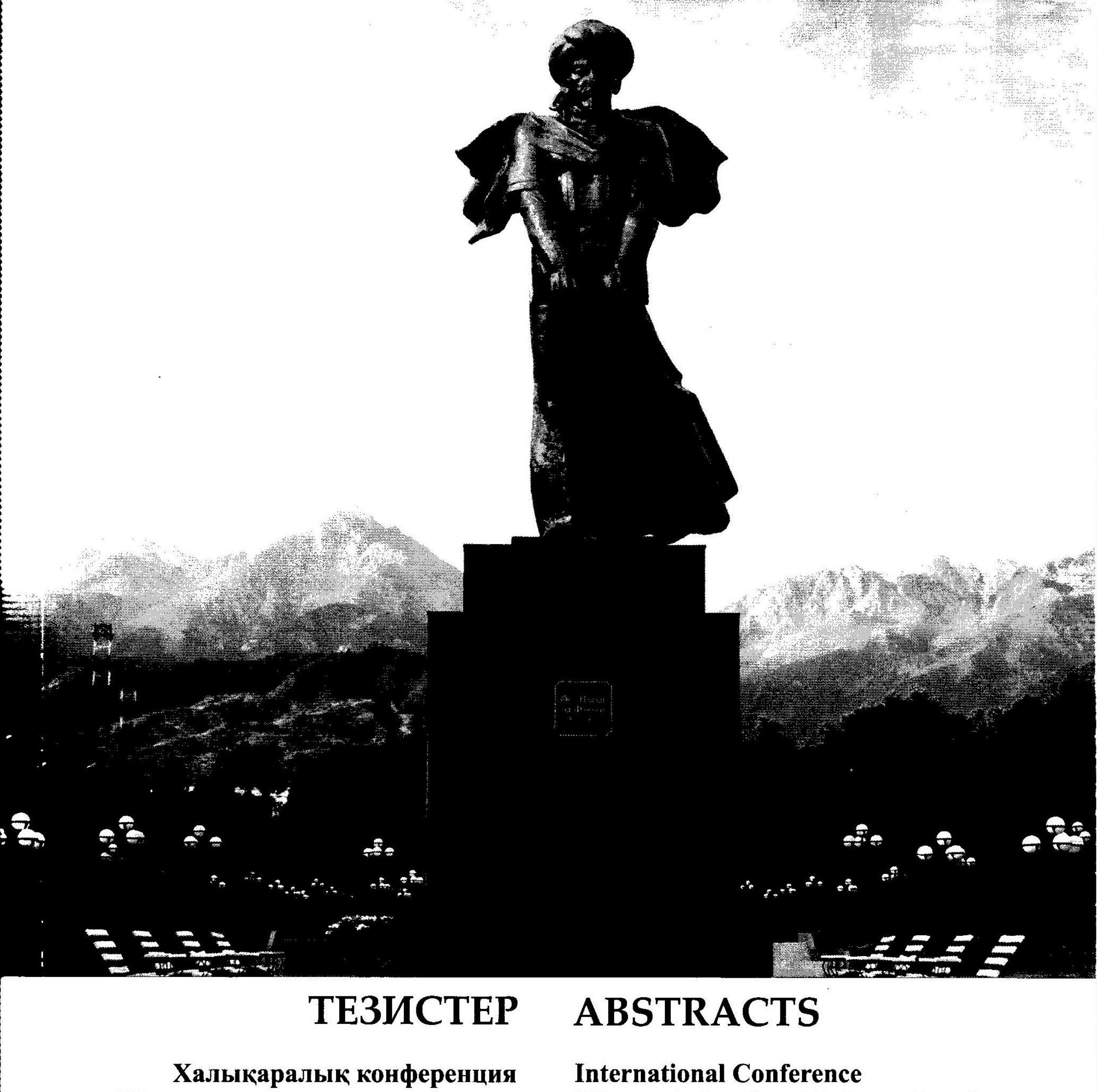
Әл-Фараби атындағы Қазақ ұлттық университеті	Al-Farabi Kazakh National University
РҒА СБ есептеу технологиялары институты	Institute of Computational Technologies of SB RAS
Қазақстан Республикасының Ұлттық Инженерлік академиясы	National Engineering Academy of the Republic of Kazakhstan
Штутгарт өнімділігі жоғары есептеу орталығы	High Performance Computing Centre in Stuttgart
Косовска Митровицасындағы Приштин университеті	University of Pristina in Kosovska Mitrovica
Абу-Даби университеті	Abu Dhabi University
Новосібір ұлттық зерттеу мемлекеттік университеті	Novosibirsk National Research State University
Новосібір мемлекеттік техникалық университеті	Novosibirsk State Technical University
Сібір телекоммуникация және информатика мемлекеттік университеті	Siberian State University of Telecommunications and Information Sciences
Ақпараттық және есептеу технологиялар институты	Institute of Information and Computational Technologies



ТЕЗИСТЕР ABSTRACTS

Халықаралық конференция “Ғылымдағы, техникадағы және білім берудегі есептеулер мен ақпараттар технологиясы”

International Conference “Computational and Informational Technologies in Science, Engineering and Education”

CITech2015

24-27 қыркүйек 2015
Алматы, Қазақстан

September 24-27 2015
Almaty, Kazakhstan

[illegible] А.А.

Al-Farabi Kazakh National University
Institute of Computational Technologies of SB RAS
National Engineering Academy of the Republic of Kazakhstan
High Performance Computing Centre in Stuttgart
University of Pristina in Kosovska Mitrovica
Abu Dhabi University
Novosibirsk National Research State University
Novosibirsk State Technical University
Siberian State University of Telecommunications and Information Sciences
Institute of Information and Computational Technologies

ABSTRACTS

International Conference "Computational and Informational Technologies in Science, Engineering and Education"

2015, Almaty, Kazakhstan

Section 2. INFORMATION MANAGEMENT, PROCESSING AND SECURITY 41

K.A. Aidarov, G.T. Balakaeva, *Admission control for server clusters based on QoS requirements* 42

B. Akhmetov, I. Aleksandr, Y. Funtikova, Z. Alibiyeva, *Multicriteria statistical analysis of test biometric data* 43

B. Akhmetov, S. Kachalin, A. Bezyaev, K. Mukapil, *Solving the inverse task of neural network biometrics without mutations and Jenkins' "nightmare" in the implementation of genetic algorithms* 44

Y.N. Amirgaliyev, A.S. Kalimoldayeva, *Module of lexical and morphological analyzer in the development of semantic engine for kazakh language* 45

E.N. Amirgaliyev, O.J. Mamyrbayev, T.A. Muratkhanova, *Recognition of isolated words using the Bayes' theorem* 46

A. Andrianova, O. Yakubailik, *Usage of GIS technology in the analysis of spatial dynamics of hydrobiological data (Enisey river case study* 47

B. Arsić, P. Spalević, M. Bašić, N. Arsić, G. Popović, *Facebook profiles clustering* 48

M.Z. Arslanov, *Polynomial algorithm for multiprocessor schedulling problem with three job lengths* 49

A.M. Bakiyeva, T.V. Batura, A.M. Fedotov, *Methods and Systems of Automatic Text Summarization* 50

O.E. Baklanova, A.E. Baklanov, O.Ya. Shvets, *Design of Automated Image Recognition System to Assess the Quality of the Mineral Species using CASE Technology* 51

M. Bašić, B. Arsić, *A novel approach of statistical data manipulation by using some clustering methods* 51

R.G. Biyashev, S.E. Nyssanbayeva, Ye.Ye. Begimbayeva, *A modification of the digital signature algorithm based on modular arithmetic* 53

R.G. Biyashev, M.N. Kalimoldayev, S.E. Nyssanbayeva, N.A. Kapalova, R.A. Khakimov, *Software Implementation of the Cryptographic System Models Protection With the Given Cryptostrength* 54 ✓

A. Erzin, N. Mladenovic, R. Plotnikov, *VNS-based heuristics for Communication Tree Optimal Synthesis Problem in Wireless Sensor* 55

A. Erzin, N. Shabelnikova, L. Osotova, Y. Amirgaliyev, *Wireless sensor networks and computational geometry problems* 56

[12] Lloyd, S., *Least squares quantization in PCM*, Information Theory, IEEE Transactions on, **28(2)**, 129-137 (1982).

[13] Arthur, D., and Vassilvitskii, S., *How Slow is the k-means Method?*, In Proceedings of the twenty-second annual symposium on Computational geometry, ACM, 144-153 (2006).

[14] Har-Peled, S., and Sadri, B., *How fast is the k-means method?*, Algorithmica, **41(3)**, 185-202 (2005).

► **R.G. Biyashev** - Institute of Information and Computational Technologies of MES RK (IICT), Almaty, Kazakhstan, email: brg@ipic.kz, **S.E. Nyssanbayeva** - IICT, Almaty, Kazakhstan, email: snyssanbayeva@gmail.com, **Ye.Ye. Begimbayeva** - IICT, Almaty, Kazakhstan, enlik_89@mail.ru

A modification of the digital signature algorithm based on modular arithmetic

In the information exchange security systems to protect information during transmission and data exchange between states the cryptographic encryption and digital signature (DS) systems are used. Due to the widespread using of DS many aspects of the theory and practice of public key digital signatures are currently extensively researched.

With the appearance of new mathematical methods and a substantial increase in productivity of cryptosystems, the question of cryptostrength of these algorithms becomes obvious. Developers increase the size of the system-wide parameters for algorithms to improve the cryptostrength of cryptosystems. Therefore, an important problem is to find the cryptographic transformation that would increase the algorithm's cryptostrength.

The Digital Signature Algorithm (DSA) [1] scheme represents the variation of ElGamal and K.Schnorr's digital signature scheme. Its reliability is based on the practical irresolubility of the computing problem of discrete logarithm. In DSA the conversion module length is about 1024 bits. Keys' length increased to the same length. In this regard, the computational complexity of the cryptographic transformations increases, but the speed of calculations decreases.

The model of modular system of digital signature with public key is proposed. These systems are developed on the basis of the algebraic approach using NPNs or polynomial residue number systems (polynomial RNS). In contrast to the classical RNS, where the bases are the prime numbers, in NPNs bases are represented by irreducible polynomials over GF(2) [2]. Usage of NPNs allows reducing the key length, increasing strength and efficiency of the nonpositional cryptographic algorithms [3]. Efficiency increase provided by the rules of NPNs in which all arithmetic operations can be performed in parallel on the modules of polynomial bases of NPNs. In nonpositional cryptosystems as a cryptostrength criterion was used the cryptostrength of digital signature formation algorithms, which is characterized by a full secret key.

Modified digital signature system that is being developed, based on DSA algorithm and NPNs, is characterized by improvement of the basic characteristics of the digital signature. Application of algebraic approach based on NPNs will allow reducing the key length for digital signature without significantly lowering its cryptostrength. Computer modeling of the modified cryptosystems will allow the development of recommendations for their secure usage and generation of full secret keys.

References

[1] FIPS PUB 186, *Digital Signature Standard (DSS)*, 119, (2009).

[2] Biyashev, R.G., *Development and investigation of methods of the overall increase in reliability in data exchange systems of distributed ACSs.*, Doctoral Dissertation in Technical Sciences, Moscow (1985).

[3] Biyashev, R.G. and Nyssanbayeva, S.E., *Algorithm for Creation a Digital Signature with Error Detection and Correction*, Cybernetics and Systems Analysis. **4**, 489-497 (2012).

► **R.G. Biyashev** - Institute of Information and Computational Technologies Ministry of Education and Science (IICT), Almaty, Kazakhstan , email: brg@ipic.kz, **M.N. Kalimoldayev** - IICT, Almaty, Kazakhstan, email: mnk@ipic.kz, **S.E. Nyssanbayeva** - IICT, Almaty, Kazakhstan, email: snyssanbayeva@gmail.com, **N.A. Kapalova** - IICT, Almaty, Kazakhstan, email: Kapalova@ipic.kz and **R.A. Khakimov** - IICT, Almaty, Kazakhstan, email: relesssar@mail.ru.

Software Implementation of the Cryptographic System Models Protection With the Given Cryptostrength

The models of software implementation of the system of cryptographic protection of information (SCPI) with the specified characteristics are described. This system is designed for using in systems and networks of information transmission and storage. In this system of cryptographic protection of information, the nonconventional algorithms of encryption and digital signature developed on the basis of nonpositional polynominal notations (NPNs) are implemented. The general feature of the model is that the fact the created SCPI implements encryption algorithms and digital signature formation with a given cryptostrength. The cryptostrength of these encryption algorithms is determined by the total number of possible and distinct from each other variants of choice of key sequences and systems of working base numbers. The mentioned system is the complex of computer programs which will consist of three interconnected blocks: the formation of full secret keys, the system of encryption and the digital signature scheme.For software implementation two models of cryptographic protection of information are proposed. In the first SCPI model the choice of full keys of the realized cryptoalgorithms is implemented from the DB of irreducible polynomial with binary coefficients directly in the blocks of program modules of encryption and digital signature formation. In the second SCPI, the full key for encryption and EDS computing systems is formed in the keys formation block with the use of the irreducible polynomials and is stored in the database of full keys. The creation of various models of the unconventional cryptographic systems allows to create such system of cryptographic information protection which it would be easy to transform under model changes of the implemented cryptographic algorithms.One of the planned works is to implement the SCPI model on the basis of the time pad. i.e. the full keys database will be stored on a removable memory (USB) and identified only by encryption software. The development of the system of cryptographic information protection is carried out in compliance with requirements of legal documents of the Republic of Kazakhstan in the field of informatization.

References

[1] BijashevR.G., *Development and investigation of methods of the overall increase of reliability in data exchange systems of distributed ACSs*, Doctoral Dissertation in Technical Sciences, Moscow (1985), p.328.

[2] Amerbayev B.M., Bijashev R. G. and Nyssanbayeva S.E., *Application of nonpositional polynominal notations at cryptographic protection*, // Math. Nat. Acad. Sciences of the Republic of Kazahstan.- Phys.-Math. - Almaty: Gylym (2005). - No. 3. - 84-89 p.

[3] Biyashev R., Kalimoldayev M., Nyssanbayeva S., Kapalova N., KhakimovR., *Program Modeling of the Cryptography Algorithms on Basis of Polynomial Modular Arithmetic*, The 5th International Conference on Society and Information Technologies (2014- Orlando, Florida, USA) - IIIS. pp. 49-54.

► **Adil Erzin** - Sobolev Institute of Mathematics of SB RAS, Novosibirsk, Russia, email: adilerzin@math.nsc.ru, **Nenad Mladenovic** - Belgrad, Serbia, email: nenadmladenovic12@gmail.com and **Roman Plotnikov** - Novosibirsk, Russia, email: nomad87@ngs.ru

VNS-based heuristics for Communication Tree Optimal Synthesis Problem in Wireless Sensor Networks

One of the most important issues in wireless sensor network (WSN) is minimization of energy consumption of its elements per time unit. We investigate the following problem, which occurs while minimizing the power consumption of data transmission in WSN in a case when each network element is able to adjust the transmission range:

Problem. *The simple undirected weighted graph $G = (V, E)$ with a vertex set V, $|V| = n$, and an edge set E is given. Let $c_{ij} \geq 0$ be the weight of the edge $(i, j) \in E$. We want to find a spanning tree T^* of the graph G, which is the solution to the problem:*

$$W(T) = \sum_{i\in V} \max_{j\in V_i(T)} c_{ij} \to \min_{T},$$

where Vi(T) is the set of vertices adjacent to a vertex i in the tree T.