Раздел IV. Информационная безопасность

УДК 004.422 DOI 10.18522/2311-3103-2020-4-212-221

Л.К. Бабенко, И.Д. Русаловский

МЕТОД РЕАЛИЗАЦИИ ГОМОМОРФНОГО ДЕЛЕНИЯ*

Рассматриваются проблемы гомоморфной криптографии. Гомоморфная криптография – одно из молодых направлений криптографии. Его особенность заключается в том, что можно обрабатывать зашифрованные данные без их предварительной расшифровки таким образом, что результат операций над зашифрованными данными эквивалентен после расшифровки результату операции над открытыми данными. В статье приводится краткий обзор областей применения гомоморфного шифрования. Для решения различных прикладных задач требуется поддержка всех математических операций, в том числе и операции деления, а возможность выполнить эту операцию гомоморфно позволит расшить возможности применения гомоморфного шифрования. В работе предлагается метод гомоморфного деления, основанный на абстрактном представлении шифротекста в виде обыкновенной дроби. В работе подробно описывается предложенный метод. Кроме этого статья содержит пример практической реализации предложенного метода. Предлагается разделить уровни обработки данных на 2 уровня – криптографический и математический. На криптографическом уровне используется некоторый полностью гомоморфный алгоритм шифрования и выполняются базовые гомоморфные математические операции – сложение, умножение и разность. Математический уровень является надстройкой над криптографическим и расширяет его возможности. На математическом уровне шифротекст представляется в виде простой дроби и появляется возможность выполнения операции гомоморфного деления. Также в работе приводится практический пример применения метода гомоморфного деления на базе алгоритма Джентри для целых чисел. Приводятся выводы и возможные пути дальнейшего развития.

Гомоморфное шифрование; криптографическая защита; методы и алгоритмы; гомоморфное деление.

L.K. Babenko, I.D. Rusalovsky

METHOD OF IMPLEMENTING HOMOMORPHIC DIVISION

The article deals with the problems of homomorphic cryptography. Homomorphic cryptography is one of the young directions of cryptography. Its peculiarity lies in the fact that it is possible to process encrypted data without preliminary decryption in such a way that the result of operations on encrypted data is equivalent, after decryption, to the result of operations on open data. The article provides a brief overview of the areas of application of homomorphic encryption. To solve various applied problems, support for all mathematical operations is required, including the division operation, and the ability to perform this operation homomorphically will expand the possibilities of using homomorphic encryption. The paper proposes a method of homomorphic division based on an abstract representation of the ciphertext in the form of an ordinary fraction. The paper describes in detail the proposed method. In addition, the article contains an example of the practical implementation of the proposed method. It is proposed to divide the levels of data processing into 2 levels – cryptographic and mathematical. At the cryptographic level, a complete-

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-37-90140.

ly homomorphic encryption algorithm is used and the basic homomorphic mathematical operations are performed – addition, multiplication and difference. The mathematical level is a superstructure on top of the cryptographic level and expands its capabilities. At the mathematical level, the ciphertext is represented as a simple fraction and it becomes possible to perform the homomorphic division operation. The paper also provides a practical example of applying the homomorphic division method based on the Gentry algorithm for integers. Conclusions and possible ways of further development are given.

Homomorphic encryption; cryptographic protection; methods and algorithms; homomorphic division.

Введение. Процессы информатизации и глобализации оказали значительное значение на все сферы жизни. Информационные технологии стали частью современной жизни. Человечество повсеместно пользуется благами информатизации: персональные компьютеры, удаленные сервисы, онлайн банки и покупки, интернет вещей и многое другое. Трудно представить жизнь современного человека без компьютера и глобальной сети интернет. В результате процесса информатизации вырос объем информации, возросли информационные потоки. В условиях бурного роста информационных технологий как никогда ранее стала актуальна проблема обеспечения информационной безопасности, в частности, проблема обеспечения криптографической защиты.

Криптография позволяет сохранять данные в секрете, обеспечивая их безопасную передачу. В настоящее время получило развитие новое направление – гомоморфная криптография. Его отличительной особенностью является то, что появилась возможность обрабатывать зашифрованные данные без их предварительной расшифровки таким образом, что результат операций над зашифрованными данными эквивалентен после расшифровки результату операции над открытыми данными. При этом решается одна из важных проблем криптографии, связанная с решением вопросов генерации, хранения и распространения (распределения) общих сеансовых ключей. В результате применения гомоморфного шифрования повышается уровень защищенности данных – сервер получает зашифрованные данные, обрабатывает их и возвращает зашифрованный результат, а открытые данные и ключи шифрования не покидают безопасный сегмент при сетевом взаимодействии.

Гомоморфное шифрование имеет существенные преимущества, однако и не лишено на данный момент недостатков. Основными из них являются:

- необходимость обеспечения целостности пересылаемых данных;
- высокая трудоемкость операций над зашифрованными данными;
- быстрый рост коэффициентов после выполнения операций над данными.

Первая и последняя из перечисленных проблем легко решаются. Для обеспечения целостности можно воспользоваться различными криптографическими протоколами, а чтобы избежать быстрого роста коэффициентов, можно использовать схемы с коррекцией размеров шифротекстов после выполнения операций над ними (технология бутстрэппинга, о которой будет подробно рассказано в другой статье).

На данный момент существует большое количество алгоритмов полностью гомоморфного шифрования, основанных на различных принципах. Для ряда из них выполнены практические реализации, которые находятся в общем доступе, есть и коммерческие продукты. Однако ни в одной из найденных во время анализа реализаций не было поддержки операции деления. Таким образом, актуальным является разработка метода, позволяющего расширить существующие гомоморфные алгоритмы функциональностью деления. Разработке такого метода посвящена данная статья.

Теоретические основы. Идея полностью гомоморфного шифрования была предложена изобретателями алгоритма шифрования RSA Рональдом Ривестом, Леонардом Адлеманом в соавторстве с Майклом Дертузосом в 1978 году [1]. Они выдвинули предположение, что возможно выполнение произвольных опера-

ций над зашифрованными данными без необходимости их предварительной расшифровки. В то время все попытки разработки полностью гомоморфной схемы не привели к успеху. Все криптосистемы, которые были разработаны в последующие годы, были лишь частично гомоморфными.

Лишь в начале 2000-ых годов стали появляться криптосистемы, которые выходили за рамки частичного гомоморфизма. Большой прорыв в исследовании гомоморфного шифрования сделан в 2009 году, когда Крейг Джентри, воспользовавшись криптографией на решетках, впервые представил вариант полностью гомоморфной схемы шифрования [2]. Следом за этим было опубликовано немало работ, предлагающих модификации криптосистемы Джентри, вносящих в нее улучшения и повышающие ее быстродействие. Вместе с этим активно идет работа над созданием альтернативных симметричных гомоморфных криптосистем на основе полиномов от одной, нескольких переменных и матричных полиномов.

Гомоморфное шифрование – это такая форма шифрования, которая позволяет проводить некоторые математические операции над зашифрованными данными и получать зашифрованный результат, который будет соответствовать результату операций, выполняемых над открытыми данными [3–6].

Различают два вида гомоморфного шифрования – частично и полностью гомоморфное. Криптосистема считается частично гомоморфной, если она является гомоморфной относительно умножения или сложения. Полностью гомоморфная схема гомоморфна одновременно относительно двух математических операций – сложения и умножения.

Гомоморфное шифрование – достаточно молодое направление. Его развитие и совершенствование актуально [7–18] и позволит использовать его в таких сферах как:

- Облачные вычисления.
- Облачная обработка фотографий.
- Электронные голосование (выборы).
- Защищенный поиск информации.

Анализ актуальности. Гомоморфное шифрование не так давно получило свое начальное развитие, но уже является довольно известным. Разрабатываются новые алгоритмы шифрования и совершенствуются старые, создаются библиотеки для гомоморфной обработки данных. На данный момент уже выполнено несколько реализаций библиотек для гомоморфного шифрования [19–20]. Наиболее серьезными реализациями, доступными для общего пользования, можно считать две:

- библиотека HElib, созданная Шаем Хавели и Виктор Шоуп, которая реализует криптосистему BGV с GHS оптимизацией;
- библиотека FHEW созданная Лео Дуглас и Даниэль Миккианакио, которая является реализацией комбинации криптосистемы обучения с ошибками Регева и техники создания гибкой схемы Алперин-Шериффа и Пейкерта.

Библиотеки имеют высокую скорость работы, хорошую оптимизацию. Но, проанализировав области применения гомоморфного шифрования, можно сделать вывод о необходимости выполнения операций над целыми числами, включая операцию деления. В результате поиска в открытых источниках не было найдено информации о возможной реализации метода или алгоритма гомоморфного деления. В данной статье будет рассмотрен вопрос гомоморфного деления, предложен метод и примеры его использования.

Метод гомоморфного деления. Существующие схемы и алгоритмы гомоморфного шифрования не позволяют использовать операцию деления над зашифрованными данными. Для решения данной проблемы предлагается использовать некую абстракцию, построенную над шифротекстом и расширяющую возможно-

сти по выполнению математических операций над ним. Для этого необходимо выделить два уровня представления данных – криптографический и математический. На рис. 1 приведен пример взаимодействия двух уровней и пользователя. Пунктиром выделена часть схемы, которая может иметь различные варианты реализации. Возможность замены реализации криптографического уровня может быть достигнута за счет единства интерфейса.

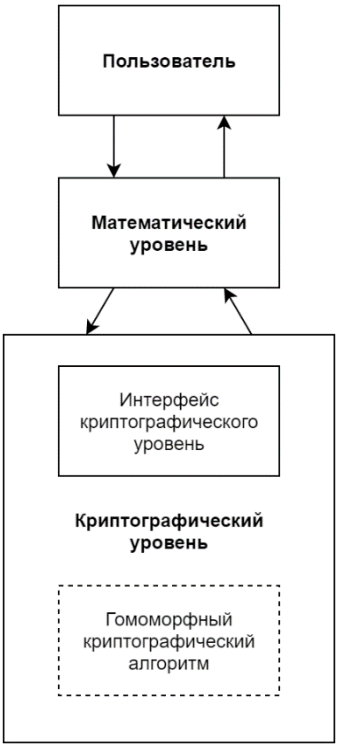

Рис. 1. Уровни представления данных и их взаимосвязь

Криптографическое ядро предложенной выше схемы может быть представлено абсолютно любым полностью гомоморфным алгоритмом шифрования. При этом алгоритм может быть и симметричным и ассиметричным. Конечный же пользователь данной схемы будет взаимодействовать только с математическим уровнем, интерфейс которого будет неизменен, какой бы гомоморфный алгоритм шифрования не был бы выбран.

Криптографический уровень представляет собой модуль, основным типом данных которого является зашифрованное гомоморфно число. На данном уровне должны быть реализованы возможности по созданию новых шифротекстов на базе открытых текстов и ключей шифрования (операция шифрования данных), получению открытых данных из шифротекста на основании ключа расшифрования (операция расшифрования данных), а также основные математические операции над шифротекстами – сложение, разность и умножение. Подобный функционал позволит реализовать любой полностью гомоморфный алгоритм, работающий с целыми числами. Криптографический уровень принимает запросы от математического, гомоморфно обрабатывает данные и возвращает результат обратно (на математический слой схемы). Пользователь не имеет доступа к криптографическому уровню напрямую, а взаимодействует только с математическим уровнем.

Математический уровень является надстройкой над криптографическим. Данный уровень необходим, чтобы обеспечить поддержку операции деления. Для этого на данном уровне данные будут содержаться в виде простой дроби, числителем и знаменателем которой являются экземпляры объектов криптографического уровня. Математический уровень является прослойкой между пользователем и криптографическим ядром. Все действия на математическом уровне выполняются как операции над простыми дробями, числитель и знаменатель которых поддерживают операции сложения, разности и умножения так, как представлены объектами криптографического уровня. К примеру, когда выполняется операция умножения двух объектов математического уровня, выполняются два запроса к криптографическому уровня для перемножения числителей (делимое – $\boldsymbol{dividend}$) и знаменателей (делитель – $\boldsymbol{divider}$) этих чисел соответственно, а в результате будет получена результирующая дробь:

$$A * B = \left\{ \begin{matrix} \boldsymbol{C.dividend} = \text{A.}\boldsymbol{dividend} * \text{ B.}\boldsymbol{dividend} \\ \boldsymbol{C.divider} = \text{A.}\boldsymbol{divider} * \text{ B.}\boldsymbol{divider} \end{matrix} \right\} = C$$

Реализация операций математического уровня будет подробней описана далее. Предложенный выше метод гомоморфного деления обладает явными плюсами – решение является гибким, так как позволяет реализовать гомоморфное деление на базе любого частично гомоморфного алгоритма шифрования. Вторым плюсом метода можно считать простоту реализации. Однако имеются и негативные стороны. Главным минусом метода является рост объема шифротекста в два раза, что является следствием использования простой дроби. При условии использования полностью гомоморфных алгоритмов, увеличение объема шифротекста практически не будет иметь негативного влияния на процесс шифрования и передачи данных.

Пример практической реализации. Приведем ниже пример реализации предложенного алгоритма в виде псевдокода. Для реализации необходимо будет создать два класса – базовый, который будет реализовать всю криптографическую функциональность и надстройку над ним, реализующую математическую функциональность. Базовый класс будет иметь наименование EncryptedData, математического – EncryptedFraction. Ниже приведена более подробная информация по каждому из уровней.

Криптографический уровень. Класс, определяющий основной тип данных криптографического уровня, содержит в себе функционал, позволяющий генерировать ключи шифрования, выполнять операции шифрования и расшифрования а также основные математические операции над зашифрованными гомоморфно числами – сложение, разность и умножение. Данный уровень может быть реализован любым аддитивным и мультипликативным гомоморфным алгоритмом. Использование же полностью гомоморфного алгоритма позволит сдерживать уровень шума и, следовательно, ограничивать объем шифротекстов. Подробнее природа и рост шума в гомоморфных алгоритмах будут рассмотрены отдельно. Интерфейс криптографического уровня представлен на рис. 2.

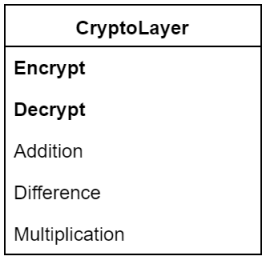

Рис. 2. Интерфейс класса криптографического уровня

Математический уровень. Данный уровень является надстройкой над криптографическим. В своей реализации он представляет собой обыкновенную дробь, в числителе и знаменателе которой объекты криптографического уровня – зашифрованные гомоморфно числа. Благодаря использованию простой дроби в математическом уровня стала возможна реализация деления с использованием только операции гомоморфного умножения. Выполнение всех математических операций на данном уровне – это выполнение операций над простыми дробями, используя гомоморфные операции сложения, разности и умножения криптографического уровня. Архитектура (интерфейс) класса представлена на рис. 3.

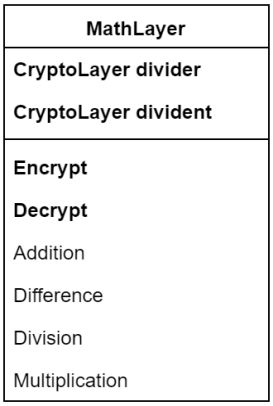

Рис. 3. Интерфейс класса математического уровня

Пример использования метода. Предложенный метод предполагает взаимодействие с математическим уровнем. Объект математического уровня содержит внутри себя делимое и делитель – объекты криптографического уровня. Во время выполнения операций над объектами математического уровня вызываются соответствующие операции над делимым и делителем – объектами криптографического уровня. Все операции выполняются как операции над обычными дробями – приведение к общему знаменателю и операции над числителями для сложения и разности, перемножение числителей и знаменателей между собой соответственно для умножения и умножение числителя первого на знаменатель второго и знаменателя первого на числитель второго для деления.

Пусть A, B – объекты математического уровня, тогда операции над ними будут реализованы следующим образом:

Сложение и разность:

$$\boldsymbol{A} \pm \boldsymbol{B} = \left\{ \begin{matrix} \boldsymbol{C.dividend} = \boldsymbol{A.dividend} * \boldsymbol{B.divider} \pm \boldsymbol{B.dividend} * \boldsymbol{A.divider} \\ \boldsymbol{C.divider} = \boldsymbol{A.divider} * \boldsymbol{B.divider} \end{matrix} \right\} = C$$

Умножение:

$$A * B = \left\{ \begin{matrix} \boldsymbol{C.dividend} = A.\boldsymbol{dividend} * B.\boldsymbol{dividend} \\ \boldsymbol{C.divider} = A.\boldsymbol{divider} * B.\boldsymbol{divider} \end{matrix} \right\} = C$$

Деление:

$$\mathrm{A} \div \mathrm{B} = \left\{ \begin{matrix} \boldsymbol{C.dividend} = \mathrm{A.dividend} * \mathrm{B.divider} \\ \boldsymbol{C.divider} = \mathrm{A.divider} * \mathrm{B.dividend} \end{matrix} \right\} = C$$

Пример с численными значениями. В рамках данного примера в качестве алгоритма шифрования будет использован алгоритм гомоморфного шифрования целых чисел, предложенный Джентри [21–22]. Схема шифрования в предложенном алгоритме имеет вид:

$$C = P * r + s * e + m,$$

где P – секретный ключ, r – небольшая случайная константа, s – пространство открытого текста, e – небольшая случайна величина (ошибка).

Схема расшифрования может быть описана как:

$$m = (C \bmod P) \bmod s.$$

Пусть параметры схемы шифрования P = 997, r = 5, s = 11, e = 2. Тогда вычислим объекты A, B математического уровня для исходных текстов a = 4, b = 2:

$$C1 = P * r + s * e + a = 997 * 5 + 11 * 2 + 4 = 5011$$

$$C2 = P * r + s * e + a = 997 * 5 + 11 * 2 + 2 = 5009$$

$$\boldsymbol{A} = \left\{ \begin{matrix} \boldsymbol{A.dividend} = 5011 \\ \boldsymbol{A.divider} = \boldsymbol{1} \end{matrix} \right\}$$

$$\boldsymbol{B} = \left\{ \begin{matrix} \boldsymbol{B.dividend} = 5009 \\ \boldsymbol{B.divider} = \boldsymbol{1} \end{matrix} \right\}.$$

Сложение:

$$\boldsymbol{C} = \boldsymbol{A} + \boldsymbol{B} = \left\{ \begin{matrix} \boldsymbol{C.dividend} = \boldsymbol{5011} * \boldsymbol{1} + 5009 * \boldsymbol{1} \\ \boldsymbol{C.divider} = \boldsymbol{1} * \boldsymbol{1} \end{matrix} \right\}$$

$$C = \left\{ \begin{matrix} C.\boldsymbol{dividend} = \boldsymbol{10020} \\ C.\boldsymbol{divider} = \boldsymbol{1} \end{matrix} \right\}$$

$$m = (\boldsymbol{10020}\ mod\ 997)\ mod\ 11\ /\ (1\ mod\ 997)\ mod\ 11 = 6\ /\ 1 = 6.$$

Разность:

$$\boldsymbol{C} = \boldsymbol{A} - \boldsymbol{B} = \left\{ \begin{matrix} \boldsymbol{C.dividend} = \boldsymbol{5011} * \boldsymbol{1} - 5009 * \boldsymbol{1} \\ \boldsymbol{C.divider} = \boldsymbol{1} * \boldsymbol{1} \end{matrix} \right\}$$

$$C = \left\{ \begin{matrix} C.\boldsymbol{dividend} = \boldsymbol{2} \\ C.\boldsymbol{divider} = \boldsymbol{1} \end{matrix} \right\}$$

$$m = (\boldsymbol{2}\ mod\ 997)\ mod\ 53\ /\ (1\ mod\ 997)\ mod\ 53 = 2\ /\ 1 = 2$$

Умножение:

$$\boldsymbol{C} = \boldsymbol{A} * \boldsymbol{B} = \left\{ \begin{matrix} \boldsymbol{C.dividend} = \boldsymbol{5011} * \boldsymbol{5009} \\ \boldsymbol{C.divider} = \boldsymbol{1} * \boldsymbol{1} \end{matrix} \right\}$$

$$C = \left\{ \begin{matrix} C.\boldsymbol{dividend} = \boldsymbol{25\ 100\ 099} \\ C.\boldsymbol{divider} = \boldsymbol{1} \end{matrix} \right\}$$

$$m = (\boldsymbol{25\ 100\ 099}\ mod\ 997)\ mod\ 53\ /\ (1\ mod\ 997)\ mod\ 53 = 8\ /\ 1 = 8$$

Деление:

$$\boldsymbol{C} = \boldsymbol{A} \div \boldsymbol{B} = \left\{ \begin{matrix} \boldsymbol{C.dividend} = \boldsymbol{5011} * \boldsymbol{1} \\ \boldsymbol{C.divider} = \boldsymbol{1} * \boldsymbol{5009} \end{matrix} \right\}$$

$$C = \left\{ \begin{matrix} C.\boldsymbol{dividend} = \boldsymbol{5011} \\ C.\boldsymbol{divider} = \boldsymbol{5009} \end{matrix} \right\}$$

$$m = (\boldsymbol{5011}\ mod\ 997)\ mod\ 53\ /\ (\boldsymbol{5009}\ mod\ 997)\ mod\ 53 = 4\ /\ 2 = 2.$$

Заключение. В рамках данной статьи рассмотрена проблема гомоморфного деления целых чисел, предложен и описан метод реализации гомоморфного деления и приведены практические примеры применения вышеописанного метода. Практическая ценность работы состоит в решении одной из проблем гомоморфного шифрования – реализация гомоморфного деления позволяет расширить область практического применения гомоморфного шифрования в таких областях, как облачные вычисления, решение задач защиты информации, машинное обучение.

Предложенный в работе метод гомоморфного деления обладает рядом недостатков:

- Требует использования в криптографическом ядре алгоритмов полностью гомоморфного шифрования, удовлетворяющих критериям Джентри.
- Независимо от используемого алгоритма шифрования объем шифротекстов увеличивается вдвое.

В перспективе планируется работать над улучшением предложенного метода и продолжать поиск лучшего решения для реализации гомоморфного деления. Также предполагается практическая реализация предложенного метода.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Rivest R.L., Adleman L., Dertouzos M.L.* On data banks and privacy homomorphisms // Foundations of secure computation. – 1978. – Vol. 32, No. 4. – P. 169-178.
2. *Gentry C.* A fully homomorphic encryption scheme // A dissertation submitted to the department of computer science and the committee on graduate students of Standford University. – 2009.
3. *Diffie W. and Hellman M.* New directions in cryptography // IEEE Transactions on Information Theory. – 1976. – Vol. IT-22. – P. 644-654.
4. *Gentry C.* Fully homomorphic encryption using ideal lattices // STOC. – 2009. – P. 169-178.
5. *Rivest R., Adleman L., Dertouzos M.* On data banks and privacy homomorphisms // Foundations of Secure Computation. Academic Press. – 1978. – P. 169-177.
6. *Goldwasser S., Micali S.* Probabilistic encryption // Journal of Computer and System Sciences. – 1984. – Vol. 28, No. 2. – P. 270-299.
7. *Бабенко Л.К., Буртыка Ф.Б., Макаревич О.Б., Трепачева А.В.* Методы полностью гомоморфного шифрования на основе матричных полиномов // Вопросы кибербезопасности, – 2015. – № 1. – С. 17-20.
8. *Бабенко Л.К., Буртыка Ф.Б., Макаревич О.Б., Трепачева А.В.* Полностью гомоморфное шифрование (обзор) // Вопросы защиты информации. – 2015. – № 3. – С. 3-26.
9. *Бабенко Л.К., Буртыка Ф.Б., Макаревич О.Б., Трепачева А.В.* Защищенные вычисления и гомоморфное шифрование // Программные системы: теория и приложения. – 2014. – 25 с.
10. *Макаревич О.Б., Буртыка Ф.Б.* Защищенная облачная база данных с применением гомоморфной криптографии // Тез. докл. 6-й Росс. мультиконференции «Информационные технологии в управлении» (ИТУ–2014). – СПб., 2014. – С. 567-572.
11. *Буртыка Ф.Б.* Пакетное симметричное полностью гомоморфное шифрование на основе матричных полиномов // Тр. Института системного программирования РАН. – 2014. – Т. 26, № -5. – С. 99-116.
12. *Буртыка Ф.Б.* Симметричное полностью гомоморфное шифрование с использованием неприводимых матричных полиномов // Известия ЮФУ. Технические науки. – 2014. – № 8 (157). – С. 107-122.
13. *Трепачева А.В.* Криптоанализ симметричных полностью гомоморфных линейных криптосистем на основе задачи факторизации чисел // Известия ЮФУ. Технические науки. – 2015. – № 5 (166). – С. 89-102.
14. *Brakerski Vaikuntanathan.* Efficient fully homomorphic encryption from (standard) LWE // FOCS. – 2011.
15. *Rao G.V., Kakulapati V., Purushoththaman M.* Privacy homomorphism in mobile ad hoc networks // International Journal of Research & Reviews in Computer Science. – 2011.
16. *Жиров А.О., Жирова А.О., Кренделев С.Ф.* Безопасные облачные вычисления с помощью гомоморфной криптографии // Безопасность информационных технологий. – 2013. – №. 1. – С. 6-12.
17. *Regev O.* New lattice-based cryptographic constructions // J. ACM. – 2004. – Vol. 51, No. 6. – P. 899-942.
18. *Regev O.* On lattices, learning with errors, random linear codes, and cryptography // STOC. – 2005. – P. 84-93.
19. Helib. – URL: https://github.com/homenc/HElib (дата обращения: 01.06.2020).
20. FHEW. – URL: https://github.com/lducas/FHEW (дата обращения: 01.06.2020).

21. *Gentry C., Halevi S.* Implementing gentry's fully-homomorphic encryption scheme // EUROCRYPT, ser. Lecture Notes in Computer Science, K. G. Paterson, Ed. – Vol. 6632. – Springer, 2011. – P. 129-148.
22. *Dijk M., Gentry C., Halevi S., Vaikuntanathan V.* Fully Homomorphic Encryption over the Integers // Eurocrypt. – 2010.

REFERENCES

1. *Rivest R.L., Adleman L., Dertouzos M.L.* On data banks and privacy homomorphisms, *Foundations of secure computation,* 1978, Vol. 32, No. 4, pp. 169-178.
2. *Gentry C.* A fully homomorphic encryption scheme, *A dissertation submitted to the department of computer science and the committee on graduate students of Standford University,* 2009.
3. *Diffie W. and Hellman M.* New directions in cryptography, I*EEE Transactions on Information Theory,* 1976, Vol. IT-22, pp. 644-654.
4. *Gentry C.* Fully homomorphic encryption using ideal lattices, *STOC,* 2009, pp. 169-178.
5. *Rivest R., Adleman L., Dertouzos M.* On data banks and privacy homomorphisms, *Foundations of Secure Computation. Academic Press*, 1978, pp. 169-177.
6. *Goldwasser S., Micali S.* Probabilistic encryption, *Journal of Computer and System Sciences,* 1984, Vol. 28, No. 2, pp. 270-299.
7. *Babenko L.K., Burtyka F.B., Makarevich O.B., Trepacheva A.V.* Metody polnost'yu gomomorfnogo shifrovaniya na osnove matrichnykh polinomov [Methods of fully homomorphic encryption based on matrix polynomials], *Voprosy kiberbezopasnosti* [Cybersecurity issues], 2015, No. 1, pp. 17-20.
8. *Babenko L.K., Burtyka F.B., Makarevich O.B., Trepacheva A.V.* Polnost'yu gomomorfnoe shifrovanie (obzor) [Fully Homomorphic Encryption (Overview)], *Voprosy zashchity informatsii* [Information Security Issues], 2015, No. 3, pp. 3-26.
9. *Babenko L.K., Burtyka F.B., Makarevich O.B., Trepacheva A.V.* Zashchishchennye vychisleniya i gomomorfnoe shifrovanie [Secure computing and homomorphic encryption], *Programmnye sistemy: teoriya i prilozheniya* [Software systems: theory and applications], 2014, 25 p.
10. *Makarevich O.B., Burtyka F.B.* Zashchishchennaya oblachnaya baza dannykh s primeneniem gomomorfnoy kriptografii [Secure cloud database using homomorphic cryptography], *Tez. dokl. 6-y Ross. mul'tikonferentsii «Informatsionnye tekhnologii v upravlenii» (ITU–2014)* [Proceedings of 6th Russian multiconference «Information Technologies in Control» (ITU-2014). Saint Petersburg, 2014, pp. 567-572.
11. *Burtyka F.B.* Paketnoe simmetrichnoe polnost'yu gomomorfnoe shifrovanie na osnove matrichnykh polinomov [Batch symmetric fully homomorphic encryption based on matrix polynomials], *Tr. Instituta sistemnogo programmirovaniya RAN* [Proceedings of the Institute for System Programming RAS], 2014, Vol. 26, No. 5, pp. 99-116.
12. *Burtyka F.B.* Simmetrichnoe polnost'yu gomomorfnoe shifrovanie s ispol'zovaniem neprivodimykh matrichnykh polinomov [Symmetric fully homomorphic encryption using irreducible matrix polynomials], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2014, No. 8 (157), pp. 107-122.
13. *Trepacheva A.V.* Kriptoanaliz simmetrichnykh polnost'yu gomomorfnykh lineynykh kriptosistem na osnove zadachi faktorizatsii chisel [Cryptanalysis of symmetric fully homomorphic linear cryptosystems based on the number factorization problem], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2015, No. 5 (166), pp. 89-102.
14. *Brakerski Vaikuntanathan.* Efficient fully homomorphic encryption from (standard) LWE, *FOCS,* 2011.
15. *Rao G.V., Kakulapati V., Purushoththaman M.* Privacy homomorphism in mobile ad hoc networks, *International Journal of Research & Reviews in Computer Science,* 2011.
16. *Zhirov A.O., Zhirova A.O., Krendelev S.F.* Bezopasnye oblachnye vychisleniya s pomoshch'yu gomomorfnoy kriptografii [Secure Cloud Computing with Homomorphic Cryptography], *Bezopasnost' informatsionnykh tekhnologiy* [Information technology security], 2013, № 1, pp. 6-12.
17. *Regev O.* New lattice-based cryptographic constructions, *J. ACM,* 2004, Vol. 51, No. 6, pp. 899-942.

18. *Regev O*. On lattices, learning with errors, random linear codes, and cryptography, *STOC*, 2005, pp. 84-93.
19. Helib. Available at: https://github.com/homenc/HElib (accessed 01 June 2020).
20. FHEW. Available at: https://github.com/lducas/FHEW (accessed 01 June 2020).
21. *Gentry C., Halevi S.* Implementing gentry's fully-homomorphic encryption scheme, *EUROCRYPT, ser. Lecture Notes in Computer Science*, K.G. Paterson, Ed.,Vol. 6632. Springer, 2011, pp. 129-148.
22. *Dijk M., Gentry C., Halevi S., Vaikuntanathan V.* Fully Homomorphic Encryption over the Integers, *Eurocrypt*, 2010.

Статью рекомендовал к опубликованию профессор И.А. Калмыков.

Бабенко Людмила Климентьевна – Южный федеральный университет; e-mail: blk@tsure.ru; 347928, г. Таганрог, ул. Чехова, 2, корпус "И"; тел.: +79054530191; кафедра безопасности информационных технологий; д.т.н.; профессор.

Русаловский Илья Дмитриевич – e-mail: ilya.rusalovskiy@mail.ru; тел.: +79885526701; кафедра безопасности информационных технологий; аспирант.

Babenko Lyudmila Kliment'evna – Southern Federal University; e-mail: blk@tsure.ru; Block "I", 2, Chekhov street, Taganrog, 347928, Russia; phone: +79054530191; the department of information technologies security; dr. of eng. sc.; professor.

Rusalovsky Il'ya Dmitrievich – e-mail: ilya.rusalovskiy@mail.ru; phone: +79885526701; the department of information technologies security; postgraduate student.

УДК 621.396.96 DOI 10.18522/2311-3103-2020-4-221-229

Я.К. Миронов, П.Д. Миронова, К.Е. Румянцев

ВЕРОЯТНОСТНЫЕ ХАРАКТЕРИСТИКИ ПОРОГОВОГО АЛГОРИТМА ОБНАРУЖЕНИЯ СИНХРОИМПУЛЬСОВ В СИСТЕМЕ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА НА ОСНОВЕ ИНФОРМАЦИИ СО СМЕЖНОЙ ПАРЫ ВРЕМЕННЫХ СЕГМЕНТОВ*

Системы квантового распределения ключа (КРК) обеспечивают повышенную защищённость передаваемой информации. Для стабильной работы системы КРК необходима точная синхронизация станций пользователей при минимальных временных затратах. Предложен алгоритм обнаружения синхросигнала с пороговым тестом. Предполагается, что синхроимпульс одновременно находится в двух соседних временных сегментах. Вероятность обнаружения пары временных сегментов, где присутствует синхроимпульс, определяется вероятностью превышения порогового уровня суммарным количеством сигнальных и шумовых импульсов, регистрируемых в двух соседних сегментах. Цель исследований направлена на сравнительный анализ порогового уровня и вероятностных характеристик аппаратуры синхронизации при пороговом тестировании каждой пары временных сегментов внутри временного кадра, полученных при ориентации на модели Гаусса и Пуассона для числа фотонов и импульсов темнового тока (ИТТ), принимаемых за время анализа временного сегмента. Исследованы вероятностные характеристики алгоритма обнаружения синхросигналов в системе квантового распределения ключа на основе сравнения числа фотонов со смежной пары временных сегментов с пороговым уровнем. Анализируется применение аппроксимации статистических свойств процессов на выходе фотодетектора законом Пуассона и нормальным распределением. Оценивается влияния модели Пуассона и Гаусса на выбор порогового уровня и расчёт эффективности синхронизации при пороговом тестировании каждой пары временных сегментов внутри временного кадра,

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-37-90040.