РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 276 465** (13) **C2**

(51) МПК
*H04L 9/22* (2006.01)
*G06F 7/72* (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

# (12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2002133218/09, 15.05.2001**

(24) Дата начала отсчета срока действия патента:
**15.05.2001**

(30) Конвенционный приоритет:
**17.05.2000 DE 10024325.8**

(43) Дата публикации заявки: **20.04.2004**

(45) Опубликовано: **10.05.2006 Бюл. № 13**

(56) Список документов, цитированных в отчете о поиске: **WO 98/52319 A1, 19.11.1998. RU 2110157 C1, 27.04.1998. GB 2318892 A1, 06.05.1998. EP 0682327 A2, 15.11.1995.**

(85) Дата перевода заявки PCT на национальную фазу: **17.12.2002**

(86) Заявка PCT:
**EP 01/05532 (15.05.2001)**

(87) Публикация PCT:
**WO 01/88693 (22.11.2001)**

Адрес для переписки:
**101000, Москва, М.Златоустинский пер., 10, кв.15, "ЕВРОМАРКПАТ", пат.пов. Р.А.Каксису, рег.№899**

(72) Автор(ы):
**ЗЕЙЗЕН Мартин (DE)**

(73) Патентообладатель(и):
**ГИЗЕКЕ УНД ДЕВРИЕНТ ГМБХ (DE)**

RU 2276465 C2

## (54) КРИПТОГРАФИЧЕСКИЙ СПОСОБ И ЧИП-КАРТА ДЛЯ ЕГО ОСУЩЕСТВЛЕНИЯ

(57) Реферат:

Изобретение относится к криптографическому способу и чип-карте для шифрования информации и к методам создания электронных подписей. Сущность изобретения заключается в том, что выполняют по меньшей мере один этап вычислений, обеспечивающий выполнение операции E модульного возведения в степень по формуле $E=x^q(\mathrm{mod}\ p{\cdot}q)$, где d и mod p·q являются компонентами секретного ключа, причем p представляет собой первый простой множитель, q представляет собой второй простой множитель, d представляет собой показатель степени, а x представляет собой основание, при этом операцию E модульного возведения в степень осуществляют в соответствии с китайской теоремой об остатках. Технический результат - сокращение количества вычислительных операций и затрат машинного времени при одновременном повышении степени защиты данных от несанкционированного доступа. 4 н. и 26 з.п. ф-лы.

RU 2276465 C2

RUSSIAN FEDERATION

(19) **RU** (11) **2 276 465** (13) **C2**

(51) Int. Cl.
*H04L 9/22* (2006.01)
*G06F 7/72* (2006.01)

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

# (12) ABSTRACT OF INVENTION

(21), (22) Application: **2002133218/09, 15.05.2001**

(24) Effective date for property rights: **15.05.2001**

(30) Priority:
**17.05.2000 DE 10024325.8**

(43) Application published: **20.04.2004**

(45) Date of publication: **10.05.2006 Bull. 13**

(85) Commencement of national phase: **17.12.2002**

(86) PCT application:
**EP 01/05532 (15.05.2001)**

(87) PCT publication:
**WO 01/88693 (22.11.2001)**

Mail address:
**101000, Moskva, M.Zlatoustinskij per., 10, kv.15, "EVROMARKPAT", pat.pov. R.A.Kaksisu, reg.№899**

(72) Inventor(s):
**ZEJZEN Martin (DE)**

(73) Proprietor(s):
**GIZEKE UND DEVRIENT GMBKh (DE)**

## (54) CRYPTOGRAPHIC METHOD AND CHIP-CARD FOR REALIZATION OF SAID METHOD (VARIANTS)

(57) Abstract:

FIELD: cryptographic method and chip-card for encoding information, methods for creating electronic signatures.

SUBSTANCE: at least one calculation step is performed, providing for realization of E operation of modular exponentiation in accordance to formula $E=x^d(\mathrm{mod}\ p\cdot q)$, where d and mod p·q are components of a secret key, while parallel represent first simple multiplier, q is second simple multiplier, d is level coefficient, and x represents base, while operation E of modular exponentiation is performed in accordance to Chinese theorem about remainders.

EFFECT: decreased amount of computing operations and machine time costs during simultaneous increase of level of data protection from unsanctioned access.

4 cl

RU 2276465 C2

RU 2276465 C2

Криптографические методы, к которым относятся методы шифрования информации и методы создания электронных подписей, находят все более широкое распространение, что обусловлено прежде всего возрастанием того значения, которое в деловой сфере приобретает электронное ведение бизнеса. Для практической реализации подобных методов обычно используются соответствующие электронные устройства, которые для этой цели могут быть оснащены, например, универсальным программируемым микроконтроллером или же специализированной электронной схемой, например, в виде специализированной интегральной схемы (ИС). Одним из представляющих особый интерес криптографических устройств является карта со встроенной микросхемой (так называемая чип-карта), поскольку на такой карте при ее соответствующем техническому назначению выполнении можно сохранить секретные параметры ключа доступа в защищенном от несанкционированного доступа к ним виде. При этом основные усилия при разработке криптографических методов направлены на повышение скорости их выполнения, а также на защиту обрабатываемой с их помощью информации от всех возможных типов получения к ней несанкционированного доступа ("взлома"). Предлагаемое в изобретении решение пригодно для его использования прежде всего применительно к чип-картам, чем, однако, не ограничиваются возможные области его применения. Более того, предлагаемое в настоящем изобретении решение может быть реализовано в криптографических устройствах всех типов.

При осуществлении целого ряда известных криптографических методов необходимо выполнять операцию модульного возведения в степень в соответствии со следующим уравнением:

$$E = x^d (\mathrm{mod}\ N) = x^d (\mathrm{mod}\ p \cdot d) \quad (1),$$

где p и q представляют собой простые числа. Наиболее значимым криптографическим методом, предусматривающим выполнение указанной операции модульного возведения в степень, является алгоритм цифровой подписи Райвеста-Шамира-Адлемана (RSA-алгоритм), известный, например, из публикации Alfred J. Menezes, Paul C. van Oorschot и Scott A. Vanstone, "Handbook of Applied Cryptography", изд-во CRC Press, Boca Raton, 1997, сс.285-291. Однако операция модульного возведения в степень используется не только в RSA-алгоритме, но и, например, в алгоритме цифровой подписи Рабина, известном из указанной выше публикации авторов Menezes и др., сс.438-442, и в алгоритме идентификации Фиата-Шамира, также известном из этой же публикации авторов Menezes и др., сс.408-410.

Надежность криптографических методов, предусматривающих выполнение операции по модульному возведению в степень, обычно зависит от сложности разложения числа N в уравнении (1) на его простые множители p и q. Решить эту задачу потенциальному злоумышленнику достаточно сложно лишь при достаточно больших значениях N, и поэтому такое число N, с одной стороны, следует выбирать предельно большим. С другой стороны, однако, с увеличением порядка числа N пропорционально возрастают и затраты машинного времени на вычисления соответствующих значений путем модульного возведения в степень согласно уравнению (1), и поэтому с точки зрения практического применения затраты машинного времени представляется целесообразным ограничить некоторым приемлемым уровнем, несмотря на оперирование с большими значениями самого числа N.

Известно, что применение так называемой "китайской теоремы об остатках" позволяет повысить скорость вычислений в 4 раза, благодаря чему, например, появляется возможность оперировать с большими значениями числа N при тех же затратах машинного времени. С этой целью вместо выполнения вычислений непосредственного в соответствии с уравнением (1) выполняется следующее преобразование:

$$E = x^d (\mathrm{mod} p \cdot q) = aE_1 + bE_2 (\mathrm{mod} N) \quad (2),$$

где

$$E_1 = x^d (\mathrm{mod}\ p) \quad (3),$$

$E_2 = x^d \pmod q$ (4).

Применение китайской теоремы об остатках позволяет оперировать при модульном возведении в степень уже не с величиной по модулю N, т.е. с вычисляемым по модулю значением того числа, в котором все еще сохраняются его собственные простые множители, разложению на которые оно подвергается, а последовательно сначала с величиной по модулю p, а затем с величиной по модулю q, т.е. при использовании подобного правила вычислений изначально необходимо знать сохраняемую в тайне методику разложения на простые множители n=p·q, что в результате приводит к разбиению всего процесса вычислений на первый этап вычислений согласно уравнению (3), на котором основной подвергаемой обработке величиной является первый простой множитель, и на второй этап вычислений согласно уравнению (4), на котором основной подвергаемой обработке величиной является второй простой множитель. Преимущество такого подхода состоит в том, что показатель степени d в уравнении (1) необходимо определять как величину, рассчитываемую по модулю $\phi(p \cdot q)$, тогда как показатели степени в уравнении (2) необходимо определять лишь как величины, рассчитываемые по модулю $\phi(p)$ и $\phi(q)$ соответственно, где через $\phi$ обозначена функция Эйлера.

Следует отметить тот представляющий интерес факт, что в последнее время получил известность алгоритм "взлома" тех криптографических методов, в которых используется описанное выше модульное возведение в степень, при этом такой алгоритм основан на том, что в результате соответствующего искусственного вмешательства в протекающий в остальном без сбоев процесс вычислений на основании искаженного результата, полученного при неверном выполнении операции по модульному возведению в степень, можно получить информацию о простых множителях, разложению на которые подвергается число N, при условии, что при этом используется конкретная реализация китайской теоремы об остатках согласно уравнениям (2)-(4). Подобный метод получения несанкционированного доступа к информации, известный как "метод "взлома", выявленный специалистами фирмы Bellcore", рассмотрен, например, в публикации Dan Boneh, Richard A. DeMillo и Richard J. Lipton, "On the importance of checking Cryptographic Protocols for Faults", Advances in Cryptology - EUROCRYPT, 97, Lecture Notes in Computer Science 1233, изд-во Springer, Berlin, 1997. Согласно приведенной в указанной публикации информации получить доступ к данным можно путем преднамеренного создания неисправностей в шифраторе, подвергая его различного рода физическим воздействиям, таким, например, как завышение тактовой частоты, подача слишком высокого напряжения питания или радиационное облучение, что с определенной, хотя и не слишком высокой вероятностью приводит к возникновению ошибок в вычислениях при выполнении операции по модульному возведению в степень в соответствии с китайской теоремой об остатках. Если подобная ошибка в вычислениях возникает при оперировании только с одним из двух членов в уравнении (2), то на основании ошибочного результата возведения в степень можно восстановить оба простых множителя p и q.

Вывод, который можно сделать исходя из подобной уязвимости алгоритмов, использующих реализованное на основе китайской теоремы об остатках модульное возведение в степень, состоит в том, что полученный в процессе вычислений результат перед его дальнейшей обработкой и прежде всего перед его выдачей в какой-либо форме, например в виде подписи, сначала необходимо проверять на корректность.

Тривиальная мера, позволяющая воспрепятствовать "взлому" данных по выявленной специалистами Bellcore методике, состоит в том, чтобы в целях указанной проверки корректности результатов вычислений по меньшей мере однократно повторять каждый процесс вычислений. При возникновении в процессе вычислений случайных ошибок можно исходить из того, что полученный при выполнении первого процесса вычислений результат отличается от результата, полученного при выполнении контрольных вычислений. Существенный недостаток такого подхода заключается в том, что уже при выполнении одного контрольного процесса вычислений затраты машинного времени удваиваются.

Из заявки WO 98/52319 A1 известен, в частности, способ защиты вычислительных операций по модульному возведению в степень в соответствии с китайской теоремой об остатках от "взлома" по выявленной специалистами Bellcore методике. Этот способ состоит в том, что сначала выбирается некоторое секретное число j, например в интервале $[0, 2^k-1]$, где $16 \le k \le 32$. После этого выполняются вычисления в соответствии со следующими выражениями:

$$v_1 = x(\mathrm{mod}\ j \cdot q) \quad (5),$$

$$v_2 = x(\mathrm{mod}\ j \cdot q) \quad (6),$$

$$d_1 = d(\mathrm{mod}\ \phi(j \cdot p)) \quad (7),$$

$$d_2 = d(\mathrm{mod}\ \phi(j \cdot p)) \quad (8),$$

$$w_1 = v_1^{d1}(\mathrm{mod}\ j \cdot p) \quad (9),$$

$$w_2 = v_2^{d2}(\mathrm{mod} j \cdot p) \quad (10).$$

Затем проверяется выполнение следующего условия:

$$w_1 = w_2(\mathrm{mod}\ j) \quad (11).$$

Если соблюдение этого условия (11) подтверждается, то согласно известному способу выполняются вычисления в соответствии со следующими выражениями:

$$y_1 = w_1(\mathrm{mod}\ p) \quad (12),$$

$$y_2 = w_2(\mathrm{mod}\ q) \quad (13),$$

на основании которых затем с помощью китайской теоремы об остатках можно определить значение

$$E = x^d(\mathrm{mod}\ N) \quad (14).$$

Преимущество этого известного способа перед простым выполнением контрольных вычислений состоит в значительном сокращении дополнительных затрат машинного времени.

В соответствии с таким известным способом оба простых числа p и q необходимо умножать на один и тот же множитель d. В заявке WO 98/52319 A1 описан также второй вариант осуществления заявленного в ней способа, позволяющий умножать простые числа p и q на разные множители r и s. При этом, однако, для выполнения контрольных вычислений может потребоваться выполнение двух дополнительных операций возведения в степень.

В основу настоящего изобретения была положена задача разработать криптографический способ, соответственно криптографическое устройство, такое как чип-карта, которые позволяли бы сократить количество вычислительных операций или затраты машинного времени при одновременном сохранении или повышении степени защиты данных от несанкционированного доступа.

Эта задача решается в предлагаемых в изобретении криптографическом способе и чип-карте для его осуществления.

Предлагаемый в изобретении криптографический способ осуществим в чип-карте и заключается в том, что выполняют по меньшей мере один этап вычислений, включающий операцию E модульного возведения в степень по формуле

$E=x^d(\mathrm{mod}\ p \cdot q)$,

где d и mod p·q являются компонентами секретного ключа, причем p представляет собой первый простой множитель, q представляет собой второй простой множитель, d представляет собой показатель степени, а x представляет собой основание.

В первом варианте предлагаемого способа для выполнения операции модульного возведения в степень выбирают два натуральных числа r и s, при условии, что величины d и $\phi$(kgV(r, s)) являются взаимно простыми, и выполняют следующие этапы вычислений:

$x_1=x(\mathrm{mod}\ p \cdot r)$,

$x_2=x(\mathrm{mod}\ q \cdot s)$,

$d\_1=d(\mathrm{mod}\ \phi(p \cdot r))$,

$d\_2=d(\mathrm{mod}\ \phi(q \cdot s))$,

$z_1 = x_1^{d-1} (\mathrm{mod}\ p \cdot r)$,

$z_2 = x_2^{d-2} (\mathrm{mod}\ p \cdot s)$,

где $\phi()$ представляет собой функцию Эйлера, а kgV(r, s) является наименьшим общим кратным для чисел r и s.

Затем в соответствии с китайской теоремой об остатках на основании величин $z_1$ и $z_2$ вычисляют число z по формулам $z=z_1(\mathrm{mod}\ p{\cdot}r)$ и $z=z_2(\mathrm{mod}\ q{\cdot}s)$.

Далее вычисляют результат операции E возведения в степень путем сокращения z по модулю p·q и ранее вычисленное число z и тем самым результат операции E возведения в степень проверяют на этапе контроля на наличие вычислительных ошибок. При этом этап контроля заключается в выполнении следующих вычислительных операций:

- вычисление наименьшего возможного натурального числа e, удовлетворяющего условию $e{\cdot}d=1(\mathrm{mod}\ \phi(\mathrm{kgV}(r, s)))$, с помощью расширенного алгоритма Евклида,

- вычисление значения $C=z^e(\mathrm{mod}\ \mathrm{kgV}(r, s))$,

- сравнение между собой значений x и C по модулю kgV(r, s).

Результат операции E модульного возведения в степень отбрасывается как ошибочный, если $x \neq C(\mathrm{mod}\ \mathrm{kgV}(r, s))$.

Во втором варианте предлагаемого способа для выполнения операции модульного возведения в степень выбирают два натуральных числа r и s, а также два числа $b_1$ и $b_2$ из интервала [1, ..., r-1], соответственно [1, ..., s-1], являющиеся взаимно простыми по отношению к числам r и s соответственно, причем эти числа $b_1$ и $b_2$ удовлетворяют условию $b_1=b_2(\mathrm{mod}\ \mathrm{ggT}(r, s))$, где ggT(r, s) представляет собой наибольший общий делитель для чисел r и s.

С помощью обоих чисел $b_1$ и $b_2$ в соответствии с китайской теоремой об остатках вычисляют числа $x_1$ и $x_2$, которые удовлетворяют следующим условиям:

$x_1=x(\mathrm{mod}\ p)$, $x_1=b_1(\mathrm{mod}\ r)$,

$x_2=x(\mathrm{mod}\ q)$, $x_2=b_2(\mathrm{mod}\ s)$,

после чего выполняют следующие этапы вычислений:

$d\_1=d(\mathrm{mod}\ \phi(p))$,

$d\_2=d(\mathrm{mod}\ \phi(q))$,

$z_1 = x_1^{d-1} (\mathrm{mod}\ p \cdot r)$,

$z_2 = x_2^{d-2} (\mathrm{mod}\ p \cdot s)$,

где $\phi()$ представляет собой функцию Эйлера, а kgV(r, s) представляет собой наименьшее общее кратное для чисел r и s.

Далее в соответствии с китайской теоремой об остатках на основании величин $z_1$ и $z_2$ вычисляют число z по формулам $z=z_1(\mathrm{mod}\ p{\cdot}r)$ и $z=z_2(\mathrm{mod}\ q{\cdot}s)$, вычисляют результат операции E возведения в степень путем сокращения z по модулю p·q и ранее вычисленное число z (а тем самым автоматически и результат операции E возведения в степень) проверяют на этапе контроля на наличие вычислительных ошибок.

Этот этап контроля заключается в выполнении следующих вычислительных операций:

- вычисление чисел

$C_1 = b_1^{d-1} (\mathrm{mod}\ r)$,

$C_2 = b_2^{d-2} (\mathrm{mod}\ s)$,

причем до выполнения операции модульного возведения в степень по модулю $\phi(r)$, соответственно $\phi(s)$, сокращают d_1 и d_2,

- сравнение между собой значений $z_1$ и $C_1$ по модулю r, а также $z_2$ и $C_2$ по модулю s.

Результат операции E модульного возведения в степень отбрасывается как ошибочный, если $C_1 \neq z_1 \bmod r$ или $C_2 \neq r_2 \bmod s$.

Как было указано выше, объектом изобретения является также чип-карта, имеющая по меньшей мере одно вычислительное устройство и выполненная в двух вариантах с обеспечением осуществления соответствующих вариантов предлагаемого криптографического способа.

Как более подробно описано ниже, при использовании определенных вычислительных устройств предпочтительным является наличие у модуля при модульном возведении в степень большого количества ведущих двоичных единиц, и поэтому использование различных множителей r и s в этом случае связано с определенными преимуществами. Помимо этого существуют оптимизированные для выполнения операций модульного возведения в степень вычислительные устройства, при этом, однако, одна лишь необходимая для выполнения операций по возведению в степень передача данных из центрального процессора в такое оптимизированное вычислительное устройство связана со значительными затратами на управление массивами данных. Предлагаемое в изобретении решение позволяет по сравнению с описанным выше известным способом сократить на одну количество операций по возведению в степень при использовании различных множителей r и s.

Согласно изобретению предлагается выбирать два целых числа r и s, например, в интервале [0, $2^k$-1], где $16 \le k \le 32$, благодаря чему величины d и $\phi$(kgV(r, s)) являются взаимно простыми, при этом kgV(r, s) представляет собой наименьшее общее кратное для чисел r и s, а $\phi$() представляет собой функцию Эйлера. Затем выполняются вычисления в соответствии со следующими выражениями:

$$x_1 = x(\mathrm{mod}\ p \cdot r) \quad (15),$$

$$x_2 = x(\mathrm{mod}\ p \cdot s) \quad (16),$$

$$d\_1 = d(\mathrm{mod}\ \phi(p \cdot r)) \quad (15),$$

$$d\_2 = d(\mathrm{mod}\ \phi(q \cdot s)) \quad (16),$$

$$z_1 = x_1^{d-1}(\mathrm{mod}\ p \cdot r) \quad (15),$$

$$z_2 = x_2^{d-2}(\mathrm{mod}\ q \cdot s) \quad (16).$$

В этом случае справедливы следующие выражения: $z_1=x^d(\mathrm{mod}\ p{\cdot}r)$ и $z_2=x^d(\mathrm{mod}\ q{\cdot}s)$. На основании известных величин $z_1$ и $z_2$ в соответствии с китайской теоремой об остатках можно легко вычислить число z согласно следующим выражениям:

$$z = z_1(\mathrm{mod} p \cdot r);\ z = z_2(\mathrm{mod} q \cdot s);\ z = x^d(\mathrm{mod} p \cdot q \cdot kgV(r,s)) \quad (17).$$

Числа r и s следует выбирать согласно изобретению таким образом, чтобы величины d и $\phi$(kgV(r, s)) были взаимно простыми. При наличии таких условий можно с помощью расширенного алгоритма Евклида легко найти натуральное число e в соответствии со следующим выражением:

$$e \cdot d = 1(\mathrm{mod}\ \phi(kgV(r,s))) \quad (18).$$

Далее с помощью чисел z и e можно следующим образом вычислить число C:

$$C = z^e(\mathrm{mod}\ kgV(r,s)) \quad (19).$$

В соответствии с теоремой Эйлера справедливо следующее выражение:

$$C = x^{d \cdot e} = x(\mathrm{mod}\ kgV(r,s)) \quad (20).$$

Сравнение между собой обоих значений C и x по модулю kgV(r, s) позволяет с высокой степенью вероятности выявить наличие ошибки в вычислениях. Если $C \ne x(\mathrm{mod}\ kgV(r, s))$, то результат модульного возведения в степень следует рассматривать как ошибочный и отбросить.

В соответствии с RSA-алгоритмом (равно как и в соответствии с алгоритмом цифровой подписи Рабина) для формирования цифровой подписи или для дешифрации следует выполнить одну операция модульного возведения в степень, при этом модуль p·q и показатель степени d зависят только от секретного ключа. По этой причине числа d, e, r и s можно вычислять лишь однократно при вводе этого секретного ключа и затем сохранять для последующего использования.

В соответствии с одним из вариантов осуществления изобретения также предлагается выбирать два целых числа r и s, например, в интервале [0, $2^k$-1], где $16 \le k \le 32$. При использовании двоичного вычислительного (арифметического) устройства в качестве чисел r и s рекомендуется выбирать нечетные числа. Кроме того, выбирают два постоянных, не зависящих от x числа $b_1$ и $b_2$ из интервала [1, ..., r-1], соответственно [1, ..., s-1],

являющихся взаимно простыми с числом r, соответственно s. Если числа r и s не являются взаимно простыми, то числа $b_1$ и $b_2$ должны удовлетворять дополнительному условию $b_1=b_2(\mathrm{mod}\ ggT(r, s))$, где ggT(r, s) представляет собой наибольший общий делитель для чисел r и s.

Далее сначала в соответствии с китайской теоремой об остатках вычисляется число $x_1$ согласно следующему выражению:

$$x_1 = x(\mathrm{mod}\ p),\ x_1 = b_1(\mathrm{mod}\ r) \quad (21).$$

Затем аналогичным образом вычисляется число $x_2$:

$$x_1 = x(\mathrm{mod}\ q),\ x_2 = b_2(\mathrm{mod}\ s) \quad (22).$$

После этого выполняются вычисления в соответствии со следующими выражениями:

$$d\_1 = d(\mathrm{mod}\ \phi(p)) \quad (23),$$

$$d\_2 = d(\mathrm{mod}\ \phi(q)) \quad (24),$$

$$z_1 = x_1^{d-1}(\mathrm{mod}\ p \cdot r) \quad (25),$$

$$z_2 = x_2^{d-2}(\mathrm{mod}\ q \cdot s) \quad (26),$$

$$C_1 = b_1^{d-1}(\mathrm{mod}\ r) \quad (27),$$

$$C_2 = b_2^{d-2}(\mathrm{mod}\ s) \quad (28).$$

Для сокращения машинного времени можно сократить показатели степени d_1 и d_2 в уравнениях (27), соответственно (28) еще до возведения в степень по модулю $\phi(r)$, соответственно $\phi(s)$. Тем самым выражения (23) и (25) сводятся к следующему виду:

$$z_1 = x^d(\mathrm{mod}\ p) \quad (29).$$

Выражения (24) и (26) в свою очередь сводятся к следующему виду:

$$z_2 = x^d(\mathrm{mod}\ q) \quad (30).$$

На основании чисел $z_1$ и $z_2$ в соответствии с китайской теоремой об остатках можно легко вычислить число z:

$$z = z_1(\mathrm{mod}\ p \cdot r);\ z = z_2(\mathrm{mod}\ q \cdot s) \quad (31)$$

Даже если числа r и s не являются взаимно простыми, то такое число z существует в любом случае, поскольку $z_1 = C_1 = b_1^{d-1} = b_2^{d-2} = C_2 = z_2(\mathrm{mod}\ ggT(r, s))$.

Поскольку числа p и q являются взаимно простыми, из выражений (29), (30) и (31) следует, что:

$$z = x^d(\mathrm{mod}\ p \cdot q) \quad (32),$$

и поэтому искомое число z легко определить на основании двух вычисленных выше значений.

Из выражений (21), (25) и (27) следует, что

$$z_1 = C_1(\mathrm{mod}\ r) \quad (33).$$

Из выражений (22), (26) и (28) следует, что

$$z_2 = C_2(\mathrm{mod}\ s) \quad (34).$$

Проверка соблюдения условий (33) и (34) позволяет с высокой степенью вероятности выявить ошибку. Если при такой проверке будет установлено несоблюдение одного из условий (33) и (34), то результат модульного возведения в степень следует рассматривать как ошибочный и отбросить.

В отличие от способа, представленного в п.8 в заявке WO 98/52319 A1, в рассмотренном выше варианте осуществления предлагаемого в изобретении способа числа $b_1$ и $b_2$ не зависят от основания x. Обычно при использовании RSA-алгоритма или алгоритма цифровой подписи Рабина секретный ключ однократно вводится в криптографическое устройство, например в чип-карту, и затем многократно используется. При этом при выполнении используемой в этих алгоритмах операции модульного возведения в степень показатель степени d, равно как и модуль p·q, являются неизменными и постоянными компонентами секретного ключа. По этой причине значения $C_1$ и $C_2$ требуется вычислять лишь однократно при вводе ключа в криптографическое устройство и затем их можно сохранить в памяти этого устройства. По сравнению с известным из заявки WO 98/52319 A1 способом сохранение этих значений

позволяет на две сократить количество операций по модульному возведению в степень.

В состав обычного криптографического устройства, например чип-карты, оснащенного дополнительными аппаратными средствами для ускорения выполнения арифметических модульных операций, входят быстродействующие сумматоры и/или умножители, тогда как для выполнения необходимой для модульного сокращения операции деления на многозначное число требуется применять стандартные методы, известные, например, из публикации Donald Knuth, "The Art of Computer Programming", т.2: Seminumerical Algorithms, 2-е изд., изд-во Addison-Wesley, 1981. Один из известных методов, позволяющих упростить подобную операцию деления, состоит в умножении модуля p на число r до выполнения операции по возведению в степень, и поэтому в двоичном представлении произведения p·r присутствует максимально возможное количество единиц (см., например, указанную выше публикацию авторов Menezes и др., сс.598-599). Деление на число, содержащее максимально возможное количество ведущих единиц, является значительно более простой операцией по сравнению с делением на некоторое отвлеченное число.

Множитель r выбирают согласно изобретению таким образом, чтобы величины d и $\phi(r)$ были взаимно простыми. Однако в рассмотренном выше варианте осуществления изобретения наличие подобной взаимной простоты не требуется. Для каждого модуля p существует зависящий от конкретной технической реализации операции деления оптимальный множитель $r_{опт}$. Если выбранное в качестве r значение несколько меньше оптимального, то количество содержащихся в произведении p·r ведущих единиц все еще остается достаточным для того, чтобы можно было упростить выполнение операции деления. При этом число d с высокой вероятностью является взаимно простым по отношению по меньшей мере к одному из значений $\phi(r_{опт}-i)$; i=1, ..., k, при этом k представляет собой малое число, зависящее от конкретной реализации.

В противном случае r заменяется на величину $2^i \cdot r$, где $2^i$ представляет собой зависящую от конкретной реализации приемлемую степень двойки.

Аналогичные подстановки соответственно возможны и применительно ко второму простому множителю q. Поскольку множители r (для p) и s (для q) можно выбирать независимо один от другого, соответствующим образом можно выбирать и значения для множителя s.

## Формула изобретения

1. Криптографический способ, осуществляемый в чип-карте и заключающийся в том, что

а) выполняют по меньшей мере один этап вычислений, включающий операцию E модульного возведения в степень по формуле

$E=x^d(\mathrm{mod}\ p\cdot q)$,

где d и mod p·q являются компонентами секретного ключа, причем p представляет собой первый простой множитель, q представляет собой второй простой множитель, d представляет собой показатель степени, а x представляет собой основание, при этом

б) для выполнения операции модульного возведения в степень выбирают два натуральных числа r и s при условии, что величины d и $\phi$(kgV(r, s)) являются взаимно простыми, и выполняют следующие этапы вычислений:

$x_1=x(\mathrm{mod}\ p\cdot r)$,

$x_2=x(\mathrm{mod}\ q\cdot s)$,

$d\_1=d(\mathrm{mod}\ \phi(p\cdot r))$,

$d\_2=d(\mathrm{mod}\ \phi)(q\cdot s))$,

$$z_1 = x_1^{d-1}(\mathrm{mod}\ p\cdot r),$$

$$z_2 = x_2^{d-2}(\mathrm{mod}\ q\cdot s),$$

где $\phi()$ представляет собой функцию Эйлера, а kgV(r, s) является наименьшим общим кратным для чисел r и s, после чего

в) в соответствии с китайской теоремой об остатках на основании величин $z_1$ и $z_2$ вычисляют число z по формулам

$z=z_1(\mathrm{mod}\ p\cdot r)$ и $z=z_2(\mathrm{mod}\ q\cdot s)$,

г) вычисляют результат операции E возведения в степень путем сокращения z по модулю $p\cdot q$,

д) ранее вычисленное число z и тем самым результат операции E возведения в степень проверяют на этапе контроля на наличие вычислительных ошибок, при этом

е) указанный этап контроля заключается в выполнении следующих вычислительных операций:

е1) вычисление наименьшего возможного натурального числа e, удовлетворяющего условию $e\cdot d=1(\mathrm{mod}\ \phi(kgV(r, s)))$, с помощью расширенного алгоритма Евклида,

е2) вычисление значения $C=z^e(\mathrm{mod}\ kgV(r, s))$,

е3) сравнение между собой значений x и C по модулю kgV(r, s), при этом результат операции E модульного возведения в степень отбрасывается как ошибочный, если $x\neq C(\mathrm{mod}\ kgV(r, s))$.

2. Криптографический способ, осуществляемый в чип-карте и заключающийся в том, что

а) выполняют по меньшей мере один этап вычислений, включающий операцию E модульного возведения в степень по формуле

$E=x^d(\mathrm{mod}\ p\cdot q)$,

где d и mod $p\cdot q$ являются компонентами секретного ключа, причем p представляет собой первый простой множитель, q представляет собой второй простой множитель, d представляет собой показатель степени, а x представляет собой основание, при этом

б) для выполнения операции модульного возведения в степень выбирают два натуральных числа r и s, а также два числа $b_1$ и $b_2$ из интервала [1, ..., r-1], соответственно [1, ..., s-1], являющихся взаимно простыми по отношению к числам r и s соответственно, причем эти числа $b_1$ и $b_2$ удовлетворяют условию $b_1=b_2(\mathrm{mod}\ ggT(r, s))$, где ggT(r, s) представляет собой наибольший общий делитель для чисел r и s,

в) с помощью обоих этих чисел $b_1$ и $b_2$ в соответствии с китайской теоремой об остатках вычисляют числа $x_1$ и $x_2$, которые удовлетворяют следующим условиям:

$x_1=x(\mathrm{mod}\ p)$, $x_1=b_1(\mathrm{mod}\ r)$,

$x_2=x(\mathrm{mod}\ q)$, $x_2=b_2(\mathrm{mod}\ s)$,

после чего выполняют следующие этапы вычислений:

$d\_1=d(\mathrm{mod}\ \phi(p))$,

$d\_2=d(\mathrm{mod}\ \phi(q))$,

$$z_1 = x_1^{d\_1}(\mathrm{mod}\ p\cdot r),$$

$$z_2 = x_2^{d\_2}(\mathrm{mod}\ q\cdot s),$$

где $\phi()$ представляет собой функцию Эйлера, а kgV(r, s) представляет собой наименьшее общее кратное для чисел r и s, после чего

г) в соответствии с китайской теоремой об остатках на основании величин $z_1$ и $z_2$ вычисляют число z по формулам

$z=z_1(\mathrm{mod}\ p\cdot r)$ и $z=z_2(\mathrm{mod}\ q\cdot s)$,

д) вычисляют результат операции E возведения в степень путем сокращения z по модулю $p\cdot q$,

е) ранее вычисленное число z (а тем самым автоматически и результат операции E возведения в степень) проверяют на этапе контроля на наличие вычислительных ошибок, при этом

ж) указанный этап контроля заключается в выполнении следующих вычислительных операций:

ж1) вычисление чисел

$$C_1 = b_1^{d\_1}(\mathrm{mod}\ r),$$

$$C_2 = b_2^{d\_2}(\mathrm{mod}\ s),$$

причем до выполнения операции модульного возведения в степень по модулю $\phi(r)$, соответственно $\phi(s)$ сокращают d_1 и d_2,

ж2) сравнение между собой значений $z_1$ и $C_1$ по модулю r, а также $z_2$ и $C_2$ по модулю s, при этом результат операции E модульного возведения в степень отбрасывается как ошибочный, если $C_1 \neq z_1 \bmod r$ или $C_2 \neq z_2 \bmod s$.

3. Способ по п.2, отличающийся тем, что числа r и s являются нечетными.

4. Способ по любому из пп.1-3, отличающийся тем, что числа r и s выбирают из интервала $[0, 2^k-1]$, где $16 \leq k \leq 32$.

5. Способ по любому из пп.1-3, отличающийся тем, что по меньшей мере одно из чисел r и s выбирают таким образом, чтобы в двоичном представлении произведения p·r, соответственно q·s присутствовало максимально большое количество ведущих единиц.

6. Способ по п.5, отличающийся тем, что

а) сначала на первом подэтапе по меньшей мере для одного из чисел r и s выбирают соответствующее оптимальное число $r_{опт}$, соответственно $s_{опт}$, не ограничивая такой выбор условием, согласно которому величины d и $\phi(kgV(r, s))$ должны быть взаимно простыми, и

б) на втором подэтапе выбирают по соседнему значению $r=r_{опт}-i$, соответственно $s=s_{опт}-i$, где i=0, 1, ..., k, таким образом, чтобы величины d и $\phi(kgV(r, s))$ были взаимно простыми.

7. Способ по п.5, отличающийся тем, что

а) на первом подэтапе для каждого из чисел r и s выбирают соответствующее оптимальное число $r_{опт}$, соответственно $s_{опт}$, не ограничивая такой выбор условием, согласно которому величины d и $\phi(kgV(r, s))$ должны быть взаимно простыми, и

б) на втором подэтапе выбирают по значению $r=2^1 \cdot r_{опт}$, соответственно $s=2^1 \cdot s_{опт}$, где 1= 0, 1, ..., j, таким образом, чтобы величины d и $\phi(kgV(r, s))$ были взаимно простыми.

8. Способ по п.5, отличающийся тем, что

а) сначала на первом подэтапе выбирают по меньшей мере одно из чисел $r_{опт}$ и $s_{опт}$, не ограничивая такой выбор условием, согласно которому величины d и $\phi(kgV(r, s))$ должны быть взаимно простыми,

б) на втором подэтапе выбирают по соседнему значению $r=r_{опт}-i$, соответственно $s=s_{опт}-i$, где i=0, 1, ..., k, таким образом, чтобы величины d и $\phi(kgV(r, s))$ были взаимно простыми, при условии, что такое значение существует для i=0, 1, ..., k, и

в) на третьем подэтапе в том случае, если на втором подэтапе не было выбрано ни одного значения, выбирают по значению $r=2^1 \cdot r_{опт}$, соответственно $s=2^1 \cdot s_{опт}$, где 1=0, 1, ..., j, таким образом, чтобы величины d и $\phi(kgV(r, s))$ были взаимно простыми.

9. Способ по любому из пп.1-3, отличающийся тем, что оба числа r и s выбирают таким образом, чтобы в двоичном представлении произведения p·r и произведения q·s присутствовало максимально большое количество ведущих единиц.

10. Способ по п.9, отличающийся тем, что

а) сначала на первом подэтапе по меньшей мере для одного из чисел r и s выбирают соответствующее оптимальное число $r_{опт}$, соответственно $s_{опт}$, не ограничивая такой выбор условием, согласно которому величины d и $\phi(kgV(r, s))$ должны быть взаимно простыми, и

б) на втором подэтапе выбирают по соседнему значению $r=r_{опт}-i$, соответственно $s=s_{опт}-i$, где i=0, 1, ..., k, таким образом, чтобы величины d и $\phi(kgV(r, s))$ были взаимно простыми.

11. Способ по п.9, отличающийся тем, что а) на первом подэтапе для каждого из чисел r и s выбирают соответствующее оптимальное число $r_{опт}$, соответственно $s_{опт}$, не ограничивая такой выбор условием, согласно которому величины d и $\phi(kgV(r, s))$ должны быть взаимно простыми, и

б) на втором подэтапе выбирают по значению $r=2^1 \cdot r_{опт}$, соответственно $s=2^1 \cdot s_{опт}$, где 1=

0, 1, ..., j, таким образом, чтобы величины d и $\phi$(kgV(r, s)) были взаимно простыми.

12. Способ по п.9, отличающийся тем, что

а) сначала на первом подэтапе выбирают по меньшей мере одно из чисел $r_{опт}$ и $s_{опт}$, не ограничивая такой выбор условием, согласно которому величины d и $\phi$(kgV(r, s)) должны быть взаимно простыми,

б) на втором подэтапе выбирают по соседнему значению $r=r_{опт}-i$, соответственно $s=s_{опт}-i$, где i=0, 1, ..., k, таким образом, чтобы величины d и $\phi$(kgV(r, s)) были взаимно простыми, при условии, что такое значение существует для i=0, 1, ..., k, и

в) на третьем подэтапе в том случае, если на втором подэтапе не было выбрано ни одного значения, выбирают по значению $r=2^1 \cdot r_{опт}$, соответственно $s=2^1 \cdot s_{опт}$, где 1=0, 1, ..., j, таким образом, чтобы величины d и $\phi$(kgV(r, s)) были взаимно простыми.

13. Способ по любому из пп.1-3, отличающийся тем, что криптографический способ предусматривает выполнение алгоритма Райвеста-Шамира-Адлемана.

14. Способ по любому из пп.1-3, отличающийся тем, что криптографический способ предусматривает выполнение алгоритма цифровой подписи Рабина.

15. Способ по любому из пп.1-3, отличающийся тем, что криптографический способ предусматривает выполнение алгоритма идентификации Фиата-Шамира.

16. Чип-карта, имеющая по меньшей мере одно вычислительное устройство, обеспечивающее

а) выполнение этапа вычислений, включающего операцию E модульного возведения в степень по формуле

$E=x^d(\mathrm{mod}\ p \cdot q)$,

где d и mod p·q являются компонентами секретного ключа, причем p представляет собой первый простой множитель, q представляет собой второй простой множитель, d представляет собой показатель степени, а x представляет собой основание, при этом

б) для выполнения операции модульного возведения в степень выбираются два натуральных числа r и s при условии, что величины d и $\phi$(kgV(r, s)) являются взаимно простыми, и выполняются следующие этапы вычислений:

$x_1=x(\mathrm{mod}\ p \cdot r)$,

$x_2=x(\mathrm{mod}\ q \cdot s)$,

$d\_1=d(\mathrm{mod}\ \phi(p \cdot r))$,

$d\_2=d(\mathrm{mod}\ \phi(q \cdot s))$,

$$z_1 = x_1^{d-1}(\mathrm{mod}\ p \cdot r),$$

$$z_2 = x_2^{d-2}(\mathrm{mod}\ q \cdot s),$$

где $\phi$() представляет собой функцию Эйлера, а kgV(r, s) является наименьшим общим кратным для чисел r и s, после чего

в) в соответствии с китайской теоремой об остатках на основании величин $z_1$ и $z_2$ вычисляется число z по формулам

$z=z_1(\mathrm{mod}\ p \cdot r)$ и $z=z_2(\mathrm{mod}\ q \cdot s)$,

г) вычисляется результат операции E возведения в степень путем сокращения z по модулю p·q,

д) ранее вычисленное число z (а тем самым автоматически и результат операции E возведения в степень) проверяется на этапе контроля на наличие вычислительных ошибок, при этом

е) указанный этап контроля заключается в выполнении следующих вычислительных операций:

е1) вычисление наименьшего возможного натурального числа e, удовлетворяющего условию $e \cdot d=1(\mathrm{mod}\ \phi(kgV(r, s)))$, с помощью расширенного алгоритма Евклида,

е2) вычисление значения $C=z^e(\mathrm{mod}\ kgV(r, s))$,

е3) сравнение между собой значений x и C по модулю kgV(r, s), при этом результат операции E модульного возведения в степень отбрасывается как ошибочный,

если $x \neq C(\text{mod } kgV(r, s))$.

17. Чип-карта, имеющая по меньшей мере одно вычислительное устройство, обеспечивающее

а) выполнение этапа вычислений, включающего операцию E модульного возведения в степень по формуле

$E=x^d(\text{mod } p \cdot q)$,

где d и mod p·q являются компонентами секретного ключа, причем p представляет собой первый простой множитель, q представляет собой второй простой множитель, d представляет собой показатель степени, а x представляет собой основание, при этом

б) для выполнения операции модульного возведения в степень выбираются два натуральных числа r и s, а также два числа $b_1$ и $b_2$ из интервала [1, ..., r-1], соответственно [1, ..., s-1], являющихся взаимно простыми по отношению к числам r и s соответственно, причем эти числа $b_1$ и $b_2$ удовлетворяют условию $b_1=b_2(\text{mod } ggT(r, s))$, где ggT(r, s) представляет собой наибольший общий делитель для чисел r и s,

в) с помощью обоих этих чисел $b_1$ и $b_2$ в соответствии с китайской теоремой об остатках вычисляются числа $x_1$ и $x_2$, которые удовлетворяют следующим условиям:

$x_1=x(\text{mod } p)$, $x_1=b_1(\text{mod } r)$,

$x_2=x(\text{mod } q)$, $x_2=b_2(\text{mod } s)$,

после чего выполняются следующие этапы вычислений:

d_1=d(mod $\phi$(p)),

d_2=d(mod $\phi$(q)),

$$z_1 = x_1^{d-1}(\text{mod } p \cdot r),$$

$$z_2 = x_2^{d-2}(\text{mod } q \cdot s),$$

где $\phi$() представляет собой функцию Эйлера, а kgV(r, s) представляет собой наименьшее общее кратное для чисел r и s, после чего

г) в соответствии с китайской теоремой об остатках на основании величин $z_1$ и $z_2$ вычисляется число z по формулам

$z=z_1(\text{mod } p \cdot r)$ и $z=z_2(\text{mod } q \cdot s)$,

д) вычисляется результат операции E возведения в степень путем сокращения z по модулю p·q,

е) ранее вычисленное число z (а тем самым автоматически и результат операции E возведения в степень) проверяются на этапе контроля на наличие вычислительных ошибок, при этом

ж) указанный этап контроля заключается в выполнении следующих вычислительных операций:

ж1) вычисление чисел

$$C_1 = b_1^{d-1}(\text{mod } r),$$

$$C_2 = b_2^{d-2}(\text{mod } s),$$

причем до выполнения операции модульного возведения в степень по модулю $\phi$(r), соответственно $\phi$(s) сокращаются d_1 и d_2,

ж2) сравнение между собой значений $z_1$ и $C_1$ по модулю r, а также $z_2$ и $C_2$ по модулю s, при этом результат операции E модульного возведения в степень отбрасывается как ошибочный, если $C_1 \neq z_1 \text{mod } r$ или $C_2 \neq z_2 \text{mod } s$.

18. Чип-карта по п.17, отличающаяся тем, что числа r и s являются нечетными.

19. Чип-карта по любому из пп.16-18, отличающаяся тем, что числа r и s выбираются из интервала $[0, 2^k-1]$, где $16 \leq k \leq 32$.

20. Чип-карта по любому из пп.16-18, отличающаяся тем, что по меньшей мере одно из чисел r и s выбирается таким образом, чтобы в двоичном представлении произведения p·r, соответственно q·s присутствовало максимально большое количество ведущих единиц.

21. Чип-карта по п.20, отличающаяся тем, что

а) сначала на первом подэтапе по меньшей мере для одного из чисел r и s выбирается соответствующее оптимальное число $r_{опт}$, соответственно $s_{опт}$ без ограничения такого выбора условием, согласно которому величины d и $\phi(kgV(r, s))$ должны быть взаимно простыми, и

б) на втором подэтапе выбирается по соседнему значению $r=r_{опт}-i$, соответственно $s=s_{опт}-i$, где i=0, 1, ..., k, таким образом, чтобы величины d и $\phi(kgV(r, s))$ были взаимно простыми.

22. Чип-карта по п.20, отличающаяся тем, что

а) на первом подэтапе для каждого из чисел r и s выбирается соответствующее оптимальное число $r_{опт}$, соответственно $s_{опт}$ без ограничения такого выбора условием, согласно которому величины d и $\phi(kgV(r, s))$ должны быть взаимно простыми, и

б) на втором подэтапе выбирается по значению $r=2^1 \cdot r_{опт}$, соответственно $s=2^1 \cdot s_{опт}$, где 1=0, 1, ..., j, таким образом, чтобы величины d и $\phi(kgV(r, s))$ были взаимно простыми.

23. Чип-карта по п.20, отличающаяся тем, что

а) сначала на первом подэтапе выбирается по меньшей мере одно из чисел $r_{опт}$ и $s_{опт}$ без ограничения такого выбора условием, согласно которому величины d и $\phi(kgV(r, s))$ должны быть взаимно простыми,

б) на втором подэтапе выбирается по соседнему значению $r=r_{опт}-i$, соответственно $s=s_{опт}-i$, где i=0, 1, ..., k, таким образом, чтобы величины d и $\phi(kgV(r, s))$ были взаимно простыми, при условии, что такое значение существует для i=0, 1, ..., k, и

в) на третьем подэтапе в том случае, если на втором подэтапе не было выбрано ни одного значения, выбирается по значению $r=2^1 \cdot r_{опт}$, соответственно $s=2^1 \cdot s_{опт}$, где 1=0, 1, ..., j, таким образом, чтобы величины d и $\phi(kgV(r, s))$ были взаимно простыми.

24. Чип-карта по любому из пп.16-18, отличающаяся тем, что оба числа r и s выбираются таким образом, чтобы в двоичном представлении произведения $p \cdot r$ и произведения $q \cdot s$ присутствовало максимально большое количество ведущих единиц.

25. Чип-карта по п.24, отличающаяся тем, что

а) сначала на первом подэтапе по меньшей мере для одного из чисел r и s выбирается соответствующее оптимальное число $r_{опт}$, соответственно $s_{опт}$ без ограничения такого выбора условием, согласно которому величины d и $\phi(kgV(r, s))$ должны быть взаимно простыми, и

б) на втором подэтапе выбирается по соседнему значению $r=r_{опт}-i$, соответственно $s=s_{опт}-i$, где i=0, 1, ..., k, таким образом, чтобы величины d и $\phi(kgV(r, s))$ были взаимно простыми.

26. Чип-карта по п.24, отличающаяся тем, что

а) на первом подэтапе для каждого из чисел r и s выбирается соответствующее оптимальное число $r_{опт}$, соответственно $s_{опт}$ без ограничения такого выбора условием, согласно которому величины d и $\phi(kgV(r, s))$ должны быть взаимно простыми, и

б) на втором подэтапе выбирается по значению $r=2^1 \cdot r_{опт}$, соответственно $s=2^1 \cdot s_{опт}$, где 1=0, 1, ..., j, таким образом, чтобы величины d и $\phi(kgV(r, s))$ были взаимно простыми.

27. Чип-карта по п.24, отличающаяся тем, что

а) сначала на первом подэтапе выбирается по меньшей мере одно из чисел $r_{опт}$ и $s_{опт}$ без ограничения такого выбора условием, согласно которому величины d и $\phi(kgV(r, s))$ должны быть взаимно простыми,

б) на втором подэтапе выбирается по соседнему значению $r=r_{опт}-i$, соответственно $s=s_{опт}-i$, где i=0, 1, ..., k, таким образом, чтобы величины d и $\phi(kgV(r, s))$ были взаимно простыми, при условии, что такое значение существует для i=0, 1, ..., k, и

в) на третьем подэтапе в том случае, если на втором подэтапе не было выбрано ни одного значения, выбирается по значению $r=2^1 \cdot r_{опт}$, соответственно $s=2^1 \cdot s_{опт}$, где 1=0, 1, ..., j, таким образом, чтобы величины d и $\phi(kgV(r, s))$ были взаимно простыми.

28. Чип-карта по любому из пп.16-18, отличающаяся тем, что она выполнена с

возможностью осуществления криптографического способа, предусматривающего выполнение алгоритма Райвеста-Шамира-Адлемана.

29. Чип-карта по любому из пп.16-18, отличающаяся тем, что она выполнена с возможностью осуществления криптографического способа, предусматривающего выполнение алгоритма цифровой подписи Рабина.

30. Чип-карта по любому из пп.16-18, отличающаяся тем, что она выполнена с возможностью осуществления криптографического способа, предусматривающего выполнение алгоритма идентификации Фиата-Шамира.