## Виктор Ю. Кадыков1, Алла Б. Левина2

*1Санкт-Петербургский национальный исследовательский университет   
информационных технологий, механики и оптики,*

*Кронверский пр-т, 49, Санкт-Петербург, 197101, Россия*

*2Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»*

*ул. Профессора Попова, 5, Санкт-Петербург, 197376, Россия*

*1e-mail: pflyers@rambler.ru, https://orcid.prg/0000-0002-6896-38022e-mail: alla\_levina@mail.ru, https://orcid.prg/0000-0003-4421-2411*

СОЗДАНИЕ ОБЩЕГО СЕКРЕТНОГО КЛЮЧА В РЕДУЦИРУЮЩЕМ ГОМОМОРФНОМ ШИФРОВАНИИ ДЛЯ КЛАССА КОНГРУЭНТНЫХ СИСТЕМ

*DOI: http://dx.doi.org/10.26583/bit.2021.2.10*

*Аннотация*. В настоящее время в области информационной безопасности особое внимание уделяется системам с гомоморфным шифрованием. В данной статье рассмотрены системы гомоморфного шифрования, использующие решетки идеалов. Решетки идеалов, как математический примитив, позволяют достичь существенной производительности по сравнению с основными стандартами шифрования. Также системы гомоморфного шифрования на решетках идеалов являются перспективными за счет устойчивости к атакам с применением квантовых компьютеров. Для класса конгруэнтных систем шифрования получен параметр шума как отношение параметров отображения шифртекста на различных классах сравнений или, в рассматриваемых случаях, на операциях взятия по модулю. В зависимости от параметров, задающих указанные классы, получены условия корректной расшифровки шифртекста. Установлено, что секретные ключи участников системы шифрования могут быть объединены в общий секретный ключ с помощью факторизации целых чисел. Результаты работы могут быть использованы для модификации существующей системы NTRU (Nth‑degree TRUncated polynomial ring) и для дополнения ее гомоморфным операциями, свойства которых для указанного класса систем были открыты относительно недавно. В статье используются положения теории множеств, вводится понятие конгруэнтного перехода, выводится необходимое условие вероятностной системы шифрования. Полученная математическая модель позволяет осуществлять обобщение на системы шифрования с большей размерностью или большим количеством участников, определяя эти параметры через выражение для общего секретного ключа, которое в свою очередь представлено как запись групповых операций на идеалах, используемых при построении структуры шифртекста. В настоящее время проводятся исследования по улучшению вычислительной эффективности полностью гомоморфных систем шифрования.

*Ключевые слова: гомоморфное шифрование, решетки идеалов, секретный ключ, теория множеств, информационная безопасность.*

*Для цитирования: КАДЫКОВ, Виктор Ю.; ЛЕВИНА, Алла Б.* *СОЗДАНИЕ ОБЩЕГО СЕКРЕТНОГО КЛЮЧА В РЕДУЦИРУЮЩЕМ ГОМОМОРФНОМ ШИФРОВАНИИ ДЛЯ КЛАССА КОНГРУЭНТНЫХ СИСТЕМ. Безопасность информационных технологий, [S.l.], v. 28, n. 2, p. 107–117, apr. 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1352>. Дата доступа: 25 may 2021.   
DOI: http://dx.doi.org/10.26583/bit.2021.2.10.*

Victor Y. Kadykov1, Alla B. Levina2*1Saint Petersburg National Research University of Information Technologies,   
Mechanics and Optics,   
Kronverksky prospect, 49, bldg. A, St. Petersburg, 197101, Russia*

*2Saint Petersburg Electrotechnical University "LETI",*

*Professora Popova str., 5, 197376, Saint-Petersburg, Russian*

*1e-mail: pflyers@rambler.ru, https://orcid.prg/0000-0002-6896-38022e-mail: alla\_levina@mail.ru, https://orcid.prg/0000-0003-4421-2411*

**Creating a joint secret key in reducing homomorphic encryption   
for a class of congruent systems**

*DOI: http://dx.doi.org/10.26583/bit.2021.2.10*

*Abstract.* Today special attention is paid to homomorphic encryption in the field of information security. Systems of homomorphic encryption represent such systems that allow arbitrary operations over ciphertext that are homomorphic to algebraic operations with plaintext. Some of such systems with ciphertext constructed over ideal lattices are reviewed in the paper. Ideal lattices, in turn, are promising mathematical primitives that allow achieving significant performance as compared to existing encryption systems. In addition, they are resistant to attacks based on quantum computer algorithms. The analysis of sets transforms in the reviewed systems showed that local dependencies and patterns exist between relations of its elements. For congruential encryption class systems, the relation between decryption conditions and noise levels is found. Moreover the private keys of encryption system participants can be hidden in a joint private key which is constructed with the factorial difficulty of recovery. The results can be used for modifying the existing NTRU encryption system and its complementation with homomorphic operations properties discovered recently. The study uses the provisions of set theory, introduces the concept of congruent transition, and deduces the necessary condition for a probabilistic encryption system. The obtained mathematical model is quite simple and allows a generalization of joint private key construction for arbitrary known number operations on a ciphertext. Research is underway to improve the computational efficiency of fully homomorphic encryption systems.

*Keywords: Homomorphic Encryption, Ideal Lattices, Joint Private Key, Sets Theory, Information Security.   
For citation: KADYKOV, Victor Y.; LEVINA, Alla B. Creating a joint secret key in reducing homomorphic encryption for a class of congruent systems. IT Security (Russia), [S.l.], v. 28, n. 2, p. 107–117, apr. 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1352>. Date accessed: 25 may 2021.   
DOI: http://dx.doi.org/10.26583/bit.2021.2.10.*

**Введение**

В настоящее время активно исследуется возможность обработки и изменений зашифрованных данных без знания секретного ключа и предварительного расшифровывания этих данных. Данная идея составляет основу процесса гомоморфного шифрования и может быть реализована, например, в механизме работы облачных технологий. Так, для гомоморфного шифрования справедливы соотношения:

где , – передаваемые сообщения, – функция шифрования, ,  
 – шифртекст, – некоторые операции над шифртекстом, которые часто можно представить композицией различных групповых операций в пространстве шифртекста . В представленных формулах операции , обеспечивают алгебраический гомоморфизм между шифртекстом и открытым текстом.

Первоначальная идея гомоморфного шифрования была предложена Джефри Хоффштейном в [1]. В тот момент существовали системы, поддерживающие гомоморфизм лишь для одной алгебраической операции, либо способные производить ограниченное количество вычислений – так называемые системы с частичным гомоморфизмом. Получение полного алгебраического гомоморфизма – задача, решение которой долгое время не было известно. Только в 1991 г. появилось формализованное определение гомоморфного шифрования [2], а затем была получена первая полностью гомоморфная система шифрования [3]. В качестве основы предложенной системы использовались решетки идеалов.

Данная идея продолжала совершенствоваться, и на протяжении нескольких поколений появились системы полностью гомоморфного шифрования и их модификации, пригодные для применения в различных областях, например, для сбора медицинских данных [4–6]. Новые системы были более практичными – менее требовательными к вычислительным ресурсам при неизменной длине ключа. Это удалось достичь за счет усложнения схем шифрования, однако, основная проблема произвольного увеличения размера шифртекста при вычислительных операциях до сих пор занимает центральное место в области гомоморфного шифрования. Проблему увеличения размера шифротекста связывают с накоплением шума после каждой операции, наличие которого обусловлено необходимостью внесения случайного параметра для защиты от атак на основе подобранного шифртекста, т.е. необходимостью построения вероятностной системы шифрования. Так, в [7, 8] было представлено доказательство того, что безопасность детерминированной системы может быть скомпрометирована при проведении атаки по выбранному шифртексту. В результате современные системы гомоморфного шифрования строятся вокруг операции динамического снижения шума и сильно зависят от нее, поскольку она занимает на несколько порядков больше вычислительных ресурсов, чем сами гомоморфные операции.

Другой проблемой для полностью гомоморфного шифрования является обеспечение криптостойкости, при наличии у атакующего множества из наборов выбранных шифртекстов. Данный вопрос не изучен в достаточной мере и в общем случае анализ стойкости системы сводится к оценке эффективности алгоритмов редукции базиса решетки в применяемой математической модели, например, алгоритмом Ленстры-Ленстры-Ловаса (LLL) или блочным алгоритмом Коркина-Золотарёва [9, 10].

В настоящее время подавляющее большинство работ, исследующих полностью гомоморфное шифрование, сосредоточено на улучшении эффективности систем последнего поколения построенных на основе математических примитивов использующих решетки идеалов и изучении свойств систем для снижения шума. Прежде всего, это обусловлено стойкостью решеток к атакам, использующим вычислительные алгоритмы на основе квантовой архитектуры компьютеров, в частности, использующим алгоритм Шора. Это создает впечатление, что решетки идеалов могут оказаться единственным примитивом, способным обеспечить полностью гомоморфное шифрование [11].

В данной работе исследуется структура шифртекста для конгруэнтной системы шифрования [12], в том числе структура шумовой составляющей. Вводится понятие конгруэнтного перехода, свойства которого используются при построении шифртекста. Показано, какое воздействие он оказывает на шумовую составляющую, и каким образом он может использоваться для формирования общего секретного ключа для гомоморфного шифрования с известным количеством операций.

Отличительной особенностью систем шифрования на решётках идеалов является то, что структура шифртекста поддерживает некоторый гомоморфизм изначально – на основе групповых операций и без дополнительных конструкций. В качестве практических результатов используется обобщение на реальную систему шифрования, использующую решетки идеалов – систему на усеченных полиноминальных кольцах, Nth-degree TRUncated polynomial ring system или NTRU [13]. Эта система дополнена гомоморфными операциями, и в статье отображено каким образом шумовая составляющая оказывает влияние на корректность расшифровывания.

1. **Теоретические сведения**

В общем случае негомоморфная симметричная система шифрования может быть представлена набором элементов , где - множество открытых текстов, – множество шифртекстов, – множество ключей, – функция шифрования, – функция дешифрования, т.е. для фиксированного ключа , открытого текста , шифртекста имеют место отображения:

В рассматриваемом случае множества открытого текста и шифртекста представляют собой идеалы, и для формирования необходимой структуры шифртекста и должны принадлежать одному решетчатому пространству (или решетке, обозначается ):

где – отображение решетки на базисе векторов , – размерность решетки,  
 – некоторый базис , состоящий из линейно независимых векторов, – элементы множества векторов, построенные с использованием выбранного базиса. Таким образом, решетка представляет собой все линейные комбинации базисных векторов с целочисленными коэффициентами.

Корректность шифрования обеспечивается соотношением:

где – шифруемое сообщение, а – сообщение, полученное после дешифрования. Условие выполняется для всех элементов подмножества открытого текста, входящего в пространство решетки. Любой идеал, как подмножество решетки, можно определить классом сравнений вида , и, таким образом, задать решетку, элементы которой порождаются заданными идеалами. Все это предполагает их использование в количестве отличном от одного. Предметом исследования данной работы выступают конгруэнтные классы идеалов, то есть классы, определяющие различные множества усеченных колец в пределах общего пространства решетки.

Зададим два класса идеалов для набора элементов системы:

где и представляют смежные классы (числовые кольца) по модулю и соответственно.

Согласно [7] детерминированные системы шифрования не являются стойкими для вычислений с применением компьютеров на квантовой архитектуре. Поэтому целесообразно будет рассматривать систему шифрования с вероятностной составляющей, тогда набор элементов системы преобразуется к виду:

где представляет собой множество случайных значений.

Чтобы акцентировать внимание на вопросах безопасности, допустим, что система шифрования является абсолютно стойкой, т.е. выполнено следующее равенство:

где – элемент множества открытого текста, – элемент множества шифртекста.

Введем понятие конгруэнтного перехода.

**Определение**. Отображение между подмножествами и называется конгруэнтным переходом от одного идеала к другому.

Подобный переход можно обеспечить построением системы линейных уравнений, взятых по модулю, для которой согласно следствию из китайской теоремы об остатках существует биективное отображение между и вектором значений {,}. Кроме этого, биективным является также отображение гомоморфной алгебры над шифртекстом по отношению к соответствующей ей алгебре над открытым текстом, причем как по модулю *q*, так и по модулю .

Согласно теореме Шеннона для абсолютно стойкой системы шифрования [14] чтобы такое отображение было возможным необходимо соблюдать непересечение множеств и , что определяется параметрами и , соответственно. Эти значения также являются ключевой информацией и составляют весь или часть секрета . При этих условиях можно рассматривать выстраиваемую математическую модель с допущениями, которые не затрагивают вопросы исходных данных (семплирования).

При открытый текст однозначно отображается в множество шифртекстов и ключом выступает сама схема преобразования, что не удовлетворяет принципу Кегрофсса.

При шифртекст не может быть однозначно расшифрован из-за возможных коллизий соответствующих множеств.

Выполнение неравенства является необходимым условием для построения вероятностной системы шифрования. В этом случае и, соответственно, отображение происходит без коллизий. Кроме этого, , то есть одному и тому же шифртексту может соответствовать несколько различных элементов в при фиксированном ключе, где – множество открытых сообщений, .

Конгруэнтный переход позволяет отделить в некотором множестве счетную часть множества от несчетной части, для ясности, например, ту часть, которую нельзя представить в виде линейной комбинации базисных векторов. В качестве основного способа может быть применена теорема арифметики о делении для случая целых чисел, используемых к качестве математического примитива для решетки . Таким способом можно выделить вероятностную составляющую шифртекста с целью дальнейшего преобразования значащей части.

1. **Конгруэнтная система шифрования**

Рассмотрим как работает описанный выше метод на примере конгруэнтной системы шифрования. Условия выбора параметров, при которых работает данная система, следующие:

Процесс получения расшифрованного сообщения представляет собой функцию от пяти параметров соответственно: – зашифрованный текст, – передаваемое сообщение, – случайное целое число, , – параметры системы, и , – секретные значения.

После выбора параметров системы участник выбирает значение секрета и вычисляет . В этом обозначении нижний индекс указывает на то, что обратное значение вычисляется по модулю :

Далее, для шифрования сообщения вычисляется ключ шифрования , выбирается случайное значение и происходит формирование шифртекста по описанной выше структуре, включающей объединение двух идеалов [16]:

Так как, исходя из условий системы, значение может быть гораздо больше , то после взятия по модулю злоумышленнику необходимо перебрать весь диапазон возможных случайных значений даже при известном ключе шифрования , что и составляет верхнюю границу стойкости системы.

Расшифровывание сообщения происходит в два этапа. На первом этапе сообщение домножается на секретный ключ , известный лишь участникам системы:

Символом для удобства обозначена локальная единица по модулю . То есть, это некоторое число, не равное единице, но при этом удовлетворяющее соотношению:

Соответственно, для успешного осуществления данного перехода необходимым является выполнение условия:

После взятия по модулю получаем:

На втором этапе результат домножается на величину обратную , но уже по модулю . Существование подобной величины определено условием взаимно простых чисел:

.

И при выполнении условия получаем после взятия модуля расшифрованное сообщение:

1. **Построение общего секретного ключа**

Подход к построению систем шифрования, при котором используются свойства конгруэнтного перехода, позволяет не только выделить шумовую составляющую, но и получить возможность объединения ключей участников системы при гомоморфном шифровании в один общий секретный ключ.

Покажем это на примере системы NTRU [13], схема шифрования которой представляет собой аналогичную схему для конгруэнтного шифрования за исключением использования усеченных полиноминальных колец вида (при вычислении используются, соответственно, вектора размерности ) вместо целых чисел. Это повышает эффективность в вычислительном плане, так при использовании циклотомического (кругового) полинома групповая операция умножения преобразуется в операцию свертки, которая реализуется существенно более быстрым алгоритмом.

Отличительной особенностью рассматриваемых систем является то, что структура шифртекста поддерживает гомоморфную алгебру без дополнительных конструкций [15].

Перейдем непосредственно к системе шифрования по аналогии с рассматриваемой выше конгруэнтной системой шифрования. Вычисление ключей шифрования и построение шифртекста теперь происходит непосредственно для двух участников системы, которых обозначим с помощью индексов и :

При сложении и умножении шифртекст сохраняет свою структуру. Далее рассматривается случай для сложения:

Для расшифрования необходимы секреты и , на основе которых можно построить общий секретный ключ:

Далее, домножая результат сложения на общий секретный ключ, получаем возможность выделения шумовой составляющей за счет конгруэнтного перехода:

При условии, что:

,

после взятия по модулю получаем промежуточное значение:

Для расшифрования необходима величина обратная значению общего секретного ключа:

Далее, при выполнении условия получаем расшифрованное сообщение:

Аналогичные построения можно выполнить и для операции умножения:

Кроме этого, построение можно обобщить на произвольное выражение с оператором для групповой операции, получив следующую закономерность для известного числа операций :

Отличия будут заключаться в различных условиях для корректности расшифрования под модулем и соответственно. Условием полностью гомоморфного шифрования будет наличие операции F с понижением уровня шума, при которой нарушается свойство ассоциативности в пространстве решетки :

Для оценки практической значимости шифрования на идеалах приведем сравнение для систем шифрования RSA, являющейся полностью гомоморфной относительно операции умножения, и NTRU, рассмотренной выше. В [17] приводится следующий анализ для ассиметричных систем:

|  |  |  |  |
| --- | --- | --- | --- |
| Стойкость | Размер открытого ключа (длина в битах) | | |
| NTRU | ECC | RSA |
|  | 2008 | 160 | 1024 |
|  | 3033 | 224 | 2048 |
|  | 3501 | 256 | 3072 |
|  | 4383 | 320 | 4096 |
|  | 5193 | 384 | 7680 |
|  | 7690 | 521 | 15360 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Система | Стойкость  (MIPS-год) | Размер открытого ключа (биты) | Время создания ключа (мс) | Шифрование  (блок/сек) | Расшифрование  (блок/сек) |
| RSA 512 |  | 512 | 260 | 2441 | 122 |
| NTRU 167 |  | 1169 | 4.0 | 5941 | 2812 |
| RSA 1024 |  | 1024 | 1280 | 932 | 22 |
| NTRU 263 |  | 1841 | 7.5 | 3676 | 1619 |
| RSA 2048 |  | 2048 | 4195 | 310 | 3 |
| RSA 4096 |  | 4096 | - | - | - |
| NTRU 503 |  | 4024 | 17.3 | 1471 | 608 |

Как можно заметить в сравнении, NTRU неоднозначно можно сравнить с RSA по необходимому объему данных: для коротких ключей NTRU значительно уступает RSA и выигрывает при относительно большой длине ключа. Однако по производительности NTRU существенно выигрывает RSA, так как требование к вычислительным ресурсам растет линейно по отношению к длине ключа. Тем не менее, методы атаки на системы, использующие решетки, и стойкость систем изучены в значительно меньшей степени, чем для систем использующих факторизацию целых чисел. На данный момент в академическом сообществе существуют дискуссии на этот счет, и для сегодняшнего состояния вычислительных средств принято считать эквивалентную стойкость перебора достаточной и NTRU способна ее обеспечить при лучших скоростях создания ключа, шифрования и расшифрования, чем RSA.

**Заключение**

В данной статье рассмотрены конгруэнтные системы шифрования, построенные с использованием решёток идеалов, показано, что использование идеалов позволяет создать вложенную структуру шифртекста, где для каждого уровня соблюдаются определенные общие закономерности.

Особенностью таких систем является то, что структура шифртекста поддерживает гомоморфную алгебру без дополнительных конструкций, и в схеме их работы можно выделить конгруэнтный переход, который позволяет реализовать однонаправленную функцию. Однако это же приводит к увеличению вероятности ошибки при дешифровании, что обусловлено шумовой составляющей при формировании шифртекста. Накопление шума происходит после каждой групповой операции с идеалами в пространстве шифртекста. В работе прослеживается вложенная структура шума, что может быть использовано при разработке схемы понижения шума.

Выделение значащих частей происходит с использованием конгруэнтного перехода. Этот способ позволяет построить общий секретный ключ, скрывающий часть информации об участниках системы шифрования. Встречной задачей выступает выбор параметров системы для поддержки допустимого количества операций.

Практическая значимость гомоморфного шифрования заключается в возможности делегировать алгоритм вычислений третьей стороне, не разглашая структуру самого алгоритма. К сожалению, в современных схемах полностью гомоморфного шифрования наличие шифрования, происходящее после выполнения каждой групповой операции, ведет к полиноминальному снижению производительности в зависимости от длины цепочки вычислений. При этом на практике реализация таких алгоритмов требует их низкоуровневого представления в виде булевых функций, что также может приводить к чрезвычайно большим арифметическим схемам.

В качестве дальнейшего направления исследований можно предложить реализацию качественно других арифметических схем, представленный в данной работе метод конгруэнтного перехода может найти широкое применение на практике.

СПИСОК ЛИТЕРАТУРЫ:

1. Rivest R.L., Adleman L., Dertouzos M.L., et al. On data banks and privacy homomorphisms. Foundations of secure computation. Vol. 4, no. 11, 1978. P. 169–180. URL: https://luca-giuzzi.unibs.it/corsi/Support/papers-cryptography/RAD78.pdf (дата обращения: 01.02.2021).
2. Feigenbaum J. Distributed computing and cryptography: proceedings of a DIMACS Workshop, October 4–6, 1989. American Mathematical Soc., 1991. – 262 p.
3. Craig Gentry. 2009. Fully homomorphic encryption using ideal lattices. In Proceedings of the forty-first annual ACM symposium on Theory of computing (STOC '09). Association for Computing Machinery, New York, NY, USA, 169–178. DOI: https://doi.org/10.1145/1536414.1536440.
4. Brakerski Z. and Vaikuntanathan V. Efficient Fully Homomorphic Encryption from (Standard) LWE.   
   IEEE 52nd Annual Symposium on Foundations of Computer Science, 2011. P. 97–106, DOI: https://doi.org/10.1109/FOCS.2011.12.
5. Brakerski Z., Gentry C., Vaikuntanathan V. (Leveled) Fully Homomorphic Encryption without Bootstrapping. ACM Trans. Comput. Theory 6, 3, Article 13. July 2014. – 36 p. DOI: https://doi.org/10.1145/2633600.
6. Brakerski Z., Gentry C., Halevi S. (2013) Packed Ciphertexts in LWE-Based Homomorphic Encryption. In: Kurosawa K., Hanaoka G. (eds) Public-Key Cryptography – PKC 2013. PKC 2013. Lecture Notes in Computer Science. Vol. 7778. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-36362-7\_1.
7. Maurer U., Raub D. Black-box extension fields and the inexistence of field-homomorphic one-way permutations //International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2007. P. 427–443. DOI: https://doi.org/10.1007/978-3-540-76900-2\_26.
8. Boneh D. and Lipton R. Searching for Elements in Black-Box Fields and Applications. In Crypto’ 96, LNCS 1109. P. 283–297. Springer-Verlag, 1996. URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.42.4296 (дата обращения: 01.02.2021).
9. Li J., Nguyen P.Q. A complete analysis of the bkz lattice reduction algorithm. – Cryptology ePrint Archive, Report 2020/1237, 2020. URL: https://eprint.iacr.org/2020/1237 (дата обращения: 01.02.2021).
10. Korkine A., Zolotareff G. Sur les formes quadratiques. Math. Ann. 6, 366–389 (1873).   
    DOI: https://doi.org/10.1007/BF01442795.
11. Бабенко Л.К. и др. Полностью гомоморфное шифрование (обзор) //Вопросы защиты информации. 2015. №. 3. С. 3–26. URL: https://elibrary.ru/item.asp?id=24833959 (дата обращения: 01.02.2021).
12. Silverman J.H., Pipher J., Hoffstein J. An introduction to mathematical cryptography. Springer, New York, NY, 2008. – 524 p. DOI: https://doi.org/10.1007/978-0-387-77993-5.
13. Hoffstein J., Pipher J., Silverman J.H. (1998) NTRU: A ring-based public key cryptosystem. In: Buhler J.P. (eds) Algorithmic Number Theory. ANTS 1998. Lecture Notes in Computer Science. Vol. 1423. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/BFb0054868.
14. Smart N.P. Cryptography: an introduction. New York: McGraw-Hill, 2004. – 433 p. ISBN: 9780077099879.
15. Abbas Acar, Hidayet Aksu, A. Selcuk Uluagac, and Mauro Conti. A Survey on Homomorphic Encryption Schemes: Theory and Implementation. ACM Comput. Surv. 51, 4, Article 79. September,   
    2018. – 35 p. DOI: https://doi.org/10.1145/3214303.
16. Кадыков В.Ю., Левина А.Б. Гомоморфные операции в системах шифрования с применением решеток идеалов // Вестник компьютерных и информационных технологий. 2020. Т. 17. №. 11. С. 40–46.   
    URL. https://www.elibrary.ru/item.asp?id=44421628 (дата обращения: 01.02.2021).
17. Mersin A. The comparative performance analysis of lattice based NTRU cryptosystem with other asymmetrical cryptosystems. İzmir Institute of Technology, Master's thesis, 2007. URL: https://core.ac.uk/download/pdf/324140901.pdf (дата обращения: 01.02.2021).

REFERENCES:

1. Rivest R.L., Adleman L., Dertouzos M.L., et al. On data banks and privacy homomorphisms. Foundations of secure computation. Vol. 4, no. 11, 1978. P. 169–180. URL: https://luca-giuzzi.unibs.it/corsi/Support/papers-cryptography/RAD78.pdf (accessed: 01.02.2021).
2. Feigenbaum J. Distributed computing and cryptography: proceedings of a DIMACS Workshop, October 4-6, 1989. American Mathematical Soc., 1991. – 262 p.
3. Craig Gentry. 2009. Fully homomorphic encryption using ideal lattices. In Proceedings of the forty-first annual ACM symposium on Theory of computing (STOC '09). Association for Computing Machinery, New York, NY, USA, 169–178. DOI: https://doi.org/10.1145/1536414.1536440.
4. Brakerski Z. and Vaikuntanathan V. Efficient Fully Homomorphic Encryption from (Standard) LWE.   
   IEEE 52nd Annual Symposium on Foundations of Computer Science, 2011. P. 97–106, DOI: https://doi.org/10.1109/FOCS.2011.12.
5. Brakerski Z., Gentry C., Vaikuntanathan V. (Leveled) Fully Homomorphic Encryption without Bootstrapping. ACM Trans. Comput. Theory 6, 3, Article 13. July 2014. – 36 p. DOI: https://doi.org/10.1145/2633600.
6. Brakerski Z., Gentry C., Halevi S. (2013) Packed Ciphertexts in LWE-Based Homomorphic Encryption. In: Kurosawa K., Hanaoka G. (eds) Public-Key Cryptography – PKC 2013. PKC 2013. Lecture Notes in Computer Science. Vol. 7778. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-36362-7\_1.
7. Maurer U., Raub D. Black-box extension ﬁelds and the inexistence of field-homomorphic one-way permutations. International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2007. P. 427–443. DOI:  https://doi.org/10.1007/978-3-540-76900-2\_26.
8. Boneh D. and Lipton R. Searching for Elements in Black-Box Fields and Applications. In Crypto’ 96, LNCS 1109. P. 283–297. Springer-Verlag, 1996. URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.42.4296 (дата обращения: 01.02.2021) (accessed: 01.02.2021).
9. Li J., Nguyen P.Q. A complete analysis of the BKZ lattice reduction algorithm, tech. rep. Cryptology ePrint Archive, Report 2020/1237, 2020. URL: https://eprint.iacr.org/2020/1237 (accessed: 01.02.2021)
10. Korkine, A., Zolotareff G. Sur les formes quadratiques. Math. Ann. 6, 366–389 (1873).   
    DOI: https://doi.org/10.1007/BF01442795.
11. Babenko L.K. u dr. Polnost'ju gomomorfnoe shifrovanie (obzor) [Fully Homomorphic Encryption (review)], Information security questions (ISQ), 2015, no. 3. P. 3–26. URL: https://elibrary.ru/item.asp?id=24833959 (accessed: 01.02.2021) (in Russian).
12. Silverman J.H., Pipher J., Hoffstein J. An introduction to mathematical cryptography. Springer, New York, NY, 2008. – 524 p. DOI: https://doi.org/10.1007/978-0-387-77993-5.
13. Hoffstein J., Pipher J., Silverman J.H. (1998) NTRU: A ring-based public key cryptosystem. In: Buhler J.P. (eds) Algorithmic Number Theory. ANTS 1998. Lecture Notes in Computer Science. Vol. 1423. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/BFb0054868.
14. Smart N.P. Cryptography: an introduction. New York: McGraw-Hill, 2004. – 433 p. ISBN: 9780077099879.
15. Abbas Acar, Hidayet Aksu, A. Selcuk Uluagac, and Mauro Conti. A Survey on Homomorphic Encryption Schemes: Theory and Implementation. ACM Comput. Surv. 51, 4, Article 79. September,   
    2018. – 35 p. DOI: https://doi.org/10.1145/3214303.
16. Kadykov V.Yu., Levina A.B. (2020). Homomorphic Operations in Encryption Systems Using Ideal Lattices. Vestnik komp'yuternyh i informatsionnyh tekhnologiy. Vol. 17, no. 11. P. 40–46.   
    URL. https://www.elibrary.ru/item.asp?id=44421628 (accessed: 01.02.2021) (in Russian).
17. Mersin A. The comparative performance analysis of lattice based NTRU cryptosystem with other asymmetrical cryptosystems. İzmir Institute of Technology, Master's thesis, 2007. URL: https://core.ac.uk/download/pdf/324140901.pdf (accessed: 01.02.2021).

*Поступила в редакцию – 10 апреля 2021 г. Окончательный вариант – 23 мая 2021 г.*

*Received – April 10, 2021. The final version – May 23, 2021.*