие устройства хорошо известны. В частности, в качестве датчиков случайных чисел могут использоваться датчики «псевдослучайных» чисел.

Взаимная простота рандомизированного маскировочного ключа с каждой допустимой открытой RSA-экспонентой достигается, в частности, либо корректировкой выходных данных датчика случайных чисел допустимыми открытыми RSA-экспонентами, либо тестированием выходных данных датчика случайных чисел. Кратность рандомизированного маскировочного ключа маскирующему множителю G достигается, в частности, корректировкой выходных данных датчика случайных чисел маскирующим множителем.

С помощью маскировочного ключа R податель производит маскировку исходных данных M, создавая на их основе замаскированные данные M' посредством RSA-шифрования исходных данных шифровальным RSA-ключом, модуль которого совпадает с RSA-модулем N, а экспонента которого совпадает с маскировочным ключом R. Такое шифрование может быть осуществлено, в частности, модулярным экспоненциатором. Замаскированные данные M' удовлетворяют соотношению $M' \equiv M^R \pmod N$. Созданные замаскированные данные M' предоставляют подписывающей стороне, которая создает цифровую RSA-подпись S' для замаскированных данных M' секретным RSA-ключом, соответствующим произвольной допустимой открытой RSA-экспоненте E. При этом под соответствием секретного RSA-ключа открытой RSA-экспоненте E имеется в виду соответствие секретного RSA-ключа и RSA-ключа с модулем N и экспонентой E. Создание цифровой RSA-подпись S' для замаскированных данных M' может быть осуществлено, в частности, посредством модулярного экспоненциатора, а созданная цифровая RSA-подпись S' для замаскированных данных M' удовлетворяет соотношению $S' \equiv (M')^D \pmod N$.

Изготовление цифровой RSA-подписи S для исходных данных M завершают демаскировкой цифровой RSA-подписи для замаскированных данных. Принципиальная возможность демаскировки вытекает из соотношения $S \equiv (S')^A \cdot M^B \pmod N$, где A и B произвольные целые числа, удовлетворяющие условию $A \cdot R + B \cdot E = 1$, и взаимной простоты маскировочного ключа R и открытой RSA-экспоненты E, что обес-

печено выбором маскировочного ключа R взаимно простым относительно каждой допустимой открытой RSA-экспоненты. Практически демаскировку производят введением цифровой RSA-подписи для замаскированных данных S', маскировочного ключа R, RSA-модуля N и открытой RSA-экспоненты E в подходящий демаскирующий преобразователь, на выходе которого получают цифровую RSA-подпись S для исходных данных M. Такой демаскирующий преобразователь может быть реализован, например, модулярным мультипликативным евклидовым преобразователем (ММЕП), то есть устройством с модульным входом, двумя базовыми входами, двумя соответствующими экспонентными входами и выходом, причем, если на модульный вход ММЕП подано целое положительное число N, на один из базовых входов подано взаимно простое с N целое число X, на соответствующий ему экспонентный вход подано целое число A, на другой базовый вход подано взаимно простое с N целое число Y, а на соответствующий ему экспонентный вход подано целое число B, причем целые числа A и B взаимно просты, то на выходе появляется целое число Z такое, что $Z \equiv X^C \cdot Y^D \pmod N$, где C и D произвольные целые числа, удовлетворяющие соотношению $A \cdot C + B \cdot D = 1$. Для подтверждения реализуемости ММЕП в приведенном далее примере 5 заявитель описывает пример конкретной реализации ММЕП и его работы. Иные примеры ММЕП могли бы быть реализованы специалистами среднего уровня на основе известных сведений. Например, целые числа C и D могут быть определены по целым числам A и B с помощью устройства, реализующего известный обобщенный алгоритм Евклида (Д. Кнут, Искусство программирования для ЭВМ, т.2, Получисленные алгоритмы, Москва, «Мир», 1977, стр. 367-368), после чего Z может быть получено посредством модулярных экспоненциаторов и модулярного умножителя.

Непрослеживаемость в способе изготовления вслепую цифровой RSA-подписи по первому варианту обеспечивают, в частности, таким выбором секретных множителей и маскирующего множителя, которые обеспечивают подходящий уровень маскировки. Под уровнем маскировки имеется в виду вероятность того, что для случайных исходных данных X, равномерно распределенных среди обратимых вычетов по модулю N, и случайных независимых данных Y_1 и Y_2, равномерно распределенных среди тех обратимых вычетов по модулю N, которые являются G-тыми степенями по модулю N, вероятность получения Y_1 маскировкой X равна вероятности получения Y_2 маскировкой X. Если уровень маскировки близок к единице, то практически каждые замаскированные данные могут с равной вероятностью соответствовать практически каждым исходным данным, что обеспечивает непрослеживаемость. Меньшие значения уровня маскировки обеспечивают меньшую непрослеживаемость. Если, например уровень маскировки близок к одной трети, то при большом числе исходных данных подписывающая сторона может связать, в общем случае, индивидуальные исходные данные с одной из трех групп замаскированных данных. При этом внутри каждой из трех групп все соответствия между исходными данными и замаскированными данными будут равновероятны. Приемлемость такой непрослеживаемости определяется на практике по решаемой задаче.

Наперед заданный уровень маскировки обеспечивают, в частности, выбором RSA-модуля, соответствующего в точности двух секретным множителям P и Q и

выбором маскирующего множителя G кратным как наибольшему общему делителю чисел P-1 и Q-1, так и всем тем делителям каждого из чисел P-1 и Q-1, которые меньше подходящей наперед заданной границы U.

Выбор подходящей границы U, в частности, обеспечен тем, что в случае выбора в точности двух секретных множителей P и Q и такого маскирующего множителя G, который кратен как наибольшему общему делителю чисел P-1 и Q-1, так и всем тем делителям каждого из чисел P-1 и Q-1, которые меньше U, уровень маскировки больше, чем $(1 - \mathrm{Log}(N)/[U\cdot\mathrm{Log}(U + 1)])^2$. Например, если RSA-модуль имеет размер в 1024 бита и $U = 10^8$ уровень маскировки больше, чем $1 - 4\cdot10^{-7}$. Эта оценка подтверждается тем, что уровень маскировки не меньше, чем $(1 - W)^2$, где W вероятность того, что множество всех замаскированных данных, которые могут быть созданы на основе случайных и равномерно распределенных среди обратимых вычетов по модулю N исходных данных M, то есть множество обратимых вычетов вида $M^R \pmod N$, где R пробегает все целые числа кратные G, совпадает с группой Z всех обратимых вычетов вида $C^G \pmod N$, где C пробегает все обратимые вычеты по модулю N. Вероятность W не превосходит $1 - \prod(1 - L^{-1})$, где произведение берется по всем простым делителям L числа $(P - 1)\cdot(Q - 1)$, большим U. В частности, вероятность W меньше, чем $\mathrm{Log}(N)/[U\cdot\mathrm{Log}(U + 1)]$.

Кратность маскирующего множителя G всем тем делителям каждого из чисел P-1 и Q-1, которые меньше наперед заданной границы U, обеспечивают, в частности, тем, что при выборе секретных множителей P и Q их тестируют на сравнимость с единицей по модулю всех тех делителей, которые больше двух и меньше U, а по тестированию маскирующий множитель выбирают кратным всем тем делителям, которые меньше U, и по модулю которых сравним с единицей, по меньшей мере, один из выбранных секретных множителей.

Помимо этого, кратность маскирующего множителя G всем тем делителям каждого из чисел P-1 и Q-1, которые меньше наперед заданной границы U, обеспечивают, в частности, тем, что выбирают такие секретные множители P и Q, для которых P-1 и Q-1 не делятся ни на один из тех делителей, которые больше двух и меньше наперед заданной границы U, и которые не являются делителями выбранного маскирующего множителя G.

Кратность маскирующего множителя G наибольшему общему делителю уменьшенных на единицу секретных множителей обеспечивают, в частности, дополнительным попарным тестированием секретных множителей на сравнимость с единицей по модулю всех тех делителей, которые больше двух. Более того, кратность маскирующего множителя G наибольшему общему делителю чисел P-1 и Q-1 может быть обеспечена тем, что маскирующий множитель G выбирают четным, а секретные множители P и Q выбирают такими, что наибольший общий делитель чисел P-1 и Q-1 равен двум.

Помимо этого, кратность маскирующего множителя G наибольшему общему делителю чисел P-1 и Q-1, обеспечивают, в частности, тем, что маскирующий множитель G выбирают кратным наибольшему из тех делителей числа N-1, который взаимно прост относительно выбранных допустимых открытых RSA-экспонент. В этом случае кратность G наибольшему общему делителю чисел P-1 и Q-1 подтверждается

тем, что N -1 делится на все общие делители P-1 и Q-1, так как N -1 = (P-1)·Q + (Q-1). Более того, кратность выбираемого маскирующего множителя G наибольшему из тех делителей числа N-1, которые взаимно просты относительно выбранных допустимых открытых RSA-экспонент, обеспечивают выбором допустимых открытых RSA-экспонент взаимно простых относительно N-1, и выбором в качестве маскирующего множителя G числа N-1.

Высокая неожидаемость способа изготовления вслепую цифровой RSA-подписи по первому варианту обеспечена, в частности произвольным выбором секретного RSA-ключа, соответствующего выбранным секретным множителям и произвольной допустимой открытой RSA-экспоненте и выбором сколь угодно большого набора допустимых открытых RSA-экспонент, каждая из которых соответствует определенному виду подписи. Выбор вида подписи, то есть открытой RSA-экспоненты, соответствующей используемому при изготовлении подписи для замаскированных данных секретному ключу может производиться подателем, подписывающей стороной, совместно подателем и подписывающей стороной или иным способом.

Кроме того, высокая неожидаемость способа изготовления вслепую цифровой RSA-подписи по первому варианту обеспечена тем, что при маскировке исходных данных не требуются сами допустимые открытые RSA-экспоненты, а требуется лишь обеспечить взаимную простоту маскировочного ключа относительно каждой допустимой открытой RSA-экспоненты. Такой выбор, даже при очень большом наборе допустимых открытых RSA-экспонент, может быть осуществлен весьма эффективно. Например, если при выборе допустимых открытых RSA-экспонент выбирают, по меньшей мере, одну базовую открытую RSA-экспоненту, а качестве допустимой открытой RSA-экспоненты принимают произвольную открытую RSA-экспоненту, делителями которой являются делители выбранных базовых открытых RSA-экспонент, то выбор маскировочного ключа взаимно простым относительно каждой допустимой открытой RSA-экспоненты осуществляют тестированием его взаимной простоты относительно каждой базовой открытой RSA-экспоненты. Множество базовых открытых RSA-экспонент может быть задано, например, явным перечислением, указанием его границ или иным способом. Например, если в качестве базовой открытой RSA-экспоненты выбрано целое число $L_1 \cdot \ldots \cdot L_k$, то набор допустимых открытых RSA-экспонент практически неограничен, так как любое целое число вида $L_1^{K1} \cdot \ldots \cdot L_k^{Kk}$, где $K_1, \ldots, K_k$ неотрицательные целые числа, может быть выбрано в качестве допустимой открытой RSA-экспоненты.

Как указано выше, непрослеживаемость в способе изготовления вслепую цифровой RSA-подписи по первому варианту обеспечена, в частности, выбором RSA-модуля, соответствующего в точности двух секретным множителям P и Q и выбором маскирующего множителя G кратным как наибольшему общему делителю чисел P-1 и Q-1, так и всем тем делителям каждого из чисел P-1 и Q-1, которые меньше подходящей наперед заданной границей U. Податели могут убедиться в этих свойствах секретных множителей и маскирующего множителя без раскрытия подписывающей стороной секретных множителей с помощью известного метода «cut and choose». А именно, подписывающая сторона выбирает первоначально большое количество наборов RSA-модулей и маскирующих множителей и опубликовывает их. Представи-

тель подателей выбирает достаточно большую часть опубликованных наборов, после чего подписывающая сторона раскрывает для каждого выбранного представителем подателей набора соответствующие секретные множители. Имея секретные множители, представитель подателей убеждается в свойствах секретных множителей и маскирующего множителя в выбранных им наборах. Тем самым, представитель подателей косвенным образом убеждается и в правильности выбора секретных множителей и маскирующего множителя и в невыбранных им наборах, один из которых подписывающая сторона и использует при изготовлении подписи.

Более того, достоверность непрослеживаемости в некоторых вариантах повышается за счет того, что свойства данных, обеспечивающих непрослеживаемость, могут быть протестированы непосредственно самим подателем, а не его представителем, причем в произвольный момент времени. А именно, как указано выше, непрослеживаемость, в частности, обеспечивается тем, что RSA-модуль является произведением в точности двух секретных множителей P и Q, и, что маскирующий множитель кратен всем тем делителям как P-1, так и Q-1, которые больше двух и меньше заданной границы U. В этом случае податель с помощью подписывающей стороны, но, не доверяя ни ей, ни третьей стороне, может убедиться в указанных свойствах RSA-модуля и маскирующего множителя. При этом подписывающая сторона не доверяет своих секретов никакой третей стороне.

Тестирование того, что RSA-модуль N является произведением в точности двух простых множителей, может быть, в частности, осуществлено следующим образом. Подписывающая сторона сообщает заинтересованным сторонам такую пару чисел (U, V) , что каждый обратимый вычет по модулю N сравним с одним из чисел {1, U, V, UV}, будучи помноженным на квадратичный вычет по модулю N. После этого податель может с помощью подписывающей стороны протестировать вышеуказанное свойство N, например, следующим способом. Податель предоставляет случайное число X подписывающей стороне, которая возвращает подателю данные Y такие, что $Y^2 \cdot X^{-1} \pmod N \in \{1, U, V, UV\}$. Каждый такой ответ уменьшает вероятность того, что N состоит более чем из двух множителей, по меньшей мере, в 2 раза. Для безопасности подписывающей стороны можно потребовать, чтобы X было либо простым числом, не превосходящим заданной границы, либо образом некоторой криптографической хэш-функции (A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997, p. 321) от указываемого тестером значения. Кроме того, если на такие запросы получены ответы для всех простых X меньше некоторой явной границы, то податель может быть уверен, что N является произведением не более чем двух простых чисел, так как если RSA-модуль N является произведением, по меньшей мере, трех простых чисел, а для каждого простого нечетного L, меньшего T, найдется такой вычет X по модулю N, что $L \cdot X^2 \pmod N$ принадлежит множеству {1, U, V, UV}, то при выполнении расширенной гипотезы Римана, которая хотя и не доказана математически, но в значительной степени проверена экспериментально, T меньше, чем $C[\mathrm{Log}\ (N)]^2$, где значение C может быть получено с помощью известных оценок (J. Oesterle, Versions effectives du theoreme de Chebotarev sous l'hypothese de Riemann generalisee, Soc. Math. De France, Asterisque 61, 1979, p. 165-167). В частности, достаточно взять C = 70.

Для проверки того, что маскирующий множитель кратен всем тем делителям как P-1, так и Q-1, которые больше двух и меньше заданной границы U, подателю достаточно для каждого целого числа L, которое меньше заданной границы, не делит маскирующий множитель G и либо является нечетным простым числом, либо равно четырем, убедиться в том, что P-1 и Q-1 не делятся на L. Для этого в случае нечетного L податель предоставляет подписывающей стороне запрос R и получает ответ $R^{1/L}$ (mod N). Каждый такой ответ на запрос уменьшает в L раз вероятность того, что P-1 или Q-1 делится на L. Для безопасности подписывающей стороны можно потребовать, чтобы R было либо меньше некоторой границы, либо образом некоторой криптографической хэш-функции от указываемого подателем значения. Кроме того, если на такие запросы получены ответы для всех простых R меньших меньше некоторой явной границы, то податель может быть уверен, что P-1 и Q-1 не имеют нечетных простых делителей L меньших заданной границы, так как если N делится на нечетное простое число P, причем P-1 делится на нечетное простое L, а для каждого вычета R по модулю N, где R меньше заданной границы T, имеется вычет A такой, что $A^L \equiv R \pmod N$, то при выполнении расширенной гипотезы Римана T меньше, чем $D(\text{Log } N)^2$, где значение D может быть получено с помощью известных оценок (J. Oesterle, Versions effectives du theoreme de Chebotarev sous l'hypothese de Riemann generalisee, Soc. Math. De France, Asterisque 61, 1979, p. 165-167). В частности, достаточно взять D = 70. Вместо проверки того, что P-1 и Q-1 не делятся на L для каждого индивидуального L достаточно проверить это свойство для такого набора чисел A_1, ..., A_s, для которого каждое простое, меньшее заданной границы, является делителем хотя бы одного из A_i. Убедиться в том, что P-1 и Q-1 не делятся на четыре податель может следующим образом. Во-первых, податель, убедившись, что P-1 и Q-1 не делятся на три, может быть уверен, что целое число (-3) не сравнимо ни с одним квадратом целого числа по модулю P и по модулю Q. Во-вторых, подписывающая сторона убеждает подателя в том, что целое число 3 является квадратом по модулю P и по модулю Q, предоставляя целое число R такое, что $R^2 \equiv 3 \pmod N$. Тем самым, податель убеждается в том, что целое число (-1) не сравнимо ни с одним квадратом целого числа как по модулю P, так и по модулю Q, и, следовательно, убеждается в том, что P-1 и Q-1 не делятся на четыре. Кроме того, убедившись в том, что P-1 и Q-1 не делятся на четыре, убедится в том, что P-1 и Q-1 не делятся на нечетное простое L податель может, проверив, что целое число X не сравнимо ни с одним квадратом целого числа по модулю P и по модулю Q, где X = L, если $L \equiv 1 \pmod 4$ и X = -L, если $L \equiv 3 \pmod 4$. Подписывающая сторона убеждает подателя в этом, предоставляя целое число R такое, что $R^2 \equiv -X \pmod N$. Это возможно примерно для половины нечетных чисел L.

Ниже дано описание способа изготовления вслепую цифровой RSA-подписи по второму варианту. Это описание предназначено для раскрытия способа изготовления вслепую цифровой RSA-подписи по второму варианту и не ограничивает рамки заявленного изобретения, описанного более полно где-либо еще в настоящей заявке.

В качестве секретных множителей RSA-модуля N подписывающая сторона выбирает простые числа подходящего размера, причем в наилучшем варианте выбирают два секретных множителя. Выбранный RSA-модуль N опубликовываются. Кроме то-

го, выбирают произвольные базовые открытые RSA-экспоненты E_1, ...,E_k, количество которых зависит от решаемой задачи. Такой выбор может быть осуществлен подателем, подписывающей стороной, совместно подателем и подписывающей стороной и иным другим способом. Помимо этого, в качестве ограничительных кратностей L_1, ..., L_k базовых открытых RSA-экспонент E_1, ..., E_k, соответственно, выбирают произвольные неотрицательные целые числа. Такой выбор может быть осуществлен подателем, подписывающей стороной, совместно подателем и подписывающей стороной и иным другим способом. В качестве допустимой открытой RSA-экспоненты принимают произвольную открытую RSA-экспоненту, составленную из выбранных базовых открытых RSA-экспонент, кратность каждой из которых берут в пределах выбранной ограничительной кратности. Иными словами, в качестве допустимых принимаются открытые RSA-экспоненты вида $E = E_1^{A1} \cdot \ldots \cdot E_k^{Ak}$, где каждая из кратностей A_1,..., A_k, с которыми базовые открытые RSA-экспоненты E_1, ..., E_k, соответственно, входят в E, представляет собой неотрицательное целое число, не превышающее ограничительной кратности L_1, ..., L_k, соответственно.

При изготовлении вслепую цифровой RSA-подписи для исходных данных M податель выбирает в качестве рандомизированного маскировочного ключа R целое число подходящего размера. Выбор рандомизированного маскировочного ключа R может быть осуществлен посредством датчика случайных чисел.

Податель создает замаскированные данные M' обработкой выбранных исходных данных данными F, полученными в качестве результата RSA-шифрования маскировочного ключа R. Замаскированные данные M' удовлетворяют соотношению $M' = F \cdot M \pmod N$ и могут быть получены посредством модулярного умножителя. Данные F получают RSA-шифрованием маскировочного ключа R шифровальным RSA-ключом, который соответствует RSA-модулю N и RSA-экспоненте U, составленной из выбранных базовых открытых RSA-экспонент E_1, ..., E_k, каждую из которых берут в выбранной ограничительной кратности L_1, ..., L_k, соответственно. Иными словами, $F = R^U \pmod N$, где $U = U_1 \cdot \ldots \cdot U_k$, а $U_1 = E_1^{L1}$, ..., $U_k = E_k^{Lk}$. В частности, RSA-шифрование при создании замаскированных данных может быть осуществлено посредством модулярного экспоненциатора.

Замаскированные данные M' предоставляются подписывающей стороне, которая создает цифровую RSA-подпись S' для замаскированных данных M' секретным RSA-ключом, соответствующего выбранным секретным множителям и произвольной допустимой открытой RSA-экспоненте V. Выбор используемого секретного RSA-ключа осуществляют произвольный выбором используемых кратностей K_1, ..., K_k базовых открытых RSA-экспонент E_1, ..., E_k, соответственно. При этом, используемые кратности K_1, ..., K_k выбирают в пределах выбранных ограничительных кратностей L_1, ..., L_k, соответственно. Иными словами, кратности K_1, ..., K_k представляют собой неотрицательные целые числа, не превышающие чисел L_1, ..., L_k, соответственно, а $V = E_1^{K1} \cdot \ldots \cdot E_k^{Kk}$. Создание цифровой RSA-подпись S' для замаскированных данных M' может быть, в частности, осуществлено посредством модулярного экспоненциатора. Созданная цифровая RSA-подпись S' для замаскированных данных M' удовлетворяет соотношению $S' \equiv (M')^D \pmod N$, где D представляет собой секретную RSA-экспоненту, соответствующую открытой RSA-экспоненте

E. В частности, цифровая RSA-подпись S' для замаскированных данных может быть создана посредством модулярного экспоненциатора. Созданная цифровая RSA-подпись S' для замаскированных данных M' предоставляется подателю.

Податель создает демаскировочный ключ T, соответствующий маскировочному ключу R и использованному при создании цифровой RSA-подписи для замаскированных данных секретному RSA-ключу, посредством RSA-шифрования маскировочного ключа шифровальным RSA-ключом, в качестве модуля которого берут RSA-модуль, а RSA-экспонента которого соответствует базовым открытым RSA-экспонентам, каждую из которых берут в кратности L_1-K_1,..., L_k-K_k, соответственно. Иными словами, демаскировочный ключ T удовлетворяет соотношению $T = R^V \pmod N$, где $V = V_1 \cdot \ldots \cdot V_k$, $V_1 = E_1^{L1-K1}$,..., $V_k = E_k^{Lk-Kk}$. В частности, RSA-шифрование при создании демаскировочного ключа может быть осуществлено посредством модулярного экспоненциатора. Демаскировку цифровой RSA-подписи S' для замаскированных данных осуществляют введением в демаскирующий преобразователь S', демаскировочного ключа T и RSA-модуля N. На выходе демаскирующего преобразователя получают данные S, удовлетворяющие соотношению $S = S' \cdot T^{-1} \pmod N$, которые и представляют собой цифровую RSA-подпись для исходных данных M.

В частности, RSA-шифрование маскировочного ключа R при создании замаскированных данных может быть осуществлено последовательными RSA-шифрованиями шифровальными RSA-ключами, в качестве модуля каждого из которых берут N, а в качестве RSA-экспоненты очередного шифровального ключа берут очередную базовую открытую RSA-экспоненту E_i в ограничительной кратности L_i, то есть RSA-экспоненту $U_i = E_i^{Li}$, где индекс i последовательно принимает значения от 1 до k. Кроме того, демаскировочный ключ T может быть создан последовательными RSA-шифрованиями шифровальными RSA-ключами, в качестве модуля каждого из которых берут RSA-модуль N, а в качестве RSA-экспоненты очередного шифровального ключа берут очередную базовую открытую RSA-экспоненту E_i в кратности L_i-K_i, то есть RSA-экспоненту $V_i = E_i^{Li-Ki}$, где индекс i последовательно принимает значения от 1 до k.

Предложено устройство для реализации заявленного способа изготовления цифровой RSA-подписи. Ниже дано описание предложенного устройства, которое предназначено для раскрытия заявленного устройства и не ограничивает рамки заявленного изобретения, описанного более полно где-либо еще в настоящей заявке.

В приведенном описании под вычислителем частного имеется в виду устройство со входами делимого и делителя, причем если на вход делимого подано целое число X, а на вход делителя подано положительное целое число Y, то на выходе появляется неполное частное от деления X на Y, то есть такое целое число Z, что $0 \le X - Y \cdot Z < Y$. Под вычислителем остатка имеется в виду устройство с аргументным и модульным входами, причем если на аргументный вход подано целое число X, на модульный вход подано положительное целое число Y, то на выходе появляется остаток от деления X на Y, то есть целое число Z в диапазоне от 0 до Y - 1 такое, что X – Z делится нацело на Y. Такие вычислители частного и вычислители остатка хорошо известны.

Описание проиллюстрировано Фиг.1, на которой изображено устройство для из-

готовления вслепую цифровой RSA-подписи, содержащее блок выбора маскировочного ключа 1, блок маскировки 2, блок подписи 3 и блок демаскировки 4. Блок выбора маскировочного ключа содержит датчик случайных чисел 5 и арифметический контроллер 6, имеющий вход недопустимых делителей 7, вход обязательных делителей 8 и вход пробных данных 9, причем выход датчика случайных чисел соединен со входом пробных данных 9 арифметического контроллера, а выход арифметического контроллера 6 соединен с выходом блока создания маскировочного ключа. Блок маскировки 2 имеет вход исходных данных 10, модульный вход 11, вход маскировочного ключа 12 и содержит не показанный на Фиг.1 модулярный экспоненциатор, причем вход исходных данных 10, вход маскировочного ключа 12 и модульный вход 11 блока маскировки соединены соответственно с базовым входом, экспонентным входом и модульным входом модулярного экспоненциатора. Блок подписи 3 имеет вход секретного ключа 13 и вход данных подписи 14, причем вход данных подписи 14 блока подписи 3 соединен с выходом блока маскировки 2. Блок демаскировки 4 имеет вход данных демаскировки 15, модульный вход 16, экспонентный вход 17, вход маскировочного ключа 18 и вход исходных данных 19 и содержит не показанный на Фиг.1 модулярный мультипликативный евклидов преобразователь (ММЕП), причем модульный вход 16 соединен с модульным входом ММЕП, вход исходных данных 19 соединен с одним из базовых входов ММЕП, а вход данных демаскировки 15 соединен с другим базовым входом ММЕП, вход маскировочного ключа 18 соединен с экспонентным входом ММЕП, соответствующим базовому входу ММЕП соединенному с входом данных демаскировки15, а экспонентный вход 17 соединен с экспонентным входом ММЕП, соответствующим базовому входу ММЕП соединенному с входом исходных данных 19, а выход ММЕП соединен с выходом блока демаскировки.

Под арифметическим контроллером заявитель имеет в виду устройство, обеспечивающее заданные арифметические свойства выходных данных устройства, работу которого контролирует арифметический контроллер. В частности, в приведенном описании арифметический контроллер обеспечивает взаимную простоту выходных данных блока выбора маскировочного ключа относительно целых чисел, поданных на первый ограничительный вход арифметического контроллера, и делимость выходных данных блока выбора маскировочного ключа на целое число, поданное на второй его ограничительный вход.

Посредством предложенного устройства податель, при участии подписывающей стороны, может изготовить вслепую цифровую RSA-подпись для исходных данных по первому варианту заявленного способа. Для этого податель вводит исходные данные M на вход исходных данных, а известный из сообщения подписывающей стороны RSA-модуль N на модульный вход блока маскировки. Кроме того, податель вводит базовые открытые RSA-экспоненты на первый ограничительный вход арифметического контроллера, а маскирующий множитель на второй ограничительный вход арифметического контроллера. Маскировочный ключ R появляется на выходе блока выбора маскировочного ключа и поступает на вход маскировочного ключа блока маскировки, на выходе которого появляются замаскированные данные M'. Подписывающая сторона вводит на вход секретного ключа блока подписи исполь-

зуемый секретный RSA-ключ. На вход данных подписи блока подписи поступают замаскированные данные M', а на выходе блока подписи появляется цифровая RSA-подпись S' для замаскированных данных M', которая поступает на вход данных демаскировки блока демаскировки. Кроме того, податель вводит на модульный вход, вход исходных данных и экспонентный вход блока демаскировки, соответственно, RSA-модуль N, исходные данные M и открытую RSA-экспоненту E, соответствующую использованному секретному RSA-ключу. Помимо этого, на вход маскировочного ключа блока демаскировки поступает маскировочный ключ R с выхода блока выбора маскировочного ключа. На выходе блока демаскировки появляется цифровая RSA-подпись S для исходных данных.

Краткое описание фигур чертежей

В дальнейшем предлагаемое изобретение поясняется описанием конкретных примеров его выполнения и прилагаемыми чертежами, на которых:

Фиг.1 изображает устройство для изготовления вслепую цифровой RSA-подписи;

Фиг.2 изображает арифметический контроллер;

Фиг.3 изображает модулярный мультипликативный евклидов преобразователь.

Лучший вариант осуществления изобретения

В лучшем варианте осуществления способа изготовления вслепую цифровой RSA-подписи по первому варианту задают уровень маскировки W, определяемый по решаемой задаче. По заданному уровню маскировки задают границу U, достаточную для обеспечения заданного уровня маскировки. Граница U может быть определена с помощью формул, которые связывают ее с уровнем маскировки и приведены при раскрытии изобретения. Кроме того, в качестве базовых открытых RSA-экспонент выбирают несколько нечетных целых чисел, количество которых определяют по решаемой задаче, а в качестве допустимой открытой RSA-экспоненты принимают произвольную открытую RSA-экспоненту, делителями которой являются делители выбранных базовых открытых RSA-экспонент. Подписывающая сторона выбирает в качестве секретных множителей такие два простых числа P и Q подходящего размера, для которых каждое из целых чисел P-1 и Q-1 не имеет делителей, больших 2 и меньших заданной границы U, и взаимно просто относительно каждой из выбранных базовых открытых RSA-экспонент. Выбор таких простых чисел может быть осуществлен, например, тестированием пробных простых чисел, которые получают с помощью датчиков случайных чисел известными способами. RSA-модуль N образуют произведением выбранных секретных множителей. Выбранный RSA-модуль N, выбранные базовые допустимые экспоненты и выбранная граница U опубликовываются. В качестве маскирующего множителя G выбирают наибольший из тех делителей уменьшенного на единицу RSA-модуля, которые взаимно просты относительно выбранных допустимых открытых RSA-экспонент.

Податель, выбирает рандомизированный маскировочный ключ R, как произведение целого числа подходящего размера, полученного на выходе криптографического датчика случайных чисел (A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997, p. 185) с равномерным распределением и маскирующего множителя.

Податель производит маскировку исходных данных M, создавая на их основе за-

маскированные данные M', посредством RSA-шифрования исходных данных шифровальным RSA-ключом с модулем N и экспонентой R. Созданные замаскированные данные M' предоставляют подписывающей стороне. Подписывающая сторона осуществляет выбор вида подписи, то есть выбор допустимой открытой RSA-экспоненты E, соответствующей используемому при изготовлении подписи для замаскированных данных секретному ключу и создает цифровую RSA-подпись S' для замаскированных данных M' секретным RSA-ключом, соответствующим выбранной открытой RSA-экспоненте E. Созданная цифровая RSA-подпись S' для замаскированных данных M' предоставляется подателю вместе с информацией о выбранной допустимой открытой RSA-экспоненты E, после чего податель завершает изготовление цифровой RSA-подписи S для исходных данных M демаскировкой S' посредством демаскирующего преобразователя.

Свойство подписи цифровой RSA-подписи для исходных данных M может быть подтверждено для полученных на выходе демаскирующего преобразователя данных S как после демаскировки непосредственной проверкой, так и до демаскировки проверкой того, что S' удовлетворяет свойству цифровой RSA-подписи для замаскированных данных M'.

Кроме того, податель может убедиться в обеспечении заданного уровня маскировки, убедившись, одним из описанных при раскрытии изобретения способов, в том, что опубликованный RSA-модуль составлен в точности из двух секретных множителей, а каждый из секретных множителей не сравним с единицей по модулю делителей больших двух и меньших опубликованной границы U.

Возможность реализации вышеописанного лучшего варианта осуществления способа изготовления вслепую цифровой RSA-подписи по первому варианту поясняется следующим примером.

Пример 1.

Предположим, что используются секретные множители размером 512 битов, и считается достаточным уровень маскировки $W=1-4\cdot10^{-7}$. С помощью формул, которые приведены при раскрытии изобретения, задают границу $U=10^{-8}$, достаточную для обеспечения заданного уровня маскировки. В качестве базовых открытых RSA-экспонент выбирают целые числа $E_1=3$, $E_2=5$, $E_3=7$. Подписывающая сторона выбирает в качестве секретных множителей два простых числа P и Q размером 512 битов и RSA-модуль $N = P\cdot Q$, который получают по P и Q посредством умножителя. При этом секретные множители выбирают такими, что каждое из целых чисел P-1 и Q-1 не имеет делителей больших 2 и меньших заданной границы U, а каждое из целых чисел P-1 и Q-1 взаимно просто относительно каждой базовой открытой RSA-экспоненты. Такие секретные множители выбирают посредством тестирования указанных свойств пробных секретных множителей, в качестве которых берут простые числа размера 512 битов, полученные с помощью криптографического датчика случайных чисел. Выбор таких простых чисел и их тестирование осуществляют одним из известных способов (A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997, p. 145). Выбранный RSA-модуль N и выбранные базовые допустимые экспоненты опубликовываются.

Для выбора маскирующего множителя используют вычитатель, на вход умень-

шаемого которого вводят RSA-модуль N, а на вход вычитаемого которого вводят целое число 1. На выходе вычитателя получают целое число N-1, которое принимают в качестве пробного маскирующего множителя. Пробный маскирующий множитель подвергают последовательной обработке каждой базовой открытой RSA-экспонентой. Обработка пробного маскирующего множителя очередной базовой открытой RSA-экспонентой E_i происходит в несколько этапов, каждый из которых состоит в следующем. В случае взаимной простоты пробного маскирующего множителя и E_i, которую определяют посредством тестера взаимной простоты, считают обработку пробного маскирующего множителя очередной базовой открытой RSA-экспонентой E_i законченной и переходят к обработке пробного маскирующего множителя очередной базовой открытой RSA-экспонентой. В случае отсутствия взаимной простоты пробного маскирующего множителя и E_i пробный маскирующий множитель вводят на вход делимого, а E_i на вход делителя вычислителя частного, выход которого принимают в качестве нового пробного маскирующего множителя. После этого переходят к очередному этапу обработки пробного маскирующего множителя базовой открытой RSA-экспонентой E_i. Обработанный каждой базовой открытой RSA-экспонентой пробный маскирующий множитель принимают в качестве маскирующего множителя G.

Податель получает рандомизированный маскировочный ключ R на выходе умножителя, на входы которого подают маскирующий множитель G и целое число подходящего размера, которое взаимно просто относительно каждой из базовых открытых RSA-экспонент. Такое целое число целое число получают тестированием взаимной простоты пробных целых чисел, получаемых на выходе криптографического датчика случайных чисел с равномерным распределением, относительно каждой из базовых открытых RSA-экспонент. Податель выбирает в качестве исходных данных M произвольное целое число, представляющее подлежащие подписанию данные. Исходные данные M вводят на базовый вход модулярного экспоненциатора, маскировочный ключ R на экспонентный вход модулярного экспоненциатора, а RSA-модуль N на модульный вход модулярного экспоненциатора. На выходе модулярного экспоненциатора получают замаскированные данные M', которые доставляют подписывающей стороне посредством телекоммуникационных сетей.

Подписывающая сторона выбирает в качестве секретного ключа пару, состоящую из RSA-модуля N и секретной RSA-экспоненты D, причем выбор секретной RSA-экспоненты осуществляют выбором произвольных неотрицательных целых чисел K_1, K_2 и K_3 в качестве кратностей базовых открытых RSA-экспонент E_1, E_2 и E_3, соответственно. Секретную RSA-экспоненту D получают посредством модулярного экспоненциатора и модулярного умножителя, причем полученная секретная RSA-экспонента удовлетворяет соотношению $D \equiv D_1^{K1} \cdot D_2^{K2} \cdot D_3^{K3} (\mathrm{mod}\ (P-1)\cdot(Q-1))$. При этом D_1 получают на выходе модулярного инвертора, на модульный вход которого подают целое число $(P-1)\cdot(Q-1)$, на аргументный вход базовую открытую RSA-экспоненту E_1. Аналогично D_2 получают по E_2, а D_3 получают по E_3. Замаскированные данные M' вводят на базовый вход модулярного экспоненциатора, секретную экспоненту D вводят на экспонентный вход модулярного экспоненциатора, а RSA-модуль N вводят на модульный вход модулярного экспоненциатора. Полученные на

выходе модулярного экспоненциатора данные S' предоставляют подателю в качестве цифровой RSA-подписи для замаскированных данных вместе с выбранными кратностями K_1, K_2 и K_3.

Податель получает посредством модулярных экспоненциаторов и модулярного умножителя открытую RSA-экспоненту E, удовлетворяющую соотношению $E \equiv E_1^{K1} \cdot E_2^{K2} \cdot E_3^{K3} \pmod{(P-1)\cdot(Q-1)}$. При демаскировке цифровую RSA-подпись S' для замаскированных данных M' подают на первый базовый вход модулярного мультипликативного евклидова преобразователя, исходные данные M на второй базовый вход ММЕП, маскировочный ключ R на первый экспонентный вход ММЕП, открытую RSA-экспоненту E на второй экспонентный вход ММЕП, а RSA-модуль N на модульный вход ММЕП. На выходе ММЕП появляются данные S, которые и представляют собой цифровую RSA-подпись для исходных данных M.

Для подтверждения свойства подписи цифровой RSA-подписи для исходных данных M податель вводит данные S, полученные на выходе демаскирующего преобразователя, на базовый вход модулярного экспоненциатора, открытую RSA-экспоненту E на экспонентный вход модулярного экспоненциатора, а RSA-модуль N на модульный вход модулярного экспоненциатора. Выходные данные модулярного экспоненциатора вводят на вход компаратора, на другой вход которого вводят исходные данные M. Если на выходе компаратора получают логическое значение "Истина", то данные S, полученные на выходе демаскирующего преобразователя, принимают в качестве цифровой RSA-подписи для исходных данных M.

В лучшем варианте осуществления способа изготовления вслепую цифровой RSA-подписи по второму варианту подписывающая сторона выбирает в качестве базовых открытых RSA-экспонент несколько нечетных попарно взаимно простых целых чисел $E_1,\ldots, E_k$, количество которых определяют по решаемой задаче, а в качестве секретных множителей два простых числа P и Q подходящего размера, для которых каждое из целых чисел P-1 и Q-1 взаимно просто относительно каждой из выбранных базовых открытых RSA-экспонент. Выбор таких простых чисел может быть осуществлен, например, тестированием пробных простых чисел, которые получают с помощью датчиков случайных чисел известными способами. RSA-модуль N образуют произведением выбранных секретных множителей. Выбранные базовые допустимые экспоненты опубликовываются. Ограничительные кратности $L_1, \ldots, L_k$ базовых открытых RSA-экспонент $E_1, \ldots, E_k$, соответственно, выбирает податель по решаемой задаче. Рандомизированный маскировочный ключ R податель выбирает посредством криптографического датчика случайных чисел с равномерным распределением.

Возможность реализации вышеописанного лучшего варианта осуществления способа изготовления вслепую цифровой RSA-подписи по второму варианту поясняется следующим примером.

Пример 2.

Подписывающая сторона в качестве базовых открытых RSA-экспонент выбирает целые числа $E_1=3$, $E_2=5$, $E_3=7$. Подписывающая сторона выбирает в качестве секретных множителей два простых числа P и Q размером 512 битов и RSA-модуль $N = P \cdot Q$, который получают по P и Q посредством умножителя. При этом секретные

множители выбирают такими, что каждое из целых чисел P-1, Q-1 и N-1 взаимно просто относительно каждой базовой открытой RSA-экспоненты. Такие секретные множители выбирают посредством тестирования указанных свойств пробных секретных множителей, в качестве которых берут простые числа размера 512 битов, полученные с помощью криптографического датчика случайных чисел. Выбор таких простых чисел и их тестирование осуществляют одним из известных способов (A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997, p. 145). Выбранный RSA-модуль N и выбранные базовые допустимые экспоненты опубликовываются.

В качестве исходных данных M податель берет произвольное целое число, представляющее предназначенные для подписания данные. В качестве ограничительных кратностей L_1, L_2, L_3 базовых открытых RSA-экспонент E_1, E_2, E_3, соответственно, податель выбирает произвольные неотрицательные целые числа в зависимости от решаемой задачи, в этом примере $L_1 = 100$, $L_2 = 50$, $L_3 = 10$. В качестве рандомизированного маскировочного ключа R податель берет целое число размера 1024 бита, появляющееся на выходе криптографического датчика случайных чисел с равномерным распределением.

Податель получает по маскировочному ключу R цепочку данных F_0, F_1,..., F_L, где $L=L_1 + L_2 + L_3$. При этом в качестве данных F_0 берут маскировочный ключ R, а очередные данные F_j, получают на выходе модулярного экспоненциатора, на модульный вход которого подают RSA-модуль N, на базовый вход которого подают предыдущий элемент цепочки, а на экспонентный вход которого подают L_1 раз RSA-экспоненту E_1, L_2 раз RSA-экспоненту E_2, и L_3 раз RSA-экспоненту E_3. Полученные данные F_L вводят на аргументный вход модулярного умножителя, на другой вход которого вводят исходные данные M, а на модульный вход которого вводят RSA-модуль N. На выходе модулярного умножителя получают замаскированные данные M', которые доставляют подписывающей стороне посредством телекоммуникационных сетей, вместе с информацией о выбранных ограничительных кратностях L_1, L_1, L_3.

Подписывающая сторона выбирает используемые кратности K_1, K_1, K_3 базовых открытых RSA-экспонент E_1, E_2, E_3, соответственно. При этом используемые кратности K_1, K_1, K_3 выбирают в пределах выбранных ограничительных кратностей L_1, L_1, L_3, соответственно. В этом примере выбирают $K_1 = 90$, $K_2 = 40$, $K_3 = 1$. Секретный RSA-ключ и цифровую RSA-подпись S' для замаскированных данных M' создают так же, как в примере 1.

Податель получает по маскировочному ключу R цепочку данных T_0, T_1,..., T_I, где $I = L_1\text{-}K_1 + L_2\text{-}K_2 + L_3\text{-}K_3$. При этом в качестве данных T_0 берут маскировочный ключ R, а очередные данные T_j, получают на выходе модулярного экспоненциатора, на модульный вход которого подают RSA-модуль N, на базовый вход которого подают предыдущий элемент цепочки, а на экспонентный вход которого подают $(L_1\text{-}K_1)$ раз RSA-экспоненту E_1, $(L_2\text{-}K_2)$ раз RSA-экспоненту E_2, и $(L_3\text{-}K_3)$ раз RSA-экспоненту E_3. Полученные данные T_I берут в качестве демаскировочного ключа T. В качестве демаскирующего преобразователя используют модулярный вычислитель частного. При демаскировке цифровую RSA-подпись S' для замаскированных данных, дема-

скировочный ключ T и RSA-модуль N вводят, соответственно, на вход делимого, вход делителя и модульный вход модулярного вычислителя частного. На выходе демаскирующего преобразователя получают цифровую RSA-подпись для исходных данных M.

В лучшем варианте реализации устройства для изготовления вслепую цифровой RSA-подписи в качестве датчика случайных чисел используют криптографический датчик случайных чисел с равномерным распределением. Возможность реализации устройства для изготовления вслепую цифровой RSA-подписи поясняется следующим конкретным примером, который проиллюстрирован Фиг.1, описанной при раскрытии заявленного устройства.

Пример 3.

Хотя в реальных системах цифровой RSA-подписи используются секретные множители, состоящие из многих десятков цифр, для простоты в этом примере секретные множители состоят из небольшого количества цифр. Предположим, что подписывающая сторона выбрала секретные множители P = 419 и Q = 863, RSA-модуль N = 361597, открытую базовую RSA-экспоненту E = 3, после чего сообщила N и E всем заинтересованным сторонам. Предположим, что податель желает изготовить вслепую цифровую RSA-подпись исходных данных M = 123456. Для этого податель вводит исходные данные M на вход исходных данных 10, а RSA-модуль N на модульный вход 11 блока маскировки 2. Кроме того, податель вводит базовую открытую RSA-экспоненту E на первый ограничительный вход 7 арифметического контроллера 6, а уменьшенный на единицу RSA-модуль N, то есть целое число 123455, на второй ограничительный вход 8 арифметического контроллера 6. Предположим, что на выходе блока выбора маскировочного ключа 111 появилось целое число R = 901. Целое число R поступает на вход маскировочного ключа 12 блока маскировки 2, на выходе которого появляются данные M' = 237367. Подписывающая сторона вводит на вход секретного ключа 13 блока подписи 3 секретный ключ (N, D), соответствующий открытой RSA-экспоненте E=3, то есть D = 240211. На вход данных подписи 14 блока подписи 3 поступает целое число M', а на выходе блока подписи 3 появляется целое число T' = 88275, которое поступает на вход данных демаскировки 15 блока демаскировки 4. Кроме того, податель вводит на модульный вход 16, вход исходных данных 19 и экспонентный вход 17 блока демаскировки 4, соответственно, RSA-модуль N, исходные данные M и открытую RSA-экспоненту E = 3. Помимо этого, на вход маскировочного ключа 18 блока демаскировки 4 поступает целое число R. На выходе блока демаскировки появляются данные T = 150340, представляющие собой цифровую RSA-подпись для исходных данных M.

Возможность реализации блока выбора маскировочного ключа устройства для изготовления вслепую цифровой RSA-подписи и относящегося к нему арифметического контроллера поясняется следующим примером.

Пример 4.

Пример проиллюстрирован Фиг.2 и Фиг.1. На Фиг.2 изображен арифметический контроллер 6, который имеет вход недопустимых делителей 7, вход обязательных делителей 8, вход пробных данных 9, содержит умножитель 20 и тестер взаимной простоты 21. При этом вход недопустимых делителей 7 соединен со входом 22 тес-

тера взаимной простоты, вход пробных данных 9 соединен со входом 23 тестера взаимной простоты и с аргументным входом 24 умножителя 20, выход тестера взаимной простоты 21 соединен со входом загрузки 25 умножителя 20, вход обязательных делителей 8 арифметического контроллера 6 соединен с аргументным входом 26 умножителя 20, выход которого соединен с выходом арифметического контроллера 6.

Конкретный пример работы блока выбора маскировочного ключа 1 вышеописанного устройства для изготовления вслепую цифровой RSA-подписи состоит в следующем. Предположим, что на выходе датчика случайных чисел 5 появляется целое число 1234, которое попадает на вход пробных данных 9 арифметического контроллера 6. Предположим, что на первый ограничительный вход 7 подано целое число 7, а на второй ограничительный вход 8 подано целое число 5. Целые числа 1234 и 7 поступают, соответственно, на входы 23 и 22 тестера взаимной простоты 21, на выходе которого появляется логическое значение 1 («истина»). Это значение поступает на вход загрузки 25 умножителя 20, после чего умножитель 20 вбирает данные 1234 и 5, поданные соответственно на его аргументные входы 24 и 26. На выходе умножителя 20 появляется целое число $1234 \cdot 5 = 6170$, которое и появляется на выходе арифметического контроллера 6 и на выходе блока выбора маскировочного ключа 1.

Для подтверждения реализуемости в приведенном ниже примере заявитель приводит пример конкретной реализации ММЕП и его работы.

Пример 5.

Пример проиллюстрирован Фиг.3. На Фиг.3 изображен ММЕП 27, который имеет базовый вход 28 и соответствующий ему экспонентный вход 29, базовый вход 30 и соответствующий ему экспонентный вход 31, модульный вход 32 и один выход. ММЕП содержит регистры 33-40, умножитель 41, модулярный экспоненциатор 42, вычитатель 43, модулярный вычислитель частного 44, вычислитель частного 45, компаратор 46 и элемент «НЕ» 47. При этом базовый вход 28 соединен со входом данных регистра 35, второй базовый вход 30 соединен со входом данных регистра 36, экспонентный вход 29 соединен со входом данных регистра 33, экспонентный вход 31 соединен со входом данных регистра 34, а модульный вход 32 соединен с модульными входами модулярного вычислителя частного 44 и модулярного экспоненциатора 42. Кроме этого ММЕП 27 содержит не показанный на Фиг.3 регистр выхода, выход которого соединен с выходом ММЕП 27, а вход данных регистра выхода соединен с выходом регистра 39. Выход регистра 33 соединен с входом делимого 48 вычислителя частного 45 и со входом уменьшаемого 49 вычитателя 43. Выход регистра 34 соединен со входом делителя 50 вычислителя частного 45, со входом 51 умножителя 41 и со входом данных регистра 37. Выход регистра 35 соединен со входом делимого 52 модулярного вычислителя частного 44. Выход регистра 36 соединен со входом 53 модулярного экспоненциатора 42 и со входом данных регистра 39. Выход вычислителя частного 45 соединен со входом 54 умножителя 41 и с экспонентным входом 55 модулярного экспоненциатора 42. Выход умножителя 41 соединен со входом вычитаемого 56 вычитателя 43, а выход модулярного экспоненциатора 42 соединен со входом делителя 57 модулярного вычислителя частного 44. Выход вычитателя 43 соединен со входом данных регистра 38, а выход модулярного вычислителя частного 44 соединен со входом данных регистра 40. Выход регистра

37 соединен со входом данных регистра 33, выход регистра 38 соединен со входом данных регистра 34, выход регистра 39 соединен со входом данных регистра 35, но эти соединения не показаны. Выход регистра 38 соединен со входом 58 компаратора 46, а выход компаратора 46 соединен со входом загрузки регистра выхода и со входом логического элемента «НЕ» 47, выход которого соединен со входами загрузки регистров 33-36, но эти соединения не показаны. Кроме того, ММЕП 27 включает схему начальной установки регистров 33-36, схему подачи нуля на вход 59 компаратора 46 и схему синхронизации, обеспечивающую пошаговый режим работы ММЕП, но эти схемы на Фиг.3 не показаны.

Конкретный пример работы ММЕП 27 состоит в следующем. На базовый вход 28 подают данные X=11, на базовый вход 30 подают данные Y = 17, на экспонентный вход 29 подают данные A = 7, на экспонентный вход 31 подают данные B = 5, а на модульный вход 32 подают данные N = 37. После этого схема начальной установки загружает в регистры 33-36 значения $R_1 = A = 7$ со входа 29, $R_2 = B = 5$ со входа 31, $U_1 = X = 11$, $U_2 = Y = 17$, соответственно. Работа ММЕП проходит пошагово, что обеспечивается схемой синхронизации.

Работа ММЕП 27 на первом шаге происходит следующим образом. На вход делимого 48 и вход делителя 50 вычислителя частного 45, соответственно, поступают данные $R_1 = 7$ из регистра 33 и $R_2 = 5$ из регистра 34, а на его выходе появляется неполное частное $Q = 1$ от деления $R_1 = 7$ на $R_2 = 5$. Данные $Q = 1$ появляются на входе 54 умножителя 41 и на экспонентном входе 55 модулярного экспоненциатора 42. На вход 51 умножителя 41 поступают данные $R_2 = 5$ из регистра 34, а на его выходе появляются данные $Q \cdot R_2 = 5$, которые и поступают на вход вычитаемого 56 вычитателя 43. На вход уменьшаемого 49 вычитателя 43 поступают данные $R_1 = 7$ из регистра 33, а на выходе вычитателя 43 появляются данные $R_1 - Q \cdot R_2 = 2$, которые поступают в регистр 38. В регистр 37 поступают данные $R_2 = 5$ из регистра 34. На базовый вход 53 модулярного экспоненциатора 42 подаются данные $U_2 = 17$ из регистра 36, на модульный вход модулярного экспоненциатора 42 подаются данные N = 37 с модульного входа 32, а на его выходе появляются данные $S = U_2^Q \pmod N = 17$, которые и попадают на вход делителя 57 модулярного вычислителя частного 44. На вход делимого 52 модулярного вычислителя частного 44 подаются данные $U_1 = 11$ из регистра 35, а на выходе модулярного вычислителя частного 44 появляются данные $U_1 \cdot S^{-1} \pmod N = 5$, которые поступают в регистр 40. В регистр 39 поступают данные $U_2 = 17$ из регистра 36. На вход 58 компаратора 46 из регистра 38 поступают данные W = 2, на вход 59 компаратора 46 схемой подачи нуля подается ноль, а на его выходе появляется логическое значение 0 («ложь»), которое попадает на входы загрузки регистров первого и второго выходов (тем самым по входам данных этих регистров в них ничего не поступает) и в логический элемент «НЕ» 47. На выходе логического элемента «НЕ» 47 появляется логическое значение 1 («истина»), которая и подается на входы загрузки регистров 33-36, после чего в этих регистрах оказываются значения $R_1 = 5$, $R_2 = 2$, $U_1 = 17$, $U_2 = 5$, соответственно, из регистров 35-38. На этом первый шаг заканчивается и начинается второй шаг.

После второго шага в регистрах 33-36 оказываются значения $R_1 = 2$, $R_2 = 1$, $U_1 = 5$, $U_2 = 14$, после чего начинается третий шаг. В ходе третьего шага в регистрах 35-38

оказываются значения 1, 0, 14, 17, соответственно. После этого на выходе компаратора 46 появляется логическое значение 1 («истина»), которое поступает на вход загрузки регистра выхода, после чего в этот регистр поступают данные Z = 14 из регистра 39, которые и появляются на выходе ММЕП 27.

Варианты осуществления изобретения

Заявитель отмечает вариант способа изготовления вслепую цифровой RSA-подписи по первому варианту, в котором в качестве маскирующего множителя G выбирают целое число два, что приводит к ускорению маскировки и демаскировки. В этом варианте подписывающая сторона выбирает в качестве секретных множителей такие два простых числа P и Q, для которых каждое из целых чисел P-1 и Q-1 не имеет делителей, больших 2 и меньших U, и взаимно просто относительно каждой из базовых открытых RSA-экспонент, а, кроме того, числа P-1 и Q-1 не имеют общих делителей больших двух. Выбор таких простых чисел может быть осуществлен дополнительным тестированием для пробных простых чисел равенства двум наибольшего общего делителя чисел P-1 и Q-1. Рандомизированный маскировочный ключ R выбирают установкой в единицу младшего бита целого числа подходящего размера, полученного на выходе криптографического датчика случайных чисел с равномерным распределением. В этом случае податель может убедиться в обеспечении заданного уровня маскировки, убедившись, описанным при раскрытии изобретения способом "cut and choose", в том, что каждый из секретных множителей не сравним с единицей по модулю делителей, больших двух и меньших опубликованной границы U, и в том, что уменьшенные на единицу секретные множители не имеют общих делителей больших двух.

В качестве других частных случаев реализации способа изготовления вслепую цифровой RSA-подписи по первому варианту заявитель отмечает возможность выбора таких секретных множителей и маскирующего множителя, при котором маскирующий множитель либо не кратен наибольшему общему делителю уменьшенных на единицу секретных множителей, либо не кратен всем делителям каждого из уменьшенных на единицу секретных множителей, меньших наперед заданной границы. Например, в качестве маскирующего множителя может быть взято целое число один. Хотя такой выбор и не позволяет обеспечить произвольную близость уровня маскировки к единице, тем не менее в некоторых практических ситуациях непрослеживаемость, достигаемая таким выбором, может быть признана достаточной.

В частном случае реализации в качестве исходных данных податель может выбрать имеющуюся у него цифровую RSA-подпись некоторых более ранних исходных данных и тем самым получить цифровую RSA-подпись более ранних исходных данных, соответствующую произведению открытых RSA-экспонент.

Кроме того, после изготовления цифровой RSA-подписи для исходных данных, соответствующей открытой RSA-экспоненте E, податель может без помощи подписывающей стороны изготовить цифровую RSA-подпись для исходных данных, соответствующую произвольной открытой RSA-экспоненте, являющейся делителем E.

В качестве частных случаев реализации способа изготовления цифровой подписи по каждому из вариантов заявитель отмечает возможность шифрования, дешифрования и перекодировки данных при их передаче от подателя к подписывающей сто-

роне и наоборот, которые не меняют сущности заявленного изобретения. В частности, вид подписи может зависеть от времени изготовления подписывающей стороной подписи для замаскированных данных, а также может выражать степень доверия подписывающей стороны к подателю. Кроме того, замаскированные данные при передаче от подателя к подписывающей стороне могут быть подвергнуты дополнительной маскировке, а цифровая RSA-подпись для замаскированных данных при передаче от подписывающей стороны к подателя может быть подвергнута соответствующей демаскировке.

При реализации способа изготовления цифровой подписи по каждому из вариантов свойство цифровой RSA-подписи изготовленной цифровой RSA-подписи для исходных данных может быть подтверждено как после демаскировки цифровой RSA-подписи для замаскированных данных непосредственной проверкой, так и до демаскировки проверкой того, что полученная цифровая RSA-подпись для замаскированных данных удовлетворяет свойству цифровой RSA-подписи по отношению к замаскированным данным.

Заявитель отмечает, что в частных случаях реализации устройства для изготовления вслепую цифровой RSA-подписи соединения между различными блоками могут быть выполнены посредством телекоммуникационных сетей, а сами блоки могут быть удалены друг от друга. В качестве других частных случаев устройства заявитель отмечает возможность его реализации в виде многих иных разбиений содержащихся в нем вспомогательных устройств на блоки, которые не меняют сущности заявленного изобретения. Также возможно выполнение соединения между блоками путем пропускания этих соединений через дополнительные устройства. Среди таких дополнительных устройств могут быть, в частности, шифровальные и дешифровальные устройства, а также кодирующие и декодирующие устройства. Кроме того, заявленное устройство может быть дополнено другими известными устройствами, в частности, устройствами для проверки RSA-подписи.

Промышленная применимость

Изобретение может быть использовано в электронных системах массового обслуживания, использующих цифровую подпись, в особенности таких, в которых желательна защита приватности пользователей при высоком многообразии видов подписи. В частности, изобретение может быть использовано в телекоммуникационных системах, криптографических системах, платежных системах, в банковской деятельности, в системах временных меток, в лотереях, в сетевых компьютерных играх, в системах ценных карточек и ценных документов, и во многих иных областях.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ изготовления вслепую цифровой RSA-подписи, заключающийся в выборе секретных множителей и соответствующего им RSA-модуля, выборе, по меньшей мере, одной допустимой открытой RSA-экспоненты, выборе исходных данных, выборе рандомизированного маскировочного ключа, выборе шифровального RSA-ключа, модуль которого соответствует выбранному RSA-модулю, а экспонента которого соответствует выбранному маскировочному ключу, которым осуществляют RSA-шифрование при создании замаскированных данных, произвольном выборе секретного RSA-ключа, соответствующего выбранным секретным множителям и произвольной допустимой открытой RSA-экспоненте, и создании соответствующей ему цифровой RSA-подписи для замаскированных данных, демаскировке созданной цифровой RSA-подписи для замаскированных данных, которую производят введением цифровой RSA-подписи для замаскированных данных, маскировочного ключа, RSA-модуля и открытой RSA-экспоненты, соответствующей секретному RSA-ключу, использованному при создании цифровой RSA-подписи для замаскированных данных, в демаскирующий преобразователь, выходные данные которого принимают в качестве цифровой RSA-подписи для выбранных исходных данных, *отличающийся тем, что* при создании замаскированных данных осуществляют RSA-шифрование выбранных исходных данных, при демаскировке созданной цифровой RSA-подписи для замаскированных данных дополнительно вводят в демаскирующий преобразователь выбранные исходные данные, дополнительно выбирают взаимно простой относительно каждой допустимой открытой RSA-экспоненты маскирующий множитель, а маскировочный ключ выбирают взаимно простым относительно каждой допустимой открытой RSA-экспоненты и кратным выбранному маскирующему множителю.

2. Способ изготовления вслепую цифровой RSA-подписи по п.1, *отличающийся тем, что* при демаскировке созданной цифровой RSA-подписи для замаскированных данных выбранные исходные данные, которые предварительно введены в демаскирующий преобразователь, подают на один из базовых входов содержащегося в нем модулярного мультипликативного евклидова преобразователя (ММЕП), на другой базовый вход которого подают созданную цифровую RSA-подпись для замаскированных данных, предварительно введенную в демаскирующий преобразователь, выбранный маскировочный ключ вводят на экспонентный вход ММЕП, соответствующий базовому входу, на который подают выбранные исходные данные, а предварительно введенную в демаскирующий преобразователь открытую RSA-экспоненту, соответствующую использованному при создании цифровой RSA-подписи для замаскированных данных секретному ключу, вводят на экспонентный вход ММЕП, соответствующий базовому входу, на который подают созданную цифровую RSA-подпись для замаскированных данных.

3. Способ изготовления вслепую цифровой RSA-подписи по п.1, *отличающийся тем, что* рандомизированный маскировочный ключ выбирают посредством датчика случайных чисел.

4. Способ изготовления вслепую цифровой RSA-подписи по п.3, *отличающийся тем*, выбор рандомизированного маскировочного ключа взаимно простым относи-

тельно выбранных допустимых открытых RSA-экспонент производят корректировкой выходных данных датчика случайных чисел выбранными допустимыми открытыми RSA-экспонентами.

5. Способ изготовления вслепую цифровой RSA-подписи по п.3, *отличающийся тем*, выбор рандомизированного маскировочного ключа производят тестированием взаимной простоты выходных данных датчика случайных чисел относительно выбранных допустимых открытых RSA-экспонент.

6. Способ изготовления вслепую цифровой RSA-подписи по п.1, *отличающийся тем, что* маскирующий множитель выбирают кратным наибольшему общему делителю уменьшенных на единицу секретных множителей, а также всем тем делителям, меньшим наперед заданной границы, по модулю которых сравним с единицей, по меньшей мере, один из секретных множителей.

7. Способ изготовления вслепую цифровой RSA-подписи по п.6, *отличающийся тем, что* выбор маскирующего множителя кратным наибольшему общему делителю уменьшенных на единицу секретных множителей осуществляют выбором RSA-модуля, соответствующего двум секретным множителям, и выбором маскирующего множителя кратным наибольшему из тех делителей уменьшенного на единицу RSA-модуля, которые взаимно просты относительно выбранных допустимых открытых RSA-экспонент.

8. Способ изготовления вслепую цифровой RSA-подписи по п.7, *отличающийся тем, что* выбор маскирующего множителя кратным наибольшему из тех делителей уменьшенного на единицу RSA-модуля, которые взаимно просты относительно выбранных допустимых открытых RSA-экспонент, осуществляют выбором допустимых открытых RSA-экспонент, взаимно простых относительно уменьшенного на единицу RSA-модуля, и выбором в качестве маскирующего множителя уменьшенного на единицу RSA-модуля.

9. Способ изготовления вслепую цифровой RSA-подписи по п.6, *отличающийся тем, что* выбор маскирующего множителя кратным всем тем делителям, меньшим наперед заданной границы, по модулю которых сравним с единицей, по меньшей мере, один из секретных множителей, осуществляют дополнительным тестированием секретных множителей на сравнимость с единицей по модулю всех тех делителей, которые больше двух и меньше наперед заданной границы.

10. Способ изготовления вслепую цифровой RSA-подписи по п.6, *отличающийся тем, что* выбор маскирующего множителя кратным наибольшему общему делителю уменьшенных на единицу секретных множителей осуществляют дополнительным попарным тестированием секретных множителей, которое производят при их выборе, на одновременную сравнимость с единицей по модулю всех тех делителей, которые больше двух, и выбором маскирующего множителя четным, причем при выборе секретных множителей в качестве критерия их отбора принимают одновременную попарную несравнимость с единицей по модулю всех тех делителей, которые больше двух.

11. Способ изготовления вслепую цифровой RSA-подписи по п.10, *отличающийся тем, что* дополнительное попарное тестирование секретных множителей на одновременную сравнимость с единицей по модулю всех тех делителей, которые больше

двух, осуществляют сравнением значения наибольшего общего делителя уменьшенных на единицу секретных множителей с целым числом, равным двум.

12. Способ изготовления вслепую цифровой RSA-подписи по п.1, *отличающийся тем, что* при создании замаскированных данных RSA-шифрование выбранных исходных данных осуществляют посредством модулярного экспоненциатора.

13. Способ изготовления вслепую цифровой RSA-подписи по п.1, *отличающийся тем, что* в качестве маскирующего множителя выбирают целое число равное двум, при выборе секретных множителей их дополнительно тестируют на сравнимость с единицей по модулю всех тех делителей, которые больше двух и меньше наперед заданной границы, и попарно на одновременную сравнимость с единицей по модулю всех тех делителей, которые больше двух, причем в качестве критерия отбора секретных множителей принимают несравнимость с единицей по модулю всех тех делителей, которые больше двух и меньше наперед заданной границы и одновременную попарную несравнимость с единицей по модулю всех тех делителей, которые больше двух.

14. Способ изготовления вслепую цифровой RSA-подписи по п.13, *отличающийся тем, что* при выборе секретных множителей дополнительное попарное тестирование секретных множителей на одновременную сравнимость с единицей по модулю всех тех делителей, которые больше двух, осуществляют сравнением значения наибольшего общего делителя уменьшенных на единицу секретных множителей с целым числом, равным двум.

15. Способ изготовления вслепую цифровой RSA-подписи по п.1, *отличающийся тем, что* цифровую RSA-подпись для замаскированных данных создают посредством модулярного экспоненциатора.

16. Способ изготовления вслепую цифровой RSA-подписи по п.1, *отличающийся тем, что* RSA-модуль выбирают соответствующим двум секретным множителям, допустимые открытые RSA-экспоненты выбирают взаимно простыми относительно уменьшенного на единицу RSA-модуля, при выборе секретных множителей их дополнительно тестируют на сравнимость с единицей по модулю всех тех делителей, которые больше двух и меньше наперед заданной границы, причем в качестве критерия отбора секретных множителей принимают несравнимость с единицей по модулю всех тех делителей, которые больше двух и меньше наперед заданной границы, а маскирующий множитель выбирают кратным уменьшенному на единицу RSA-модулю.

17. Способ изготовления вслепую цифровой RSA-подписи по п.16, *отличающийся тем, что* в качестве маскирующего множителя выбирают уменьшенный на единицу RSA-модуль.

18. Способ изготовления вслепую цифровой RSA-подписи по п.6, или п.13, или п.16, *отличающийся тем, что* наперед заданную границу выбирают по заданному уровню маскировки.

19. Способ изготовления вслепую цифровой RSA-подписи по п.1, *отличающийся тем, что* при выборе допустимых открытых RSA-экспонент в качестве допустимой открытой RSA-экспоненты принимают произвольную открытую RSA-экспоненту, делителями которой являются только делители произвольно выбранных базовых от-

крытых RSA-экспонент.

20. Способ изготовления вслепую цифровой RSA-подписи по п.19, *отличающийся тем, что* выбор маскировочного ключа взаимно простым относительно каждой допустимой открытой RSA-экспоненты осуществляют тестированием его взаимной простоты относительно каждой базовой открытой RSA-экспоненты.

21. Способ изготовления вслепую цифровой RSA-подписи по п.19, *отличающийся тем, что* выбор маскировочного ключа взаимно простым относительно каждой допустимой открытой RSA-экспоненты осуществляют корректировкой выходных данных датчика случайных чисел выбранными базовыми открытыми RSA-экспонентами.

22. Способ изготовления вслепую цифровой RSA-подписи, заключающийся в выборе секретных множителей и соответствующего им RSA-модуля, выборе, по меньшей мере, одной допустимой открытой RSA-экспоненты, выборе исходных данных, выборе рандомизированного маскировочного ключа, выборе шифровального RSA-ключа, модуль которого соответствует выбранному RSA-модулю, и которым при создании замаскированных данных осуществляют RSA-шифрование, причем результатом RSA-шифрования при создании замаскированных данных обрабатывают выбранные исходные данные, произвольном выборе секретного RSA-ключа, соответствующего выбранным секретным множителям и произвольной допустимой открытой RSA-экспоненте, и создании соответствующей ему цифровой RSA-подписи для замаскированных данных, создание демаскировочного ключа, соответствующего маскировочному ключу и использованному при создании цифровой RSA-подписи для замаскированных данных секретному RSA-ключу, демаскировки созданной цифровой RSA-подписи для замаскированных данных, которую производят введением ее, демаскировочного ключа и RSA-модуля в демаскирующий преобразователь, выходные данные которого принимают в качестве цифровой RSA-подписи для выбранных исходных данных, *отличающийся тем, что* при выборе допустимых открытых RSA-экспонент дополнительно произвольно выбирают, по меньшей мере, одну базовую открытую RSA-экспоненту, для каждой из которых выбирают произвольную ограничительную кратность, а в качестве допустимой открытой RSA-экспоненты принимают произвольную открытую RSA-экспоненту, составленную из выбранных базовых открытых RSA-экспонент, кратность каждой из которых берут в пределах выбранной ограничительной кратности, при создании замаскированных данных осуществляют RSA-шифрование выбранного маскировочного ключа, шифровальный RSA-ключ, которым осуществляют RSA-шифрование при создании замаскированных данных, выбирают соответствующим RSA-экспоненте, составленной из выбранных базовых открытых RSA-экспонент, каждую из которых берут в выбранной ограничительной кратности, произвольный выбор секретного RSA-ключа, соответствующего выбранным секретным множителям и произвольной допустимой открытой RSA-экспоненте, осуществляют произвольным выбором используемых кратностей базовых открытых RSA-экспонент в пределах выбранных ограничительных кратностей базовых открытых RSA-экспонент, а демаскировочный ключ создают посредством RSA-шифрования маскировочного ключа шифровальным RSA-ключом, в качестве модуля которого берут RSA-модуль, а RSA-экспонента которого соответствует базовым открытым RSA-экспонентам, каждую из которых берут в кратности, равной разности соответствующей ей ограничительной кратности, и выбранной при произвольном выборе секретного ключа, соответствующей ей используемой кратности.

23. Способ изготовления вслепую цифровой RSA-подписи по п. 22, *отличающийся тем, что* выбор рандомизированного маскировочного ключа производят посредством датчика случайных чисел.

24. Способ изготовления вслепую цифровой RSA-подписи по п. 22, *отличающийся тем, что* при создании замаскированных данных RSA-шифрование выбранного маскировочного ключа осуществляют последовательными RSA-шифрованиями шифровальными RSA-ключами, в качестве модуля каждого из которых берут RSA-

модуль, а в качестве RSA-экспонент которых берут базовые открытые RSA-экспоненты, причем каждую из них берут в выбранной ограничительной кратности.

25. Способ изготовления вслепую цифровой RSA-подписи по п. 22, *отличающийся тем, что* создание демаскировочного ключа посредством RSA-шифрования маскировочного ключа шифровальным RSA-ключом осуществляют последовательными RSA-шифрованиями шифровальными RSA-ключами, в качестве модуля каждого из которых берут RSA-модуль, а в качестве RSA-экспонент которых берут базовые открытые RSA-экспоненты, причем каждую из них берут в кратности равной разности соответствующей ей ограничительной кратности, и выбранной при произвольном выборе секретного ключа, соответствующей ей используемой кратности.

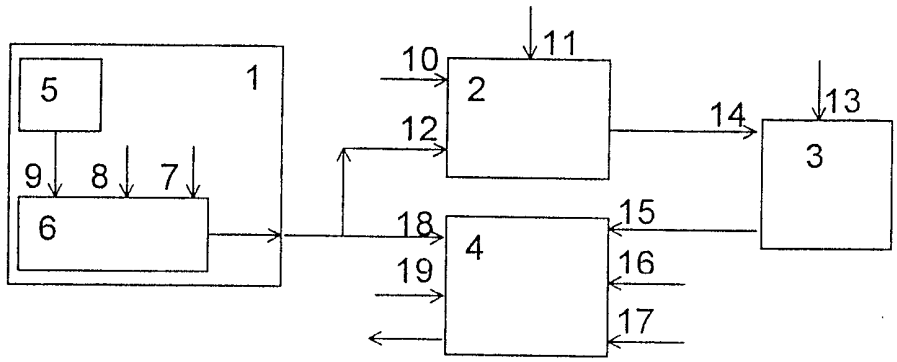
26. Способ изготовления вслепую цифровой RSA-подписи по п.22, *отличающийся тем, что* RSA-шифрование при создании замаскированных данных и при создании демаскировочного ключа осуществляют посредством модулярного экспоненциатора.

27. Способ изготовления вслепую цифровой RSA-подписи по п.22, *отличающийся тем, что* цифровую RSA-подпись для замаскированных данных создают посредством модулярного экспоненциатора.

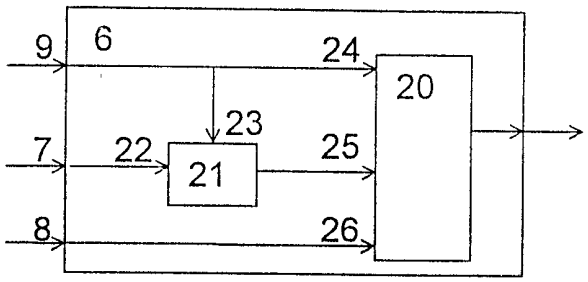
28. Устройство для изготовления вслепую цифровой RSA-подписи, содержащее блок выбора маскировочного ключа с датчиком случайных чисел, блок маскировки с модулярным экспоненциатором, модульный вход которого соединен с модульным входом блока маскировки, а экспонентный вход которого соединен со входом маскировочного ключа блока маскировки, блок маскировки имеет вход исходных данных и один выход, который соединен со входом данных подписи блока подписи, который имеет вход секретного ключа и один выход, который соединен с входом данных демаскировки блока демаскировки, который имеет выход подписи, модульный вход, экспонентный вход и вход маскировочного ключа, вход секретного ключа блока подписи, *отличающееся тем, что* базовый вход модулярного экспоненциатора блока маскировки соединен с входом исходных данных блока маскировки, а его выход соединен с выходом блока маскировки, блок демаскировки дополнительно имеет вход исходных данных и содержит модулярный мультипликативный евклидов преобразователь (ММЕП) с модульным входом, базовыми входами и соответствующими каждому из них экспонентными входами, причем модульный вход блока демаскировки соединен с модульным входом ММЕП, вход исходных данных блока демаскировки соединен с одним из базовых входов ММЕП, а вход данных демаскировки блока демаскировки соединен с другим базовым входом ММЕП, вход маскировочного ключа блока демаскировки соединен с экспонентным входом ММЕП, который соответствует базовому входу ММЕП, соединенному с входом данных демаскировки блока демаскировки, а экспонентный вход блока демаскировки соединен с экспонентным входом ММЕП, который соответствует базовому входу ММЕП, соединенному с входом исходных данных блока демаскировки, а выход блока демаскировки соединен с выходом ММЕП, блок выбора маскировочного ключа дополнительно содержит арифметический контроллер с двумя ограничительными входами, которые условно приняты за первый и второй ограничительные входы, причем арифметический контроллер соединен с датчиком случайных чисел, выход арифметического контроллера соединен с выходом блока выбора маскировочного ключа, а арифметический контроллер выполнен таким, что обеспечивает взаимную простоту выходных данных блока выбора маскировочного ключа относительно целых чисел, поданных на первый ограничительный вход арифметического контроллера, и делимость выходных данных блока выбора маскировочного ключа на целое число, поданное на второй его ограничительный вход.

29. Устройство для изготовления вслепую цифровой RSA-подписи по п.28, *отличающееся тем, что* соединение арифметического контроллера с датчиком случайных чисел выполнено путем соединения выхода датчика случайных чисел со входом, условно принятым за вход пробных данных арифметического контроллера, а взаимная простота выходных данных блока выбора маскировочного ключа относительно целых чисел, поданных на первый ограничительный вход арифметического контроллера, и делимость выходных данных блока выбора маскировочного ключа на целое число, поданное на второй его ограничительный вход, обеспечена тем, что арифметический контроллер содержит умножитель и тестер взаимной простоты, причем первый ограничительный вход арифметического контроллера соединен со входом тестера взаимной простоты, вход пробных данных соединен с другим входом

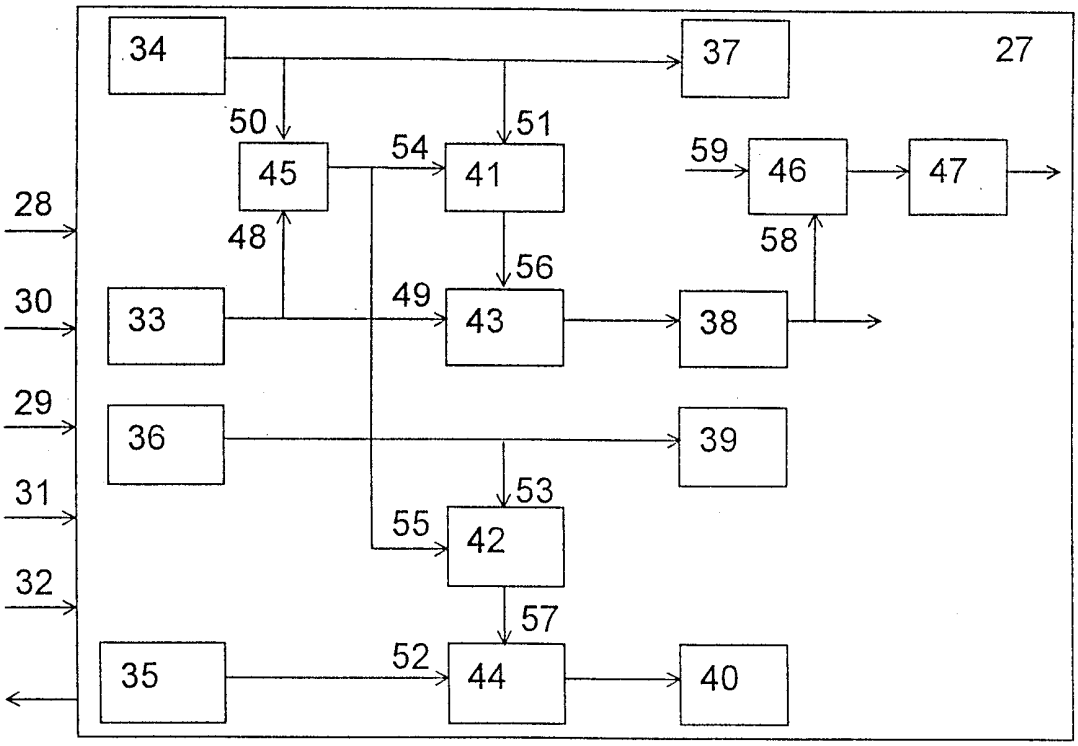
тестера взаимной простоты и с аргументным входом умножителя, выход тестера взаимной простоты соединен со входом загрузки умножителя, второй ограничительный вход арифметического контроллера соединен с аргументным входом умножителя, выход которого соединен с выходом арифметического контроллера.



Фиг. 1



Фиг. 2



Фиг. 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/RU 99/00197

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 318 097 A (CHAUM DAVID) 31 May 1989 (1989-05-31) abstract column 4, line 11 -column 5, line 24 claim 1 figure 6 ---	1-3,6, 12,13, 15,16, 19,22,28
A	US 4 759 064 A (CHAUM DAVID L) 19 July 1988 (1988-07-19) cited by the applicant abstract column 2, line 20 -column 3, line 25 column 8, line 42 - line 64 claim 1 figures 1,3 --- -/--	1-29

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 November 1999	01/12/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/RU 99/00197

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 4 996 711 A (CHAUM DAVID L) 26 February 1991 (1991-02-26) abstract column 1, line 45 -column 2, line 17 column 3, line 12 -column 4, line 44 claim 1 -----	1,3,6, 13,15, 16,19, 22,28

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/RU 99/00197

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0318097 A	31-05-1989	US 4947430 A	07-08-1990
		AT 164278 T	15-04-1998
		DE 3856149 D	23-04-1998
		DE 3856149 T	02-07-1998
US 4759064 A	19-07-1988	AT 75893 T	15-05-1992
		DE 3685186 A	11-06-1992
		EP 0218305 A	15-04-1987
		GR 3005322 T	24-05-1993
US 4996711 A	26-02-1991	NONE	

ОТЧЁТ О МЕЖДУНАРОДНОМ ПОИСКЕ

Международная заявка № PCT/RU 99/00197

A. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:
H04L 9/32
Согласно международной патентной классификации (МПК-7)

B. ОБЛАСТИ ПОИСКА:

Проверенный минимум документации (система классификации и индексы) МПК-7:
H04L

Другая проверенная документация в той мере, в какой она включена в поисковые подборки:

Электронная база данных, использовавшаяся при поиске (название базы и, если, возможно, поисковые термины):

C. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ:

Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей	Относится к пункту №
A	EP 0 318 097 A (CHAUM DAVID) 31 мая 1989 (31.05.89) реферат столбец 4, стр. 11 – столбец 5, стр. 24, п. 1 формулы, фиг. 6	1-3, 6, 12, 13, 15, 16, 19, 22, 28
A	US 4 759 064 A (CHAUM DAVID L) 19 июля 1988 (19.07.88) так как указано заявителем реферат, столбец 2, стр. 20 – столбец 3, стр. 25, столбец 8, стр. 42 – стр. 64, п. 1 формулы, фиг. 1, 3	1-29
A	US 4 996 711 A (CHAUM DAVID L) 26 февраля 1991 (26.02.91) реферат, столбец 1, стр. 45 – столбец 2, стр. 17, столбец 3, стр. 12 – столбец 4. стр. 44, п. 1 формулы	1, 3, 6, 13, 15, 16, 19, 22, 28

☐ последующие документы указаны в продолжении графы C.

☒ данные о патентах-аналогах указаны в приложении.

* Особые категории ссылочных документов:

A документ, определяющий общий уровень техники

E более ранний документ, но опубликованный на дату международной подачи или после нее

O документ, относящийся к устному раскрытию, экспонированию и т.д.

P документ, опубликованный до даты международной подачи, но после даты испрашиваемого приоритета и т.д.

"P" документ, опубликованный до даты международной подачи, но после даты испрашиваемого приоритета.

T более поздний документ, опубликованный после даты приоритета и приведенный для понимания изобретения

X документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну и изобретательский уровень

Y документ, порочащий изобретательский уровень в сочетании с одним или несколькими документами той же категории

& документ, являющийся патентом-аналогом

"&" документ, являющийся патентом-аналогом

Дата действительного завершения международного поиска:	Дата отправки настоящего отчёта о международном поиске:
24 ноября 1999 (24.11.99)	1 декабря 1999 (01.12.99)
Наименование и адрес Международного поискового органа: Европейское Патентное Ведомство	Уполномоченное лицо: Телефон №

ОТЧЕТ О МЕЖДУНАРОДНОМ ПОИСКЕ

Информация о патентах-аналогах

Международная заявка № PCT/RU 99/00197

Патентный документ указанный в международном поиске	Дата публикации	Патенты-аналоги	Дата публикации
EP 0318097 A	31-05-1989	US 4947430 A	07-08-1990
		AT 164278 T	15-04-1998
		DE 3856149 D	23-04-1998
		DE 3856149 T	02-07-1998
US 4759064 A	19-07-1988	AT 75893 T	15-05-1992
		DE 3685186 A	11-06-1992
		EP 0218305 A	15-04-1987
		GR 3005322 T	24-05-1993
US 4996711 A	26-02-1991	**НЕТ**	