

(19)



Евразийское
патентное
ведомство

(21) 202290743 (13) АЗ

(12) ОТЧЕТ О ПАТЕНТНОМ ПОИСКЕ

(43) Дата публикации заявки
2022.10.31
Дата публикации отчета
2022.12.30

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

(22) Дата подачи заявки
2022.03.30

(54) СПОСОБ И УСТРОЙСТВО ШИФРОВАНИЯ ДАННЫХ

(31) 2021108649

(32) 2021.03.30

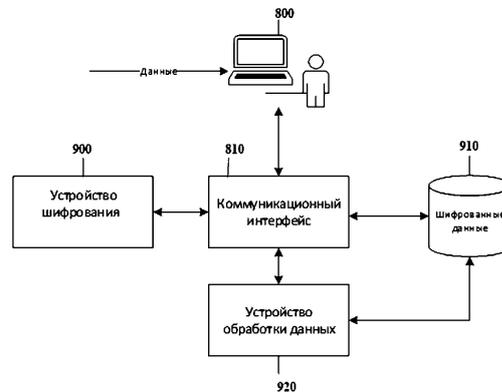
(33) RU

(88) 2022.12.30

(71) Заявитель:
АВТНОМНАЯ
НЕКОММЕРЧЕСКАЯ
ОРГАНИЗАЦИЯ ВЫСШЕГО
ОБРАЗОВАНИЯ "УНИВЕРСИТЕТ
ИННОПОЛИС" (RU)

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

(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 недовверенной 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 \vec{k} при собственном значении, равном 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.



АЗ

202290743

202290743

АЗ

ОТЧЕТ О ПАТЕНТНОМ ПОИСКЕ

(статья 15(3) ЕАПК и правило 42 Патентной инструкции к ЕАПК)

Номер евразийской заявки:

202290743А. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:
H04L 9/14 (2006.01)

Согласно Международной патентной классификации (МПК)

Б. ОБЛАСТЬ ПОИСКА:

Просмотренная документация (система классификации и индексы МПК)
H04L 9/00-9/14, G06F 17/00-17/10Электронная база данных, использовавшаяся при поиске (название базы и, если, возможно, используемые поисковые термины)
Espacenet, ЕАПАТИС, ЕРОQUE Net, Reaxys, Google

В. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ

Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей	Относится к пункту №
A	БУТЫРКА Ф. Б. Пакетное симметричное полностью гомоморфное шифрование на основе матричных полиномов. Труды ИСП РАН, том 26, вып.5, 2014 г., с. 99-115, страницы 99-108, разделы 2.1, 2.2, 4, алгоритмы 1, 2	1-2
A	RU 2652443 C1 (АКЦИОНЕРНОЕ ОБЩЕСТВО "ЛАБОРАТОРИЯ КАСПЕРСКОГО") 26.04.2018	1-2
A	RU 2691874 C2 (ИНГРАМ МИКРО ИНК.) 18.06.2019	1-2
A	US 9166785 B2 (FUJITSU LIMITED) 20.10.2015	1-2
A	US 10116437 B1 (INGRAM MICRO, INC.) 30.10.2018	1-2
A	US 10673614 B2 (MITSUBISHI ELECTRIC CORPORATION) 02.06.2020	1-2

 последующие документы указаны в продолжении

* Особые категории ссылочных документов:

«А» - документ, определяющий общий уровень техники

«D» - документ, приведенный в евразийской заявке

«E» - более ранний документ, но опубликованный на дату подачи евразийской заявки или после нее

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

"P" - документ, опубликованный до даты подачи евразийской заявки, но после даты испрашиваемого приоритета"

«Т» - более поздний документ, опубликованный после даты приоритета и приведенный для понимания изобретения

«X» - документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну или изобретательский уровень, взятый в отдельности

«Y» - документ, имеющий наиболее близкое отношение к предмету поиска, порочащий изобретательский уровень в сочетании с другими документами той же категории

«&» - документ, являющийся патентом-аналогом

«L» - документ, приведенный в других целях

Дата проведения патентного поиска: 01 ноября 2022 (01.11.2022)

Уполномоченное лицо:
Начальник Управления экспертизы

С.Е. Аверкиев