СЕКЦИЯ № 4

«ИННОВАЦИИ В IT»

UDC 004.056.55

Zh.E. Temirbekova[1,a]
[1]Kazakh National University named after al-Farabi, Almaty, Kazakhstan
[a]temyrbekovazhanerke2@gmail.com

USE HOMOMORPHIC ENCRYPTION FOR DATA SECURITY

Abstract. Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on ciphertexts and generate an encrypted result which, when decrypted, matches the result of operations performed on the plain texts. This article demonstrates homomorphic encryption in C ++.

Key words: homomorphic encryption, cloud computing, c++ language.

Аннотация. Гомоморфное шифрование - это форма шифрования, которая позволяет выполнять конкретные типы вычислений на зашифрованном тексте и генерировать зашифрованный результат. В данной статье продемонстрировано гомоморфное шифрование на языке C++.

Ключевое слова: гомоморфное шифрование, облачные вычисления, язык с ++.

Аңдатпа. Гомоморфты шифрлау бұл шифрланған мәтін бойынша есептеулердің нақты түрлерін орындауға және шифрланған нәтиже жасауға мүмкіндік беретін шифрлау нысаны болып табылады. Бұл мақалада C ++ тілінде гомоморфты шифрлау көрсетілген.

Түйінді сөздер: гомоморфты шифрлау, бұлтты есептеулер, с ++ тілі.

Among so many cryptographies, homomorphic encryption has attracted widely attentions from scholars for its special performance [1]. Common cryptography can't directly calculate on encrypted data, but homomorphic encryption can, meanwhile, the operation results of homomorphic encryption will be automatically encrypted. The application prospect of homomorphic encryption is widely and cheerful in the fields of secure multi-party computation, electronic voting, cipher text searching, encrypted mail filtering, mobile cipher. In the paper, the modified Encryption can meet multiplicative homomorphism and additive homomorphism and advance security. Finally, security analysis is test and farther research way is pointed out [2-3].

Homomorphic encryption seeks to aid in this encryption process by allowing specific types of computations to be carried out on ciphertext which produces an encrypted result which is also in cipher text [4]. Its outcome is the result of operations performed on the plaintext. Case in point, one person could add two encrypted numbers and then another person could decrypt the result, without either of them being able to find the value of the individual numbers.

Fully Homomorphic Encryption without Squashing Using Arithmetic Circuits In 2009, Craig Gentry presented the first fully homomorphic encryption scheme in his PhD dissertation. This technique allowed one to compute arbitrary functions over encrypted data without the use of a decryption key [5]. In his method, Gentry first constructs a somewhat homomorphic encryption, then compresses the decryption circuit to a more uncomplicated form. It is then bootstrapped toobtain a fully homomorphic encryption procedure. In 2011 Craig Gentry and ShaiHalevi devised an advanced approach that consisted of a fusion of SWHE and another type of encryption called multiplicatively homomorphic encryption (MHE). This novel process eliminated the need for the compression step Gentry originally proposed in his dissertation. In this method, Gentry and Halevi devised a system to condense the FHE ciphertext into a single ciphertext whose security was superior. [6].

The scheme of completely homomorphic encryption, which Gentry suggested, can be considered using the example of calculations in Z_2 [7-8]

Encryption

The process of data encryption can be represented as follows:

1. We choose an arbitrary odd number $p = 2k+1$, which is a secret parameter. Let $m \in \{0,1\}$

2. The number $z \in Z_2$ is compiled such that $z = 2r + m$, where r is an arbitrary number. This means that $z = m \bmod 2$.

3. In the process of encryption, each m is associated with the number $c = z + pq$, where q is chosen arbitrarily. Thus, $c = 2r + m + (2k+1) * q$. It is easy to see that $c \bmod 2 = (m+q) \bmod 2$ and therefore an attacker can determine only the parity of the output of encryption.

Decryption

Let the encrypted number c and the secret p be known. Then the process of decrypting the data should contain the following actions:

1. Decoding using a secret parameter $p : r = c \bmod p = (z + pq) \bmod p = z \bmod p + (pq) \bmod p$ where $r = c \bmod p$ is called noise

2. Obtaining the original encrypted bit: $m = r \bmod 2$.

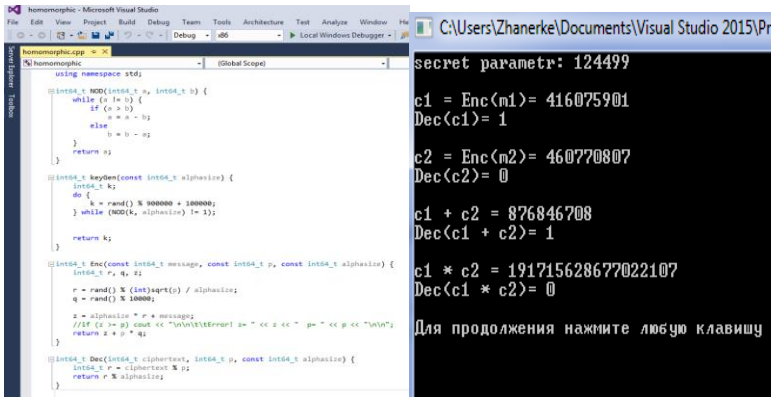

Figure 1. Demonstrated fully homomorphic encryption in C++

The use of fully homomorphic encryption

Cloud computing. One of the most important fields of application of fully homomorphic encryption is the execution of various mathematical operations on data stored on a remote cloud storage. The use of such an encryption scheme will make it possible to create a secure cloud service capable of performing various operations on user data without knowing exactly what it is for the data. [9-10]

In future I want to analyze the cloud platform with the use of homomorphic encryption features to protect data in the cloud.

REFERENCES

[1] N.P. Smart and F. Vercauteren, “Fully homomorphic encryption with relatively small key and ciphertext sizes,” public Key Cryptography-PKC Springer Berlin Heidelberg, vol. 6056, pp. 420-443, 2010.

[2] S. Goldwasser, S. Micali Probabilistic encryption // Journal of Computer and System Sciences. 1984. vol. 28. no. 2. pp. 270–299.

[3] C. Gentry. A Fully Homomorphic Encryption Scheme. PhD thesis, Stanford University, 2009. 199 p.

[4] Варновский Н.П., Шокуров А.В. Гомоморфное шифрование. // Труды ИСП РАН. 2007.

[5] C. Gentry, Theory of Computing, NY, New York, USA, 2009.

[6] А.О. Жиров, О.В. Жирова, С.Ф. Кренделев "Безопасные облачные вычисления с помощью гомоморфной криптографии"

[7] M.V. Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan, “Fully homomorphic over the integers”, In Proc. of Eurocrypt, vol. 6110, pp. 24- 43, Jan 2010

[8] I. Ahmad and A. Khandekar,“Homomorphic encryption applied to cloud computing,” International journal of Information and computer and technology, vol. 4, pp. 1519-1530, 2014.

[9] Бабенко Л.К., Буртыка Ф.Б., Макаревич О.Б., Трепачева А.В. Защищенные вычисления и гомоморфное шифрование. // III Национальный суперкомпьютерный форум (25-27 ноября 2014, г. Переславль-Залесский). ИПС имени А.К. Айламазяна РАН, 2014.

[10] Масштабные утечки данных: конец «облачным» сервисам? // Chip: журнал. - 2011.- № 8 (149).- С. 20-21. - SSN 1609-4212

UDK 004.93

B.K. Alimbayeva[1,a]
[1]al-Farabi Kazakh National University, Almaty, Kazakhstan
[a]bagilaalimbayeva@gmail.com

PROCESSING OF COMPUTED TOMOGRAPHY FOR DETECTION OF LUNG DISEASES

Abstract. Lung cancer is the leading cause of cancer-related death worldwide. In CT lung cancer screening, many millions of CT scans will have to be analyzed, which is an enormous burden for radiologists. Therefore there is a lot of interest to develop computer algorithms to optimize screening.

Key words: CT scans, computer algorithms, automatic detection of lung diseases.

Аннотация. Рак легких является основной причиной смертности от рака во всем мире. При скрининге рака легких при КТ многие миллионы КТ должны быть проанализированы, что является огромной нагрузкой для радиологов. Поэтому существует большая заинтересованность в разработке компьютерных алгоритмов для оптимизации скрининга.

Ключевые слова: КТ-сканеры, компьютерные алгоритмы, автоматическое обнаружение заболеваний легких.

Аңдатпа. Өкпенің қатерлі ісігі бүкіл әлемде онкологиялық аурулармен байланысты. КТ-да өкпе рагынының скринингінде көптеген миллиондаған КТ-тарды талдауға тура келеді, бұл радиологтарға үлкен жүктеме болып табылады. Сондықтан скринингті оңтайландыру үшін компьютерлік алгоритмдерді әзірлеуге үлкен қызығушылық бар.

Түйінді сөздер: КТ-сканерлер, компьютерлік алгоритмдер, өкпе ауруларын автоматты түрде анықтау.

Lung diseases are still one of the most common pathologies that affects all of humanity. The reason for this problem lies in the environmental pollution of air, the accumulating waste of industry, car exhausts, nuclear power products, the consequences of wars, industrial accidents, disasters, etc. A huge number of people fall ill with bronchopulmonary pathology, regardless of the current level of medical care. There are new diseases, and long-known "younger".

Please note: an important factor in the successful treatment of pulmonary ailments is the early detection of the pathological process. Here, of course, radial diagnostics is the key to solving the problem.