М.Тынышбаев атындағы
ҚАЗАҚ КӨЛІК ЖӘНЕ КОММУНИКАЦИЯЛАР АКАДЕМИЯСЫ

КАЗАХСКАЯ АКАДЕМИЯ ТРАНСПОРТА И КОММУНИКАЦИЙ
имени М.Тынышпаева

**«Көліктегі инновациялық технологиялар:
білім, ғылым, тәжірибе» атты
XLI Халықаралық ғылыми-практикалық конференцияның**

МАТЕРИАЛДАРЫ

3-4 сәуір 2017 жыл

1 том

МАТЕРИАЛЫ

**XLI Международной научно-практической конференции
на тему: «Инновационные технологии на транспорте:
образование, наука, практика»**

3-4 апреля 2017 года

Том 1

Алматы, 2017

ӘОЖ 656 (063)
КБЖ 39.1
К 67

К 67 «Көліктегі инновациялық технологиялар: білім, ғылым, тәжірибе» атты XLI Халықар. ғыл.-практ. конф. мат. (3-4 сәуір 2017 ж.) / Б.М. Ибраевтың редакциялауымен = «Инновационные технологии на транспорте: образование, наука, практика» (3-4 апреля 2017 г.) Мат. XLI Междунар. науч.-практ. конф. / Под ред. Б.М. Ибраева. – Алматы: М. Тынышбаев атындағы Қазақ көлік және коммуникациялар академиясы, 2016. – 1 т., 562 бет. – қазақша, орысша, ағылшынша.

Бұл жинаққа ҚР, Ресей, Германия, Польша, Латвия, Украина, Түрікменстан, Тәжікстан, Өзбекстан, Қырғызстанның жетекші ғалымдардың, профессор-оқытушылық құрамның, жас зерттеушілердің, көлік компанияларының және бизнес саласы өкілдерінің мақалалары кіреді. Материалдар жинағында көлік дамуының, логистика және тасымалдау үрдісін ұйымдастыруын, ресурстық үнемдеуін, темір жол жылжымалы құрамын, IT инновациясын, көлік құрылысын, көліктегі экономикасын және қазіргі заманауи кадрлар даярлау өзекті мәселелері қарастырылған.

Бұл жинақ көлік-коммуникациялық кешеннің, ғылыми-зерттеу ұйымдарының қызметкерлері мен жоғары оқу орындарына қызығушылығын тудырады.

Сборник включает статьи ведущих ученых, профессорско-преподавательского состава, молодых исследователей, представителей транспортных компаний и сферы бизнеса РК, России, Германии, Польши, Латвии, Украины, Туркменистана, Таджикистана, Узбекистана, Кыргызстана. В материалах рассмотрены актуальные проблемы развития транспорта, логистики и организации перевозочного процесса, ресурсосбережения, подвижного состава железных дорог, инноваций в IT, транспортного строительства, экономики на транспорте и подготовки кадров в современных условиях.

Настоящий сборник научных трудов представляет интерес для работников транспортно-коммуникационного комплекса, научно-исследовательских организаций и высших учебных заведений.

УДК 656 (063)
ББК 39.1

ISBN 978-601-207-996-8
ISBN 978-601-207-997-5

СОДЕРЖАНИЕ

СЕКЦИЯ № 1. ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМ АВТОМАТИКИ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ

СЕКЦИЯ № 2. РАЗВИТИЕ РАДИОЭЛЕКТРОННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ЖЕЛЕЗНОДОРОЖНОЙ ОТРАСЛИ

СЕКЦИЯ № 3. АКТУАЛЬНЫЕ ВОПРОСЫ В ЭЛЕКТРОЭНЕРГЕТИКЕ

СЕКЦИЯ № 4. ИННОВАЦИИ В IT

СЕКЦИЯ № 5. ИННОВАЦИОННЫЕ ПОДХОДЫ В ОРГАНИЗАЦИИ ПЕРЕВОЗОЧНОГО ПРОЦЕССА

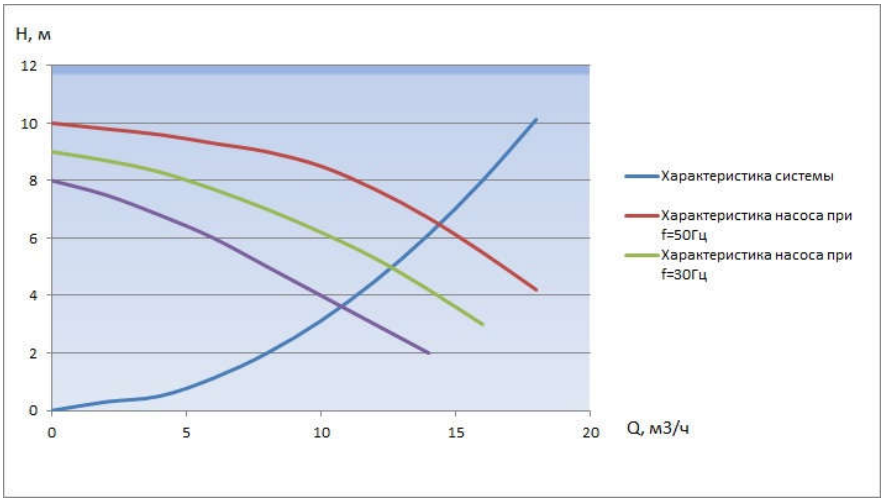

Рисунок 5 – «Q-H график» при ЧРП

Виртуальный лабораторный стенд используется для студентов специальности «5В070200 Автоматизация и управление» при проведении лабораторных работ по дисциплинам «Автоматизация объектов управления» и «Автоматизация типовых технологических процессов и производств». При использовании лабораторного стенда на лабораторных занятиях, студент должен ознакомиться с устройством и технологией работы насосной станции; выполнить все пункты задания и предоставить: таблицы расчетов напора сети для двух режимов; графики расходно-напорных характеристик насоса и сети для двух режимов; обоснованный выбор оптимального режима регулирования расходом; вывод по проделанной работе.

ЛИТЕРАТУРА

[1] Компоненты для комплексной автоматизации SIMATIC комплексная автоматизация производства. Каталог ST 70.- Алматы, 2014.

[2] Парр Э. «Программируемые контроллеры»»: руководство для инженера. – М.:БИНОМ. Лаборатория знаний, 2007. – 516 с.:ил.

[3] Петров И.В. «Программируемые контроллеры». Стандартные языки и приемы прикладного проектирования / Под ред. Проф. В.П. Дьяконова. - М.: СОЛОН-Пресс, 2004, 2007, 2008. – 256 с.:ил. – (Серия «Библиотека инженера»).

[4] Насосная азбука. - WILO, 2006.

[5] Сербин Ю.В., Прокопов А.А., Бугров В.П. Параллельная работа насосных агрегатов при использовании технологии частотного регулирования. – Информационный бюллетень, 2007, №2, ИНЖЕНЕРНЫЙ ЦЕНТР "АРТ".

УДК 51

B.K. Alimbayeva[1]

[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan, bagilaalimbayeva@gmail.com

PROGRAMMING A HOMOMORPHIC ENCRYPTION

Abstract. Currently, one of the most active areas development of information technologies – cloud computing. The main reason for this development is the opportunity for companies and individuals to reduce the cost of maintaining their own IT infrastructure by transferring. This work cloud service provider. However, in such a situation becomes unsafe storage and processing of sensitive data in the cloud, since its provider an opportunity to

uncontrolled access to the processed data. The only solution may be to encrypt all private data before transmission to the cloud.

Аннотация. В настоящее время одно из наиболее активных направлений развития информационных технологий – облачные вычисления. Основной причиной такого развития является возможность для компаний и частных лиц снижения расходов на поддержание собственной ИТ-инфраструктуры за счет передачи этой работы провайдеру облачного сервиса. Однако в такой ситуации становятся небезопасными хранение и обработка конфиденциальных данных в облачной инфраструктуре, так как у ее провайдера появляется возможность неконтролируемого доступа к обрабатываемым данным. Единственным решением этой проблемы может служить шифрование всех приватных данных перед передачей в облако.

Аңдатпа. Бұлтты есептеулер – қазіргі уақыттағы дамыған ақпараттық технологиялардың ең белсенді бағыттарының бірі. Бұл бағыттың дамуы ең алдымен компаниялар мен жеке тұлғалардың өздерінің жекеменшік АТ-инфрақұрылымын қолдаудағы шығынын азайтуға мүмкіндік береді, яғни бұл жұмысты бұлтты сервис провайдерлеріне өткізеді. Бірақ бұл ситуацияда құпия деректерді бұлтты инфрақұрылымда сақтау немесе өңдеу қауіпті болуы мүмкін, себебі провайдерлерде өңделетін деректерге бақыланбайтын қолжетімділік мүмкіндігі пайда болады. Бұл мәселенің жалғыз шешімі, бұлттық серверлерге барлық жеке деректерді беру алдында шифрлау болып табылады.

Keywords: homomorphic encryption, memory for data storage, Random Access Memory.

Ключевые слова: гомоморфное шифрование, память для хранения данных, оперативная память.

Түйінді сөздер: гомоморфты шифрлау, деректерді сақтау үшін жады, жедел жады.

Homomorphic encryption - encryption form, allowing to make certain mathematical operations with the encrypted text and receive encrypted result that matches the results of operations to be performed on plain text. For example, one person might add two encrypted numbers, and then another person could decipher the result of not using any of them. Homomorphic encryption would merge into a single whole range of services, not providing data for each service [1].

One of the areas of application - remote storage systems and services to allow for the processing of these data. certain cryptographic mechanisms are provided for the protection of information. There is one disadvantage of such systems to modify remote data transfer is necessary for the network secret key, that is simply his disclosure that puts security at risk

Homomorphic encryption is also actively used in various search engines in order to maintain the so-called "private research" - that is, the search for which a search engine does not know anything about what users send requests to it. This is very much needed for people who want to preserve the privacy of their own interests.

Furthermore, homomorphic encryption is used in the electronic voting systems, in particular, when using blind signatures [2].

Partially homomorphic cryptosystem - these cryptosystems are homomorphic with respect to only one operation (or addition or multiplication).

Partially homomorphic cryptosystem allow homomorphic computation only for a single operation (or addition or multiplication) plaintexts. Cryptosystem, which supports the addition and multiplication (thus keeping open the texts rings structure) is known as the fully homomorphic encryption and is more powerful. Using this system, any homomorphic scheme can be assessed, allowing us to efficiently create programs that can be run on the input encryption to generate the encryption output. Since such a program has never decrypt your input, it can be made unreliable party, without showing its input and internal state. In the existence of an effective and fully homomorphic cryptographic system would have great practical

implementation in the enclosed outsourcing computation, for example, in the context of the cloud. Homomorphic encryption would merge into a single whole range of services, not providing data for each service. For example, combining into one services of different companies could consistently calculate tax, apply the current exchange rate, send a transaction without providing the evidence for each of these services. Homomorphic property of various cryptographic systems can be used to create secure voting systems, hash functions, resistant to collisions, classified information and search engines enable the widespread use of public cloud computing, ensuring the confidentiality of processed data.

One of the major problems known fully homomorphic cryptosystem is their extremely low productivity. Currently, there are two main ways of its promotion in the use of "restricted homomorphism" and the so-called. "Packing method ciphertexts." The first involves a cryptosystem that can perform two types of operations (addition and multiplication), but in limited quantities. The essence of the second in that the one ciphertext recorded several plaintexts and wherein during operation of such a single batch ciphertext occurs simultaneous processing of all of its constituent ciphertexts [3].

Homomorphic encryption is a form of encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext.

This is sometimes a desirable feature in modern communication system architectures. Homomorphic encryption would allow the chaining together of different services without exposing the data to each of those services. For example, a chain of different services from different companies could calculate 1) the tax 2) the currency exchange rate 3) shipping, on a transaction without exposing the unencrypted data to each of those services. Homomorphic encryption schemes are malleable by design. This enables their use in cloud computing environment for ensuring the confidentiality of processed data. In addition the homomorphic property of various cryptosystems can be used to create many other secure systems, for example secure voting systems, collision-resistant hash functions, private information retrieval schemes, and many more.

There are several partially homomorphic crypto-systems, and also a number of fully homomorphic crypto-systems. Although a crypto-system which is unintentionally malleable can be subject to attacks on this basis, if treated carefully homomorphism can also be used to perform computations securely.

In future, I must develop an algorithm for protecting the network application. And also to study the architecture of high-performance systems and address the vulnerability of high-performance computing.

REFERENCES

[1] Craig Stuntz "What is Homomorphic Encryption, and Why Should I Care?". - 2010

[2] Ron Rivest. "Lecture Notes 15: Voting, Homomorphic Encryption" (PDF). – 2002

[3] Гомоморфное шифрование Н. П. Варновский, А. В. Шокуров //Труды Института Системного программирования: Том 12. (под Ред. В.П Иванникова) — М.:ИСП РАН, 2006, с. 27-36.

[4] Мао В. Современная криптография: Теория и практика — М.: Вильямс, 2005. — 768 с. — ISBN 5-8459-0847-7.