РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 450 457** (13) **C1**

(51) МПК
H04K 1/00 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2011120553/08, 20.05.2011**

(24) Дата начала отсчета срока действия патента:
20.05.2011

Приоритет(ы):
(22) Дата подачи заявки: **20.05.2011**

(45) Опубликовано: **10.05.2012** Бюл. № **13**

(56) Список документов, цитированных в отчете о поиске: **WO 03/007539 A1, 23.01.2003. RU 2004132057 A, 10.04.2006. WO 03/013052 A1, 13.02.2003. WO 2006/117769 A2, 09.11.2006. EP 1691503 A1, 16.08.2006. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. - СПб.: БХВ-Петербург, 2010.**

Адрес для переписки:
424000, Республика Марий Эл, г.Йошкар-Ола, пл. Ленина, 3, ГОУ ВПО Марийский государственный технический университет, отдел интеллектуальной собственности

(72) Автор(ы):
Леухин Анатолий Николаевич (RU),
Петухов Алексей Сергеевич (RU)

(73) Патентообладатель(и):
Государственное образовательное учреждение высшего профессионального образования Марийский государственный технический университет (RU)

(54) СПОСОБ ШИФРОВАНИЯ

(57) Реферат:

Изобретение относится к области электросвязи, а именно к области устройств и способов криптографической защиты информации, хранящейся на носителях информации, либо передаваемой по открытым каналам связи. Техническим результатом является повышение криптостойкости при использовании относительно невысоких степеней вычислений. Технический результат достигается тем, что формируют исходное сообщение M в виде элемента некоммутативной конечной группы Г на основе алгебры Кэли с выполнением операций по модулю простого числа p, генерируют секретный ключ шифрования в виде пары элементов X и X^{-1} группы Г и многоразрядного числа e, генерируют начальную криптограмму Y путем формирования элемента R группы Г возведением исходного сообщения M в степень e, формирования элемента V группы Г путем выполнения групповой операции над элементами X и R группы Г и последующего выполнения групповой операции над элементами V и X^{-1} группы Г, генерируют криптограмму C в виде элемента Г путем y-кратного выполнения операции, аналогичной операции генерирования начальной криптограммы Y, за исключением того, что на каждом i шаге в качестве элементов X и X^{-1} группы Г используются элементы X^i и X^{-i} соответственно, а вместо элемента M используется результат предыдущей операции ($Y, Y_1, Y_2, \ldots, Y_i$). 3 табл., 1 пр.

RU 2450457 C1

RU 2450457 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 450 457** (13) **C1**

(51) Int. Cl.
H04K 1/00 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2011120553/08, 20.05.2011**

(24) Effective date for property rights:
20.05.2011

Priority:
(22) Date of filing: **20.05.2011**

(45) Date of publication: **10.05.2012 Bull. 13**

Mail address:
424000, Respublika Marij Ehl, g.Joshkar-Ola, pl. Lenina, 3, GOU VPO Marijskij gosudarstvennyj tekhnicheskij universitet, otdel intellektual'noj sobstvennosti

(72) Inventor(s):
Leukhin Anatolij Nikolaevich (RU),
Petukhov Aleksej Sergeevich (RU)

(73) Proprietor(s):
Gosudarstvennoe obrazovatel'noe uchrezhdenie vysshego professional'nogo obrazovanija Marijskij gosudarstvennyj tekhnicheskij universitet (RU)

(54) ENCRYPTION METHOD

(57) Abstract:

FIELD: information technology.

SUBSTANCE: original message M is generated in form of a non-commutative finite group G based on Cayley algebra while performing modulo operations over a prime number p; a secret encryption key is generated in form of pairs of elements X and X^{-1} of group G and a multidigit number e; the initial cryptogram Y is generated by generating an element R of group G by raising the original message M to the power of e; an element V of group G is generated by performing a group operation over elements X and R of group G and subsequent group operation over elements V and X^{-1} of group G; a cryptogram C is generated in form of an element G by y-fold performance of an operation similar to the operation of generating the initial cryptogram Y, except that on each i-th step, elements X^i and X^{-i} are used as elements X and X^{-1} of group G, respectively, and the result of the previous operation (Y, Y_1, Y_2, …, Y_i) is used instead of element M.

EFFECT: high cryptographic robustness when using relatively low degree of computations.

3 tbl, 1 ex

RU 2450457 C1

RU 2450457 C1

Изобретение относится к области электросвязи и вычислительной техники, а именно к области информационной безопасности вычислительных и телекоммуникационных систем, и может быть использовано в системах криптографической защиты информации, обеспечивающих конфиденциальность сообщений, передаваемых по открытым каналам связи, и данных, хранящихся на информационных носителях.

Известен способ шифрования [Смарт Н. Мир программирования. Криптография. М.: ТЕХНОСФЕРА, 2005. - 525 с.; см. с.200-202], в котором генерируют конечную группу Г с операцией умножения по модулю p, где p - простое число, в качестве групповой операции. Формируют элемент G конечной группы Г. У получателя сообщения генерируют открытый ключ в виде элемента Y конечной группы Г, для чего генерируют его личный секретный ключ в виде любого натурального числа x, и вычисляют H по формуле $H=G^x \bmod p$. Открытый ключ G передают по открытому каналу отправителю сообщения. У отправителя сообщения генерируют секретный ключ шифрования в виде элемента Z конечной группы Г, для чего формируют вспомогательный секретный ключ в виде случайного k и вычисляют элемент R группы Г по формуле $R=G^k \bmod p$. По открытому ключу получателя и вспомогательному секретному ключу k генерируют секретный ключ шифрования Z по формуле $Z=H^k \bmod p$. Затем формируют сообщение в виде элемента M конечной группы Г и генерируют криптограмму в виде элемента C конечной группы Г путем выполнения групповой операции между элементами Z и M, т.е. по формуле $C=Z \cdot M \bmod p$. Недостатком данного способа шифрования является относительная сложность реализации процедуры шифрования, затраты памяти, выделяемой на хранение и обработку нескольких ключей, и относительное увеличение времени передачи сообщений, также связанное с обработкой и передачей нескольких ключей.

Также известен способ шифрования, являющийся ближайшим аналогом, заключающийся в генерации конечной группы Г, формирования сообщения в виде элемента M конечной группы Г, генерации секретного ключа шифрования, генерации криптограммы в виде элемента C конечной группы Г путем преобразования сообщения M в зависимости от секретного ключа шифрования [Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. СПб.: БХВ-Петербург, 2010. - 304 с.; см. с.245-248].

Прототип выполняет следующие действия:

1. Генерируют некоммутативную конечную группу Г.

2. Формируют сообщение в виде элемента M конечной группы Г. Генерируют секретный ключ шифрования в виде многоразрядного двоичного числа e и двух взаимно обратных элементов X и W группы Г, для которых выполняются условия $W=X^{-1}$ и $X=W^{-1}$.

3. Генерируют криптограмму C путем формирования элемента R конечной группы Г, равного e-й степени сообщения M, т.е. $R=M^e$, формирования элемента V конечной группы Г путем выполнения групповой операции между элементами X и R конечной группы Г и последующего выполнения групповой операции между элементами V и W конечной группы Г.

Недостатком прототипа является неформализованное правило умножения базисных векторов и, следовательно, неформализованный способ получения элементов конечной группы Г. Алгебры Клиффорда-Грассмана позволяют алгоритмизировать процедуру построения различных таблиц умножения элементов некоммутативных групп. Также прототип использует поиск одного сопряженного

элемента некоммутативной группы. Данная задача относится к классу сложных, однако однократное применение этой процедуры значительно уступает по сложности ее многократному применению. Разработанный способ предлагает поиск нескольких сопряженных элементов (до p), что существенно повышает криптостойкость предлагаемого алгоритма, по сравнению с прототипом.

Целью изобретения является разработка метода шифрования с четко определенным способом задания конечных некоммутативных групп, обладающего повышенной криптостойкостью при использовании относительно малых разрядностей чисел за счет значительного повышения вычислительной емкости алгоритма.

Поставленная цель достигается путем того, что генерируют конечную группу Г, формируют исходное сообщение M в виде элемента конечной группы Г, формируют секретный ключ шифрования, генерируют криптограмму C в виде элемента группы Г преобразованием исходного сообщения M секретным ключом шифрования, отличаясь тем, что в качестве конечной группы Г генерируют некоммутативную конечную группу на основе алгебры Клиффорда с выполнением групповых операций по модулю простого многоразрядного числа p, генерируют секретный ключ шифрования в виде пары элементов X и X^{-1} группы Г и многоразрядного числа e, генерируют начальную криптограмму Y путем формирования элемента R группы Г возведением исходного сообщения M в степень e, формирования элемента V группы Г путем выполнения групповой операции над элементами X и R группы Г и последующего выполнения групповой операции над элементами V и X^{-1} группы Г, генерируют криптограмму C путем y-кратного выполнения операции, аналогичной операции генерирования начальной криптограммы Y, за исключением того, что на каждом i шаге в качестве элементов X и X^{-1} группы Г используются элементы X^i и X^{-i} соответственно, а вместо элемента M используется результат предыдущей операции ($Y, Y_1, Y_2, \ldots, Y_i$).

Новым в разработанном методе является способ формирования группы Г по конкретизированному правилу умножения базисных векторов, основанному на использовании специального вида ассоциативной алгебры, называемой также алгеброй Клиффорда. Конечные ассоциативные группы, основанные на данном виде алгебры, всегда проявляют некоммутативные свойства, не требуя каких-либо дополнительных подборов коэффициентов.

Также новым в изобретении является то, что над исходным сообщением y-кратно выполняют групповые операции. Это производится с целью максимально полного использования возможного набора разрешенных элементов конечной группы, что позволяет многократно усилить криптостойкость кодированного сообщения.

Изобретательский замысел заявленного нового технического решения состоит в применении некоммутативных конечных групп, построенных по правилам алгебры Клиффорда и имеющих элементы, значения которых не превышают некоторого простого многоразрядного числа p, в которых в общем случае результат выполнения групповой операции зависит от порядка расположения элементов группы, над которыми выполняется групповая операция. Благодаря этому уравнения вида $C = X \bullet Z^e \bullet X^{-1}$ с неизвестным значением X являются трудно решаемыми при соответствующем выборе группы Г и ее элементов X и Z. Это позволяет использовать значение X в качестве секретного ключа шифрования и выполнять шифрование, предварительно формируя сообщение в виде элемента M группы Г, по формуле $Y = X \bullet M^e \bullet X^{-1}$, где e - многоразрядное число. Для получения шифротекста C с целью увеличения криптостойкости получаемого шифра применяется y-кратное выполнение

аналогичной групповой операции, в которой на каждом i шаге вместо значений X и X^{-1} принимаются элементы X^i и X^{-i} группы Г, а в качестве элемента M группы Г принимается результат предыдущего шага, т.е.

$C = X^y \bullet Y_y^e \bullet X^{-y}$, где $Y_y = X^{y-1} \bullet Y_{y-1}^e \bullet X^{-y-1}$, $Y_{y-1} = X^{y-2} \bullet Y_{y-2}^e \bullet X^{-y-2}, \ldots,$ а $Y_1 = X \bullet M^e \bullet X^{-1}$.

На начальном этапе реализации метода следует сгенерировать 2 некоммутативные конечные подгруппы: $Г_1$ для выбора из нее элемента секретного ключа X, и $Г_2$ для формирования на основе ее элементов исходного сообщения M. Данные подгруппы формируются по одному из правил алгебры Клиффорда с условием, что порядок подгрупп будет максимально возможным для выбранного способа построения, а значения элементов не превосходят выбранного многоразрядного простого числа p. Для генерации элемента секретного ключа X следует выбрать любой элемент подгруппы $Г_1$, не являющийся единичным элементом группы. Также генерируются дополнительные ключи шифрования в виде многоразрядных чисел e и y. При такой реализации заявленного способа шифрования формула шифрования примет вид:

$C = X^y \bullet Y_y^e \bullet X^{-y}$, где $Y_y = X^{y-1} \bullet Y_{y-1}^e \bullet X^{-y-1}, \ldots,$ а $Y_1 = X \bullet M^e \bullet X^{-1}$.

Формула расшифровки сообщения в этом случае примет вид:

$M = X^{-1} \bullet Y_1^d \bullet X$, где $Y_1 = X^{-2} \bullet Y_2^d \bullet X^2, \ldots,$ а $Y_y = X^{-y} \bullet C^d \bullet X^y$,

где d - дополнительный секретный ключ дешифрования, который легко вычисляется из дополнительного секретного ключа шифрования как МДМ, обратное e по модулю, равному максимальному значению p порядка элементов группы.

Как уже говорилось, правило задания конечной некоммутативной группы основывается на выполнении групповой операции по правилам алгебры Клиффорда. Это позволяет конкретизировать генерацию конечной группы и, более того, увеличить мощность шифрования, поскольку с каждым новым выбранным правилом выполнения групповой операции меняется порядок элементов конечной группы. Этот факт является дополнительным фактором в усилении стойкости алгоритма шифрования. Так, например, для известного множества векторов алгебры Клиффорда, названных кватернионами, правило выполнения групповой операции над векторами вида $(1, ie_1, je_2, ke_3)$ при построении таблицы умножения базисных векторов имеет диагональ вида (1, -1, -1, -1). Ниже приведены примеры таблиц умножения базисных векторов.

·	**1**	$\mathbf{e_1}$	$\mathbf{e_2}$	$\mathbf{e_3}$
1	1	e_1	e_2	e_3
$\mathbf{e_1}$	e_1	-1	e_3	$-e_2$
$\mathbf{e_2}$	e_2	$-e_3$	-1	e_1
$\mathbf{e_3}$	e_3	e_2	$-e_1$	-1

Таблица 1. Умножение базисных векторов с диагональю (1, -1, -1, -1)

·	**1**	$\mathbf{e_1}$	$\mathbf{e_2}$	$\mathbf{e_3}$
1	1	e_1	e_2	e_3
$\mathbf{e_1}$	e_1	1	e_3	e_2
$\mathbf{e_2}$	e_2	$-e_3$	1	$-e_1$
$\mathbf{e_3}$	e_3	$-e_2$	e_1	-1

Таблица 2. Умножение базисных векторов с диагональю (1, 1, 1, -1)

Аналогичным способом можно задается любое правило выполнения групповых операций. Также правила алгебры Клиффорда позволяют генерировать конечные некоммутативные группы с n-мерными элементами. Так, известными примерами

реализации правил n-мерной алгебры Клиффорда являются 4-мерные кватернионы, 8-мерные бикватернионы, 16-мерные седенионы, и т.д.

·	**1**	$\mathbf{e_1}$	$\mathbf{e_2}$	$\mathbf{e_3}$	$\mathbf{e_4}$	$\mathbf{e_5}$	$\mathbf{e_6}$	$\mathbf{e_7}$
1	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
$\mathbf{e_1}$	e_1	1	e_4	e_5	e_2	e_3	e_7	e_6
$\mathbf{e_2}$	e_2	$-e_4$	1	e_6	$-e_1$	$-e_7$	e_3	$-e_5$
$\mathbf{e_3}$	e_3	$-e_5$	$-e_6$	1	e_7	$-e_1$	$-e_2$	e_4
$\mathbf{e_4}$	e_4	$-e_2$	e_1	e_7	-1	$-e_6$	e_5	$-e_3$
$\mathbf{e_5}$	e_5	$-e_3$	$-e_7$	e_1	e_6	-1	$-e_4$	e_2
$\mathbf{e_6}$	e_6	e_7	$-e_3$	e_2	$-e_5$	$-e_4$	-1	$-e_1$
$\mathbf{e_7}$	e_7	e_6	$-e_5$	e_4	$-e_3$	e_2	$-e_1$	-1

Таблица 3. Умножение базисных векторов бикватернионов

Рассмотрим пример реализации заявленного способа шифрования.

Пример 1

Реализация способа шифрования сообщения с последующей его расшифровкой. Для формирования группы используется наиболее распространенное правило умножения элементов алгебры Клиффорда, формирующее множество кватернионов (Таблица 1).

1. Генерируют простое число p=67.

2. Генерируют две подгруппы Γ_1 и Γ_2.

3. Генерируют элемент секретного ключа X из подгруппы Γ_1, а также дополнительные ключи шифрования - произвольное простое число e и произвольное число y. Также из группы M_2 выберем произвольный элемент M в качестве исходного сообщения.

X=(13 40 29 54), e=13, y=7.

4. Формируют исходное сообщение в виде элемента M подгруппы Γ_2.

M=(40 13 57 59)

5. Генерируют криптограмму C

$Y_1=X \bullet M^{13} \bullet X^{-1}=(37\ 1\ 40\ 19)$,

$Y_2 = X^2 \bullet Y_1^{13} \bullet X^{-2} = (12\ 27\ 22\ 57)$

…

$C = Y_7 = X^7 \bullet Y_6^{13} \bullet X^{-7} = (60\ 3\ 11\ 24)$

В результате указанных выше действий получают криптограмму C. Для вычисления исходного сообщения M из шифра C найдем дополнительный секретный ключ расшифрования d=1381, который вычисляется из дополнительного секретного ключа шифрования как МДМ, обратное e по модулю, равному максимальному значению p порядка элементов группы.

$Y_6 = X^{-7} \bullet Y_1^{1381} \bullet X^7 = (11\ 51\ 40\ 54)$,

$Y_5 = X^{-6} \bullet Y_6^{1381} \bullet X^6 = (17\ 53\ 51\ 43)$,

…

$M = Y_0 = X^{-1} \bullet Y_1^{1381} \bullet X = (40\ 13\ 57\ 59)$

Сравнение вычисленного сообщения с исходным сообщением показывает, что

криптограмма C расшифрована правильно, т.е. из нее получено исходное сообщение M.

Таким образом, приведенные конкретные примеры реализации показывают, что заявляемый способ шифрования технически реализует и позволяет достичь сформулированный технический результат.

Формула изобретения

Способ шифрования, заключающийся в том, что генерируют конечную группу Г, формируют исходное сообщение M в виде элемента конечной группы Г, формируют секретный ключ шифрования, генерируют криптограмму C в виде элемента группы Г преобразованием исходного сообщения M секретным ключом шифрования, отличающийся тем, что в качестве конечной группы Г генерируют некоммутативную конечную группу на основе алгебры Кэли с выполнением операций по модулю простого числа p, генерируют секретный ключ шифрования в виде пары элементов X и X^{-1} группы Г и многоразрядного числа e, генерируют начальную криптограмму Y путем формирования элемента R группы Г возведением исходного сообщения M в степень e, формирования элемента V группы Г путем выполнения групповой операции над элементами X и R группы Г и последующего выполнения групповой операции над элементами V и X^{-1} группы Г, генерируют криптограмму C путем y-кратного выполнения операции, аналогичной операции генерирования начальной криптограммы Y, за исключением того, что на каждом i шаге в качестве элементов X и X^{-1} группы Г используются элементы X^i и X^{-i} соответственно, а вместо элемента M используется результат предыдущей операции ($Y, Y_1, Y_2, \ldots, Y_i$).