Main directions of research and pedagogical activities of M.M. Glukhov's scientific school

A.B. PICHKUR, A.V. TARASOV

- Mikhail Mikhailovich Glukhov (1930 - 2018) - Doctor of Physical and Mathematical Sciences, Professor, full member of the Russian Academy of Cryptography, Honored Scientist of the Russian Federation.

A brief biography

- Mikhail Glukhov was born on November 20 in 1930 in the Tatar Autonomous Soviet Socialist Republic, in a working-class family.
- In 1949 he graduated from school and enrolled in the Melekess Teachers' Institute and in 1951 he graduated with honors.
- In 1951 - 1954 he worked as a mathematics and physics teacher at school and studied at the Ulyanovsk Pedagogical Institute.
- In 1954 he graduated with honors and started teaching in the Ulyanovsk Pedagogical Institute.
- In 1958 Mikhail Glukhov as a full-time postgraduate joined Lenin MSPU and continued teaching at the Moscow Correspondence Pedagogical Institute.

A brief biography

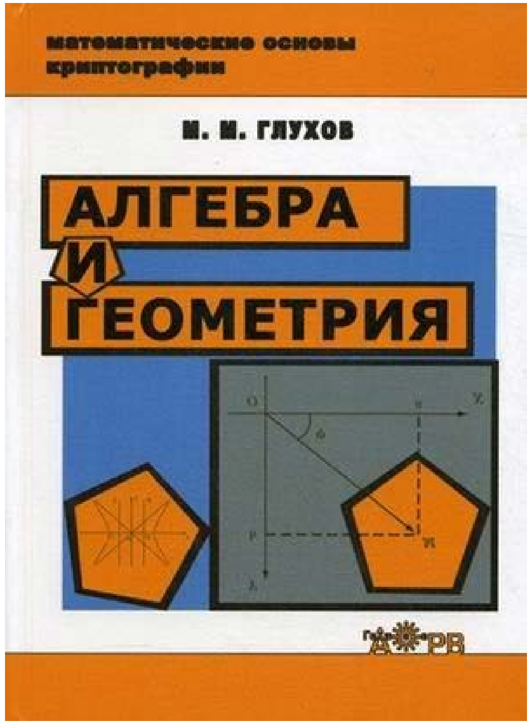
- At the end of graduate school he became the dean of the Faculty of Physics and Mathematics at Melekess Pedagogical Institute.
- In 1962 he defended his PhD thesis and then his doctoral dissertation in 1974.
- In 1973 - 1993 - Director of the Department of Mathematics.
- In 1993 - 2012 - Professor of the Department of Mathematics.
- Since 1992 Mikhail Glukhov was a full member of the Academy of Cryptography of the Russian Federation.
- Since 2005 he was Academician-Secretary of the Department of Mathematical Methods of Cryptography of Academy of Cryptography of the Russian Federation.

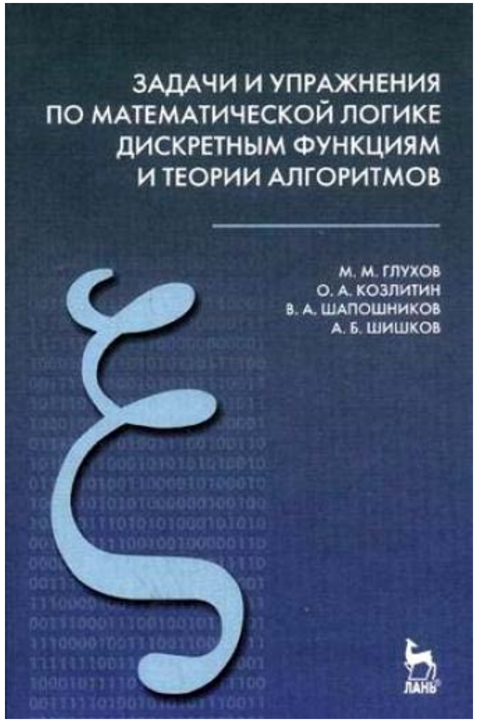
Pedagogical activity

Textbooks and tutorials:

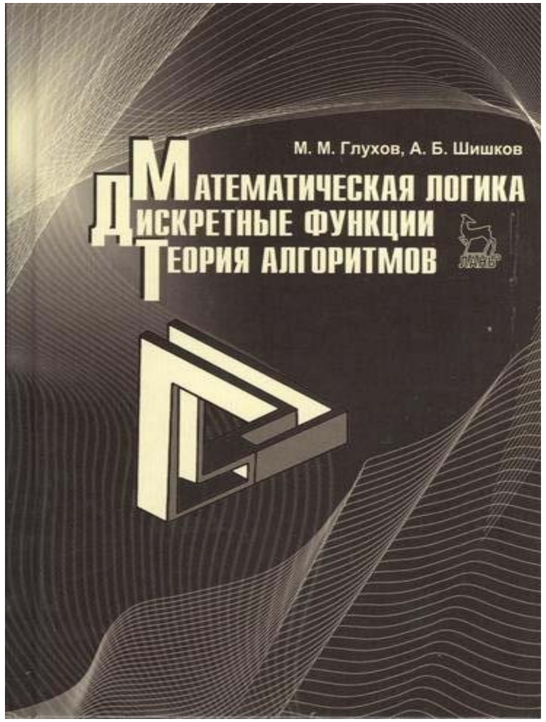
- the finite automata theory
- mathematical logic and theory of algorithms
- algebra and analytical geometry
- number-theoretic methods of cryptography
- group representation theory

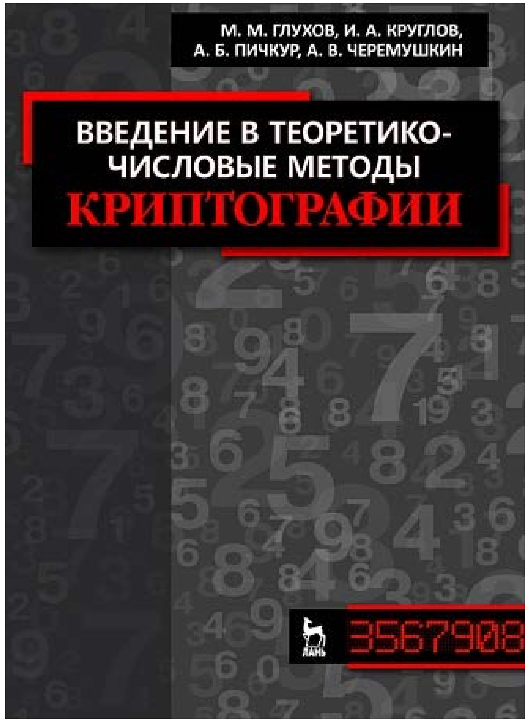
Pedagogical activity

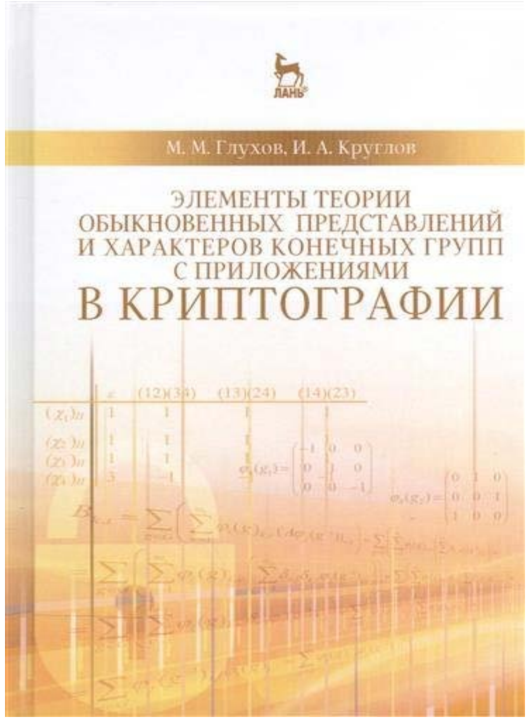




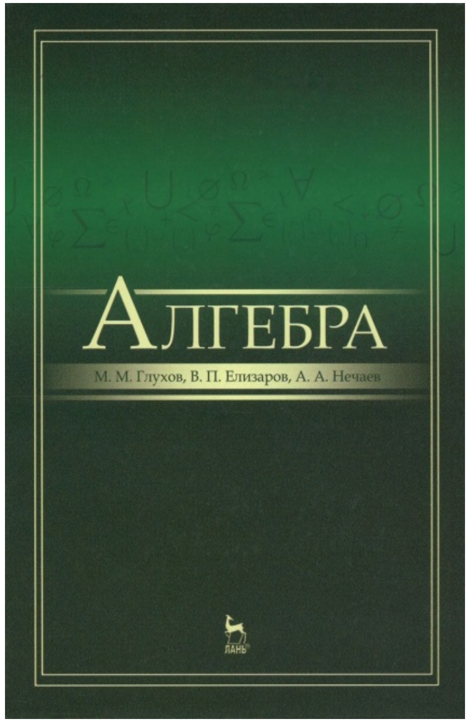
Pedagogical activity







Pedagogical activity



Algebraic aspects of cryptography

- At the turn of 1990s – 2000s there was a rapid development of the quantum computation theory
- In 1997 polynomiality of the discrete logarithm problem was proved in quantum setting
- This result initiated research in finding other difficult mathematical problems which might be used to design asymmetric cryptosystems

Algebraic aspects of cryptography

- 2007 - **Scherbakov V.A., Kostina A.A., Moldovyan P.A., Moldovyan N.A.** Proposed a public-key scheme based on the composition of conjugacy and discrete logarithm problems as a basis for national standard
- The authors' assumption was that the problem of key recovery in the scheme was not reduced to the discrete logarithm problem in a cyclic group of a finite field
- Mikhail Glukhov found a vulnerability and put the final point in the discussion about standardization of this scheme
- The Glukhov's report on this topic was the first talk presented at the 1st CTCrypt workshop in 2012

Algebraic aspects of cryptography

Let

$$A(\varepsilon)=\{(a,b,c): a,b,c \in Z/p^2\}$$

over Z/p^2 (p is large prime) with coordinate-wise addition of vectors and multiplication of vectors

$$(a,b,c)(x,y,z)=(ax+\varepsilon bz+\varepsilon cy, ay+bx+cz, az+\varepsilon by+cx),$$

where parameter $\varepsilon \in Z$, $p \mid \varepsilon$, $0<\varepsilon<p^2$.

Identity of algebra $A(\varepsilon)$ is the vector (1,0,0), element $\alpha=(a,b,c)$ is invertible if and only if $(a,p)=1$, $\Gamma=A(\varepsilon)^*$, the order of Γ is equal to $p^5(p-1)$.

Based on these data, they concluded that in the general case the group Γ is not cyclic and the maximal order of its cyclic subgroups is equal to $p^2(p-1)$.

Algebraic aspects of cryptography

In the proposed signature scheme the secret key is the pair of elements $X_1, X_2 \in \Gamma$ of order $\omega \geq p^2$, and the public key is the pair $Y_1 = X_1^p, Y_2 = X_2^p$

The security of the scheme is determined by the complexity of finding a p-th root of an element of Γ.

The authors considered two algorithms for solving this problem, the fastest of them has the complexity $O(p\sqrt{p})$ operations in Γ.

As a result they claimed that the group Γ is promising for designing signature schemes.

Algebraic aspects of cryptography

Structure of the group Γ

Lemma 1. *The set H of elements $\alpha=(a,b,c)\in\Gamma$, where $p\,|\,c$, is a subgroup of Γ, $|H|=p^4(p-1)$, and for all $\alpha=(a,b,c)\in H$ and $k\in\mathbb{N}, k\geq 2$ the following equality holds:*

$$\alpha^k=(a^k, ka^{k-1}b, ka^{k-2}(ac+C_k^2\varepsilon b^2)).$$

Lemma 2. *The set K of elements $\alpha=(a,b,c)\in\Gamma$, where $p\,|\,b$, $p\,|\,c$, is a subgroup of Γ, $|K|=p^3(p-1)$, and for all $\alpha=(a,b,c)\in K$ and $k\in\mathbb{N}$ the following equality holds:*

$$\alpha^k=(a^k, ka^{k-1}b, ka^{k-1}c).$$

Algebraic aspects of cryptography

Structure of the group Γ

Lemma 3. *Let* L *be the set of elements* $\alpha=(a,b,c)\in\Gamma$, *where* $p\,|\,b$. *Then for all* $\alpha=(a,b,c)\in L$ *and* $k\in\mathbb{N}, k\geq 5$ *the following equality holds:*

$$\alpha^k=(a^k+\varepsilon C_k^3a^{k-3}c^3, ka^{k-1}b+C_k^2a^{k-2}c^2+\varepsilon C_k^5a^{k-5}c^5, ka^{k-1}c+\varepsilon C_k^4a^{k-4}c^4)).$$

Lemma 4. *Each vector* $\alpha=(a,b,c)$ *from the set*

$$M=\{(a,b,c):(b,p)=1,(c,p)=1\}$$

can be represented in the form $\alpha=\alpha_1\alpha_2$, *where* $\alpha_1\in H\setminus K, \alpha_2\in L\setminus K$.

Algebraic aspects of cryptography

Structure of the group Γ

Theorem 1. *The following decompositions of the groups K, H and Γ into the direct product of cyclic groups hold:*

$$K = G_p^{(1)} \times G_p^{(2)} \times G_p^{(3)} \times H_{p-1},$$

$$H = G_{p^2}^{(1)} \times G_p^{(2)} \times G_p^{(3)} \times H_{p-1},$$

$$\Gamma = G_{p^2}^{(1)} \times G_{p^2}^{(2)} \times G_p^{(3)} \times H_{p-1},$$

where $G_{p^k}^{(i)}$ is the group of order p^k, $k = 1,2, i = 1,2,3,$ and H_{p-1} is the group of order $p-1$.

Theorem 2. *The complexity of finding the p-th root of an element $\xi \in \Gamma$, is $O(1)$, if $Ord\,\xi < p^2$, and $O(\log^2 p)$ or $O(\log^3 p)$, if $Ord\,\xi \geq p^2$.*

Corollary. *The complexity of finding the secret key in the examined signature scheme is $O(\log^3 p)$ binary operations.*

Algebra, cryptography and education

- A conference dedicated to the problems of teaching algebra in high school specialties in the field of information security was held in 2004
- The discussion was about which areas of algebra should be included in the student’s education
- Mikhail Glukhov explained his viewpoint on the example of AES

Algebra, cryptography …

Textblocks, keys and states are interpreted as matrices over finite field

$$GF(2^8) = GF(2)[x]/p(x),\ p(x) = x^8 + x^4 + x^3 + x + 1.$$

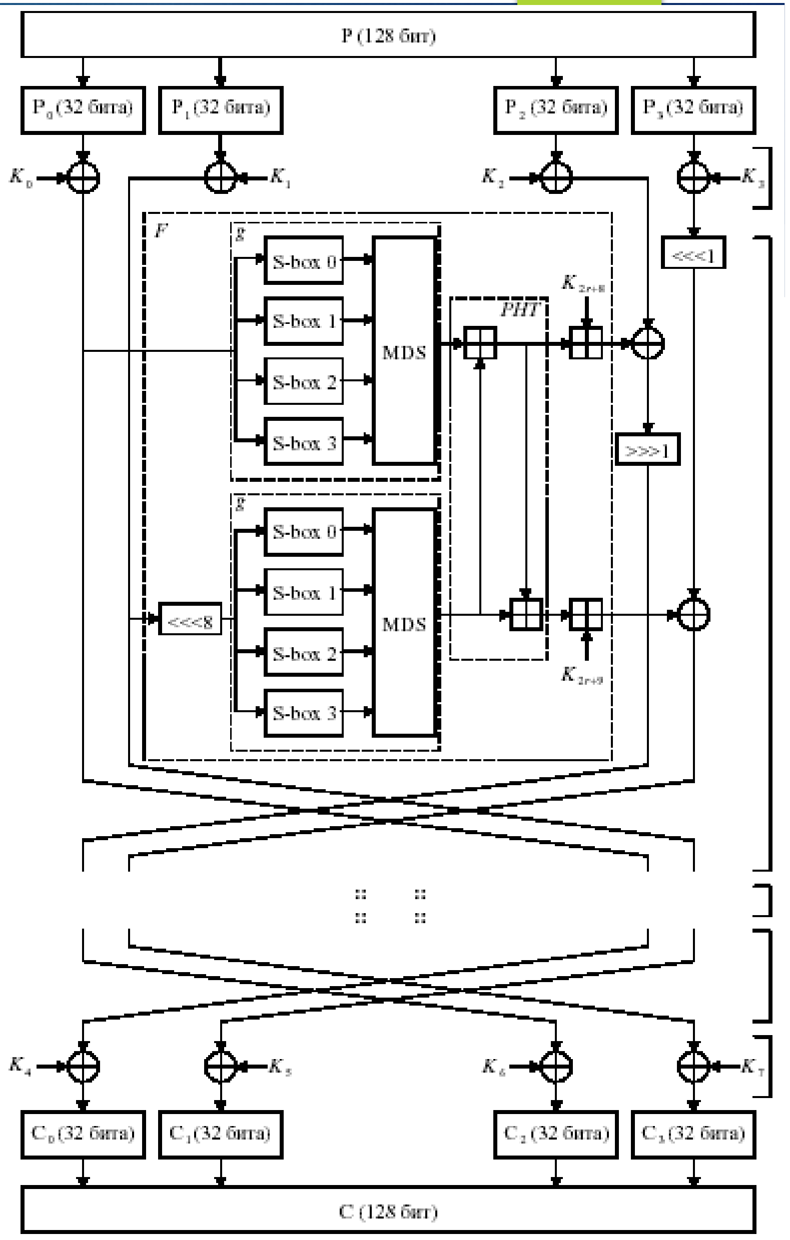
Byte $b = (b_7, b_6, \ldots, b_0)$ is interpreted as the polynomial

$$b(x) = b_7 x^7 + b_6 x^6 + \ldots + b_0 \in GF(2)[x]/p(x).$$

Matrices, which represent textblocks and keys, have 4 rows and 4 columns.

Round transformations have 3 types of slices:

- modulo 2 addition of an input block with an iterative key;
- non-linear transformation,
- linear transformation.



Algebra, cryptography and education

Non-linear transformation is represented as parallel application of 16 fixed bijective substitutions: $s_1 = \tau \cdot l \in S(GF(2^8))$, τ - reverse of non-zero elements of the field $GF(2^8)$, *l* – affine transformation of $GF(2^8)_{GF(2)}$.

Linear transformation is a composition of maps $h_1, h_2 \in GL_{16}(2^8)$:

h_1 - byte-wise cyclic shift of the three last rows of a matrix,

h_2 - multiplication on circulant matrix, may be represented as a polynomial multiplication modulo polynomial $x^8 + 1$.

Algebra, cryptography and education

Operations in AES:

- linear transformations of the vector space over the field *GF(2)*;

- substitutions;

- finite field $GF(2^8)$, as an extension of the field *GF(2)* by the root of irreducible polynomial .

Algebra, cryptography and education

Therefore an information security specialist should know:

- basics of linear algebra, the theory of vector spaces and linear transformations
- group theory fundamentals, in particular, the permutation groups theory
- basics of the theory of finite fields and polynomials over them

Actually, these areas form the basis of the algebra textbook

Publications and research areas

More than 150 papers in the

- theory of discrete functions
- theory of the finite rings
- theory of quasi-groups and their applications

The main contribution – in the theory of quasi-groups, groups and loops (non-associative quasi-groups) and their applications in cryptography

Researches on the coverage length, width and depth of the finite groups:

- length of coverage and powers of coverage layers for the main systems of generators of the symmetric group
- the value of the index measure of transitivity of the sets of round transformations of AES

Publications and research areas

- Researches in linear recursive sequences over finite rings and their applications
- Introduced iterative discrete functions and explored their properties
- Obtained the generalization of A.A. Markov theorem about non-distortion mappings
- Introduced index of affinity of discrete function, studied its connection with the function spectrum

Publications and research areas

- Obtained the group theory criteria of the planarity of the map. The map $f: GF(2^n) \rightarrow GF(2^n)$ is planar if the map $f(x+a)+f(x)+ax$ is bijective for all non-zero a.
- **Definition.** Let G_1, G_2 - equivalent abelian groups, H_1 and H_2 – their right regular representations. The map $f: G_1 \rightarrow G_2$ is *planar*, if the map $f(x+a)-f(x)$ – is bijective for all non-zero a.
- **Theorem.** The map f *is planar if and only if the set of substitutions* $H_1 f H_2$ is *2-transitive.*

Scientific school

- Under Mikhail Glukhov guidance 14 PhD theses was defended, three of his students became doctors of science
- His scientific school was supported by the grant from President of the Russian Federation

Свидетельство

Выдано
коллективу ведущей научной школы

НШ-8.2010.10,
руководитель – Глухов Михаил Михайлович

Государственное образовательное учреждение
высшего профессионального образования
«Академия Федеральной службы безопасности
Российской Федерации»

победителю конкурса на право получения средств для
государственной поддержки ведущих научных школ
Российской Федерации 2010 года.

(Область знаний - Военные и специальные технологии)

Председатель Совета по грантам
Президента Российской Федерации
академик РАН

И. Фёдоров

Scientific school

The main directions of research:

- algebraic, number-theoretic and combinatorial problems of cryptography
- finite rings and modules theory, the study of identities and corresponding polynomial functions
- multilinear recurrences and linear codes over finite bimodules
- perspective methods for constructing pseudo-random sequences with guaranteed cryptographic properties

Scientific school

The main directions of research:

- finite groups, permutation groups and corresponding operations with applications to design and analysis of cryptographic mechanisms
- properties of discrete functions, the construction of functions with specified properties, their classification by cryptographic parameters
- methods for solving systems of polynomial equations over finite rings using standard bases
- number-theoretic problems of cryptography

Scientific school

From 2003 to 2013 - 429 publications, including:

- 3 monographs
- 22 textbooks and manuals
- 195 articles in leading scientific journals
- 209 talks, of which 35 publications in foreign scientific journals

Defended: 6 doctoral and 15 PhD theses

Awards

Mikhail Glukhov was awarded:

- the Order of the Badge of Honor in 1986
- the Order of Honor in 2010 for success in teaching and research
- the title of Honored Scientist of the Russian Federation in 1997

Recommendations for young professionals

- Patriotism, morality and love of their work
- Mathematician-cryptographer should be able to build mathematical models of applied problems and show real audacity in problems formulation and solution
- A young specialist should understand that knowledge gained by him during his studies is far from sufficient to solve practical problems of information security, this is only a basis for subsequent great work in studying modern achievements in the relevant science field
- A lifetime is needed for studying new directions in science!