(19) Евразийское патентное ведомство

(11) 042189 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2023.01.23

(21) Номер заявки
202290743

(22) Дата подачи заявки
2022.03.30

(51) Int. Cl. ***H04L 9/14*** (2006.01)

(54) СПОСОБ И УСТРОЙСТВО ШИФРОВАНИЯ ДАННЫХ

(31) **2021108649**
(32) **2021.03.30**
(33) **RU**
(43) **2022.10.31**

(71)(73) Заявитель и патентовладелец:
АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ "УНИВЕРСИТЕТ ИННОПОЛИС" (RU)

(72) Изобретатель:
Осетрин Евгений Юрьевич, Петренко Сергей Анатольевич, Асадуллин Якуп Яруллович (RU)

(56) БУТЫРКА Ф. Б.: Пакетное симметричное полностью гомоморфное шифрование на основе матричных полиномов. Труды ИСП РАН, т. 26, вып. 5, 2014 г., с. 99-115, стр. 99-108, разделы 2.1, 2.2, 4, алгоритмы 1, 2
RU-C1-2652443
RU-C2-2691874
US-B2-9166785
US-B1-10116437
US-B2-10673614

(57) Изобретение относится к области вычислительной техники и может быть использовано в системах обработки информации и защиты данных. Технический результат заключается в повышении защищенности информации в недоверенной среде. Генерируют секретный ключ, генерируют ключ перешифрования, выполняют шифрование данных. При этом формирование секретного ключа K(X) происходит посредством генерации матричного полинома степени N, а при шифровании данных формируется матрица M с собственным вектором при собственном значении, равным открытому тексту, при этом $\vec{k}$ - вектор длины N. При этом способ шифрования данных дополнительно содержит этап, на котором выполняют вычисление функций от зашифрованных данных с получением результата в зашифрованном виде.

042189 B1

042189 B1

Изобретение относится к области вычислительной техники и может быть использовано в системах обработки информации и защиты данных.

Известно техническое решение "Способ защиты информации в облачных вычислениях с использованием гомоморфного шифрования" патент РФ № 2691874 от 07.11.2017 г. [2], в котором предлагается реализация системы защищенных облачных вычислений, содержащая сервер, получающий данные от клиента, причем данные поступают на сервер в зашифрованном виде, а также сервис облачных вычислений, реализованный на сервере для выполнения вычислений в интересах клиента, при этом сервер выполняет вычисления, не прибегая к дешифровке данных, и отправляет результат обратно клиенту, а клиент может расшифровать результат, причем клиентом формируется конечный набор исходных элементов, который трансформируется в набор зашифрованных элементов применением алгоритма частично или полностью гомоморфного шифрования.

К недостаткам описанного решения можно отнести то, что обращение к облачному хранилищу данных связано с потенциальной угрозой несанкционированного изменения передаваемой информации и требует высокого уровня надежности, кроме того, использование облачного программного обеспечения не обладает гибкостью настроек при шифровании данных и требует постоянное высокоскоростное подключение к сети Интернет.

Наиболее близким техническим решением является "Система и способ определения количества голосов избирателей, собираемых с помощью электронного голосования", патент РФ № 2652443 от 17.07.2017 г. [3]. Изобретение предназначено для проведения электронного голосования. Техническим результатом является повышение точности определения количества голосов проголосовавших избирателей, собираемых с помощью электронного голосования. Система содержит одно вычислительное устройство организатора голосования, имеющее средство регистрации наблюдателей, предназначенное для создания для каждого наблюдателя идентификационных данных (открытого ключа и децентрализованного реестра записей сформированных голосов, получаемых наблюдателем от соответствующих избирателей), и средство подсчета голосов избирателей, предназначенное для проверки подлинности децентрализованных реестров записей и на основании расшифрованной информации вычисления количества голосов избирателей, отданных за каждого из кандидатов, вычислительное устройство по меньшей мере двух наблюдателей, имеющее средство регистрации голосов избирателей, и вычислительные устройства избирателей

Недостатком таких системы и способа является то, что в данной системе используется частично гомоморфная криптосистема Эль-Гамаля, позволяющая вычислять только сумму зашифрованных данных.

Предлагается новый способ и устройство шифрования данных, свободные от упомянутых недостатков.

Техническим результатом предлагаемого способа и устройства является повышение защищенности и надежности информации в недоверенной среде.

Технический результат достигается тем, что в способе формирование секретного ключа K(X) происходит посредством генерации матричного полинома степени N, а при шифровании данных формируется матрица M с собственным вектором $\vec{k}$ при собственном значении равного открытому тексту, при этом $\vec{k}$ - вектор длины N, при этом способ шифрования данных дополнительно содержит этап, на котором выполняют вычисление функций от зашифрованных данных с получением результата в зашифрованном виде.

Технический результат также достигается тем, что в устройстве дополнительно содержится блок вычисления функций от зашифрованных данных для персонализированного шифрования данных, при этом блок зашифрования использует способ по п.1 для надежности информации в недоверенной среде.

Сущность изобретения показана на фигурах.

На фиг. 1 показана функциональная схема реализации способа гомоморфного шифрования данных;

на фиг. 2 показана схема взаимодействия устройства с внешними устройствами;

на фиг. 3 показана структурная схема предлагаемого устройства.

На фиг. 1 способ работает следующим образом.

Представим, что пространством открытых текстов является Zp, где p - простое число. Шифр-текстами являются матричные полиномы. Секретный ключ - это пара $^{(K(X),\,\vec{k})}$, где $\vec{k}$ - N-мерный вектор целых чисел по модулю p, K(X) - матричный полином.

В предлагаемом способе помимо секретного ключа используется ключ перешифрования, представляющий собой матричный полином rk(X), который передаётся на сторону вычислений для сокращения размеров шифр-текстов.

Тогда структура предлагаемого полного гомоморфного шифрования будет выглядит следующим образом:

1. Генерация секретного ключа

1.1. Генерируется приведённый полином K(X), не имеющий корней, степени N.

1.2. Генерируется вектор $\vec{k}$

1.3. Пара $^{(K(X),\,\vec{k})}$ сохраняется в качестве секретного ключа.

2. Генерация ключа перешифрования

Ключ перешифрования используется для предотвращения роста размера шифротекстов. После перемножения шифротекстов результат приводится по модулю ключа перешифрования.

2.1. Генерируется приведённый матричный полином R(X) степени N-1.

2.2. Полином rk(X)=R(X)·K(X) сохраняется в качестве ключа перешифрования.

3. Шифрование

3.1. Открытому тексту m ∈ Zp ставится в соответствие случайная матрица M, такая что

$$M\cdot\vec{k} = m\cdot\vec{k} \text{ и } M\cdot K(X) = K(X)\cdot M$$

т.е. матрица M имеет собственный вектор $\vec{k}$ при собственном значении m и коммутирует с матричным полиномом K(X).

3.2. Генерируется матричный полином R(X) степени N-1.

3.3. Вычисляется шифротекст C(X) = R(X)K(X)+M.

Известно, что поиск матрицы с заданными собственным вектором и собственным значением, которая должна коммутировать с заданным матричным многочленом процесс вычислительно сложный и не был описан авторами алгоритма. Поэтому на фиг. 1 предлагается новый способ преобразования данных, при котором генерируется криптографический ключ $(K(X); \vec{k})$ и происходит генерация матрицы M, которая ставится в соответствие открытому тексту m 100.

Пусть $\mathbb{Z}_p^{NxN}$ - кольцо квадратных матриц.

$\mathbb{Z}_p$ - поле вычетов, где p - простое число.

$\mathbb{Z}_p^{NxN}[X]$ - множество матричных полиномов над кольцом $\mathbb{Z}_p^{NxN}$

Секретным ключом в способе [4] полностью гомоморфного преобразования на основе матричных полиномов является пара $(K(X); \vec{k})$, где

$K(X) \in \mathbb{Z}_p^{NxN}[X]$ - матричный полином степени N,

$\vec{k} \in \mathbb{Z}_p^N$ - вектор длины N.

При генерации секретного вектора $k^{\downarrow}$ 200 все координаты генерируем случайным образом. Последняя координата не должна равняться нулю, т.е. $k_N \neq 0$.

Опишем генерацию полинома K(X) степени n.

Из теории матриц [5] известно, что

Утв.1.

Если A - одноранговая матрица, т.е. $A=a^{\downarrow}_{1xn}\cdot\vec{b}_{nx1}$, то $(\lambda, x^{\downarrow}_{1xn})$ - собственная пара матрицы A тогда и только тогда когда $x^{\downarrow}=\frac{c}{\lambda}a^{\downarrow}$, где $c=(\vec{a},\vec{b})$ - скалярное произведение векторов $\vec{a}$ и $\vec{b}$.

Пусть A_i $(i=\overline{0,n})$ - матричные коэффициенты полинома K(X) степени n. Генерацию матриц A_i 300 будем осуществлять следующим образом.

$$A_n = E_{NxN}, \quad (1)$$

т.к. по условию K(X) должен быть приведённый.

При $i\in[0;n-1]$ $A_i= k^{\downarrow}\cdot\vec{a}_i$, где $\vec{a}_i=(a_{i1},\ldots,a_{iN})$ 400 и a_{ij} - случайные числа из $\mathbb{Z}_p$ $\forall$ $j=\overline{1,N}$

У всех матриц A_i, $i=\overline{0,n-1}$ собственным вектором является вектор $k^{\downarrow}$ в силу утверждения (1).

Таким образом, секретный ключ, состоящий из вектора $k^{\downarrow}$ и матричного полинома K(X) 500 сформирован.

Далее нам нужно по открытому тексту $m\in\mathbb{Z}_p$ найти матрицу $M\in\mathbb{Z}_p^{NxN}$, такую что число m будет её собственным значением, а $\vec{k}$ - собственным вектором.

Для этого найдём такой вектор $\vec{a}_{1xN}$, чтобы скалярное произведение $(\vec{k},\vec{a})$=m, где $\vec{k}$ - секретный вектор.

Пусть $\vec{a}=(a_1,\ldots,a_{N-1},a_N)$, $\vec{k}=(k_1,\ldots,k_{N-1},k_N)$.

Числа $a_1,\ldots,a_{N-1}$ 600 выбираем случайным образом. Последнее число a_N 700 вычисляем по формуле

$$a_N=\frac{m-\sum_{i=1}^{N-1}k_i\cdot a_i}{k_N} \quad (2)$$

т.к. $k_N \neq 0$, то выражение (2) имеет смысл.

Далее производим вычисление матрицы M 800 по формуле

$$M = \vec{k}\cdot\vec{a}. \quad (3)$$

В силу утверждения 1 [5] у матрицы M вектор $\vec{k}$ будет собственным вектором, а число m собственным значением.

Доказательство коммутативности М и К(Х).

Известно, что простые матрицы А и В из $\mathbb{Z}_p^{N\text{x}N}$ коммутируют тогда и только тогда, когда они имеют одинаковые собственные вектора [5].

В нашем случае все коэффициенты A_i $(i=\overline{1,n-1})$ полинома К(Х) и матрица М имеют один и тот же собственный вектор, а именно вектор $\vec{k}$.

Поэтому матрица М коммутирует со всеми матрицами A_i $(i=\overline{1,n})$ и значит М К(Х)= К(Х) М.

Таким образом, получаем новый способ шифрования данных на основе генерации секретного ключа, состоящего из матричного полинома К(Х) с вектором $\vec{k}$, который коммутирует с матрицей М.

На фиг. 2 представлена схема взаимодействия устройства

Предлагаемое устройство шифрования данных можно использовать, например, в так называемых безопасных гомоморфных системах с обратной связью, когда необходимо сохранить анонимность пользователя и скрыть промежуточные результаты вычислений. Системы помогают осуществлять анонимный сбор отзывов (комментариев) студентов либо преподавателей об их работе. Полученные таким образом отзывы шифруются и сохраняются для последующих вычислений. Системы с обратной связью могут быть использованы для повышения осведомленности о состоянии дел и улучшения показателей работы. Известно, что достоверная обратная связь любой системы или процесса может быть обеспечена только в случаях сохранения анонимности пользователя, неизменности данных, собранных в процессе обратной связи, обеспечения безопасности внутренних операций для анализа данных.

Устройство ввода данных 800 соединёно посредством коммутационного интерфейса 810 с устройством шифрования данных 900 представляющим сопроцессор, на выходе которого получаем шифрованные данные 910. Далее шифрованные данные передаются на устройство обработки данных 920.

Устройство ввода данных 800, устройство шифрования данных 900 и устройство обработки данных 920 обмениваются информацией по каналам коммутационного интерфейса.

На фиг. 3 представлена структурная схема предлагаемого устройства.

Сущность устройства состоит в обеспечении полного гомоморфного шифрования данных, выполняемого сопроцессором (фиг. 3).

Устройство шифрования данных представляет собой сопроцессор 900, на который поступают данные-открытый текст, например, которые требуется зашифровать.

На плате сопроцессора 900 размещаются блоки: зашифрования 901, расшифрования 902, вычисления функций от зашифрованных данных 903.

Схема работы устройства содержит следующие этапы. Этап генерации секретного ключа 850, этап шифрования данных, выполняемый блоком 901, этап представления зашифрованной информации центральному процессору 800.

Блок 901 содержит на входе открытый текст, на выходе шифрованный текст 910. Шифрование текста происходит описанным выше способом (п.1 формулы изобретения).

Если данные требуется расшифровать, то данные поступают в блок расшифрования 902, который содержит на входе шифрованный текст, на выходе открытый (расшифрованный) текст.

Блок вычисления функций от зашифрованных данных 903 служит для персонализированного зашифрования данных без применения облачных систем, которые имеют уязвимость в сети Интернет. Блок 903 содержит на входе два зашифрованных сообщения – шифр-текст 1 (шт1) и шифр-текст 2 (шт2). В блоке 903 реализует две функции $f(x,y)=x\cdot y$ и $f(x,y)=x+y$, одна из которых подается на вход. На выходе блока 903 выдается результат заданной функции от переменных шт1 и шт2 в зашифрованном виде. При расшифровке результата он будет равен применению той же функции от соответствующих шт1 и шт2 открытых (незашифрованных) данных.

Устройство реализует полностью гомоморфную криптосистему на основе матричных полиномов, позволяющую вычислять помимо суммы и произведение зашифрованных данных без предварительного расшифрования.

Литература

1. «Устройство и способ обработки шифрования» патент Японии № JP2014126866 от 27.12.2012 г.

2. «Способ защиты информации в облачных вычислениях с использованием гомоморфного шифрования» патент РФ № 2691874 от 07.11.2017 г.

3. «Система и способ определения количества голосов избирателей, собираемых с помощью электронного голосования», патент РФ № 2652443 от 17.07.2017г.

4. Ф.Б. Буртыка, Пакетное симметричное полностью гомоморфное шифрование на основе матричных полиномов. Труды ИСП РАН, том 26, вып.5, 2014 г., с.99-115

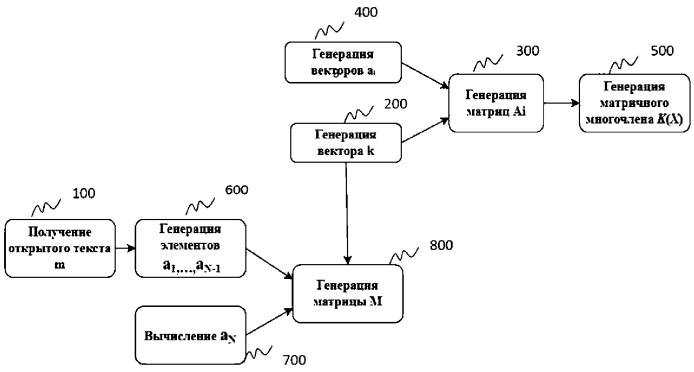
5. П.Ланкастер «Теория матриц», редакция физико-математическая литературы «Наука», 1973 г., 280 с.

6. «Прикладная гомоморфная криптография: примеры» Г.Г.Аракелов, А.В.Грибов, А.В.Михалев. Фундаментальная и прикладная математика, 2016 г., том 21, №3, с. 25—38.

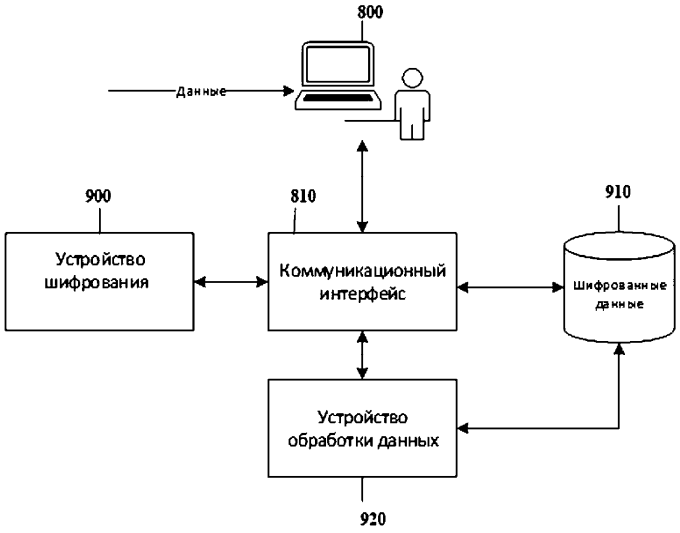
ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ шифрования данных, характеризующийся гомоморфным шифрованием данных, содержащий этапы генерации секретного ключа, генерацию ключа перешифрования, шифрование данных, отличающийся тем, что формирование секретного ключа K(X) происходит посредством генерации матричного полинома степени N, а при шифровании данных формируется матрица M с собственным вектором $\vec{k}$ при собственном значении равным открытому тексту, при этом $\vec{k}$ - вектор длины N, при этом способ шифрования данных дополнительно содержит этап, на котором выполняют вычисление функций от зашифрованных данных с получением результата в зашифрованном виде.

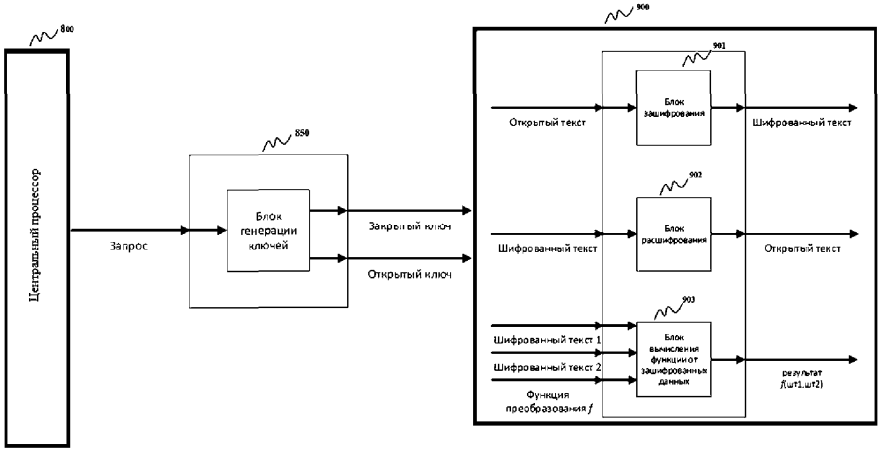
2. Устройство шифрования данных, содержащее блок генерации ключей, блок зашифрования данных, блок расшифрования данных, отличающееся тем, что устройство дополнительно содержит блок вычисления функций от зашифрованных данных, для персонализированного шифрования данных, при этом блок зашифрования использует способ по п.1 для надежности информации в недоверенной среде.



Фиг. 1


800
Данные
900
Устройство шифрования
810
Коммуникационный интерфейс
910
Шифрованные данные
Устройство обработки данных
920

Фиг. 2


800
Центральный процессор
Запрос
850
Блок генерации ключей
Закрытый ключ
Открытый ключ
900
901
Блок зашифрования
Открытый текст
Шифрованный текст
902
Блок расшифрования
Шифрованный текст
Открытый текст
903
Блок вычисления функции от зашифрованных данных
Шифрованный текст 1
Шифрованный текст 2
Функция преобразования f
результат f(шт1,шт2)

Фиг. 3