Криптография и кодирование на основе неассоциативных алгебраических структур.

Cryptograpy and coding based on non-associative algebraic structures

В.Т.Марков, А.В.Михалёв, А.А.Нечаев

Механико-математический факультет МГУ имени М.В.Ломоносова
Кафедра высшей алгебры
Кафедра теоретической информатики

Ломоносовские чтения, 2014

Introduction

The security of modern public key cryptosystems is defined by algorithmic complexity of some number-theoretic and algebraic problems, such as the number factorization problem or discrete logarithm problem in a finite field. Algebraic structures in which these cryptosystems are implemented are usually residue rings, finite fields, and point groups of algebraic curves. In this talk we discuss cryptosystems over nonassociative structures (quasigroups and quasigroup rings) and describe some construction of linearly optimal codes using left ideals in quasigroup rings.

Scheme based on a group ring. Basic notions

S.K. Rososhek (2003) suggested a cryptosystem on the following algebraic structure:

- K is an associative ring with unit,
- G is a group,
- KG is the group ring,
- Group ring KG contains enough elements with zero left annihilator,
- Groups of automorphisms $Aut\ K$ and $Aut\ G$ are non-commutative and contain enough elements.

Scheme based on a group ring. Cryptosystem description (A)

User A:

1. Constructs automorphisms $\sigma \in Aut\ K, \eta \in Aut\ G$.
2. Chooses random $\tau \in C(\sigma) \setminus \langle\sigma\rangle, \omega \in C(\eta) \setminus \langle\eta\rangle$
3. Constructs $\varphi \in Aut\ KG$ as the natural extension of the pair (τ,ω):

$$\varphi(a_{l_1} l_1 + \cdots + a_{l_n} l_n) = \tau(a_{l_1})\omega(l_1) + \cdots + \tau(a_{l_n})\omega(l_n)$$

4. Chooses random $a \in KG$
5. Computes $\varphi(a)$

Public key: $\left(\sigma, \eta, a, \varphi(a)\right)$

Secret key: φ

Scheme based on a group ring. Cryptosystem description (B)

User B:

1. Chooses random integers i, j and constructs the session automorphism $\chi \in Aut\ KG$ with the pair (σ^i, η^j).
2. Computes $\chi(a)$, $\chi(\varphi(a))$ and the left annihilator $Ann\big(\chi(\varphi(a))\big)$
3. If the latter is nonzero then a new session starts with a new element a or another session automorpisms is chosen,
4. Transforms the cleartext $m \in KG$ as follows: $m \cdot \Big[\chi(\varphi(a))\Big]$

Cryptogram: $\Big(\chi(a),\ m \cdot \Big[\chi(\varphi(a))\Big]\Big)$

User A:

1. Computes $\varphi\big(\chi(a)\big) = \chi\big(\varphi(a)\big)$, since χ and φ commute.
2. Decrypts the message by solving a linear equation system over the ring K (the condition $Ann(\chi(\varphi(a))) = 0$ implies that the solution is unique).

Modification: scheme based on a quasigroup ring

Definition

A *quasigroup* is a non-empty set equipped with one binary operation (we will write it as multiplication by default) with unique division from the left and from the right. A *loop* is a quasigroup with a left and right unit.

Let

- K be an associative ring with unit,
- L be a loop,
- KL be the non-associative quasigroup ring,
- quasigroup ring KL contain enough elements with zero left annihilator

Example

Let M be a Moufang loop with $|M| = 16$ and $|Aut\ M| = 1344$, $K = M_2(Z_5)$ and $S = M \times M$. Then $|KS| = 625^{256} > 2^{2304}$, $|Aut\ K| = |GL_2(Z_5)| = 480, |Aut\ S| = 231\ 211\ 008$, thus the number of suitable automorphisms of KS is $|Aut\ K| \cdot |Aut\ S|$=110 981 283 840.

Further modification: security parameters balancing

Instead of one element a it is possible to use r elements: $a_1, \ldots, a_r$ and construct automorphisms $\chi_1, \ldots, \chi_r$.
Cryptogram A looks like

$$\Big(\chi_1(a_1) \cdot \ldots \cdot \chi_r(a_r) \cdot \psi(x), m \cdot \Big[\chi_1\big(\varphi(a_1)\big) \cdot \ldots \cdot \chi_r\big(\varphi(a_r)\big) \cdot \psi\big(\varphi(x)\big)\Big]\Big).$$

Multiplication of elements

$$\chi_1\big(\varphi(a_1)\big) \cdot \ldots \cdot \chi_r\big(\varphi(a_r)\big) \cdot \psi\big(\varphi(x)\big)$$

and

$$\chi_1(a_1) \cdot \ \ldots \cdot \ \chi_r(a_r) \cdot \psi(x)$$

is implemented in random order.

Weakening the chosen cleartext attack

It is possible to multiply m from the left by another automoprhisms as follows:

$$\chi'(\varphi'(a')) \cdot \psi'(\varphi'(x')) \cdot \Big[m \cdot \chi(\varphi(a)) \cdot \psi(\varphi(x)) \Big].$$

Suppose also that the right annihilator of the element $\chi'(\varphi'(a')) \cdot \psi'(\varphi'(x'))$ is zero.

Such modification significantly weakens the chosen cleartext attack possibilities.

Homomorpic encription

Simplest Definition

Encryption scheme $E = (Encrypt, Decrypt)$ is homomorphic if one has:

$$Decrypt(c_1 \cdot c_2) = m_1 \cdot m_2,$$

$$Decrypt(c_1 + c_2) = m_1 + m_2,$$

where c_1, c_2 – ciphertexts corresponding to some plaintexts m_1, m_2, and $\cdot$, $+$ are operations in some ring.

Another requirement for homomorphic is that the ciphertext sizes remain bounded of the function g.

Scheme based on quasigroup ring. Homomorpic properties

The cryptosystem based on quasigoup rings is homomorphic with respect to multiplication in some cases.

Example

Consider the ring Z_2Q, where Q is a medial quasigroup (loop), i.e. $xy \cdot uv = xu \cdot yv$ for all elements of Q.
In the quasigoup ring based cryptosystem the decryption of $c_1 \cdot c_2$ gives:

$$\begin{cases} (m_1 \cdot (\psi_1(\varphi(x_1)))) \cdot (m_2 \cdot (\psi_1(\varphi(x_2)))) = r_1, \\ \varphi\big(\psi_1(x_1) \cdot \psi_2(x_2)\big) = \psi_1\big(\varphi(x_1)\big) \cdot \psi_2\big(\varphi(x_2)\big) = h_1. \end{cases}$$

Multiplication property is correct:

$$Decrypt(c_1 \cdot c_2) = m_1 \cdot m_2 = r \cdot h_1^{-1}$$

Moufang loops

Definition

A *Moufang loop* is a loop L satisfying the following identity:

$$(xy)(zx) = [x(yz)]x \quad \forall x, y, z \in L$$

Theorem (well known)

Let $(L, \cdot)$ be a Moufang loop. If $x(yz) = (xy)z$ for some $x, y, z \in L$ then x, y, z generate a subgroup in L.

Corollary

Every Moufang loop $(M, \cdot)$ is di-associative, i.e. any two elements of M generate a subgroup in M.

$[s, r]$-covers of loops

Let L be a finite loop. For any $s \times r$-matrix $A = (a_{ij})$ with elements $a_{ij} \in L$ consider the elements $A'_i = \sum_{j=1}^{r} a_{ij}$, $i = 1, \ldots, s$ of the loop ring $\mathbb{Z}L$.

Definition

An $s \times r$-matrix $A = (a_{ij})$ with elements $a_{ij} \in L$ is called an $[s, r]$-*cover* of the loop L if in the element $\sum_{\ell \in L} z_\ell \ell = \prod_{i=1}^{s} A'i$ the coefficients z_ℓ are positive for all $\ell \in L$ and this is valid for all arrangements of parentheses in the product.

Example

If $G = \langle g \rangle$ is a cyclic group of order n then the $s \times 2$ matrix $\begin{pmatrix} e & e & \ldots & e \\ g & g & \ldots & g \end{pmatrix}^T$ is a $[2, s]$-cover of G iff $s \geq n$.

Factorization problem for an $[s, r]$-cover

Let L be a finite Moufang loop and $\alpha = (a_{i,j})$ an $[s, r]$-cover of L.

Magliveras S. S., Stinson D. R., and Tran van Trung (2008) show that the complexity of factoring of any element $g = a_{1,j_1} \cdot a_{2,j_2} \cdots a_{s,j_s}$ of a finite group G is equivalent to the complexity of discrete logarithm computation in the group G.

Then in the general case the task of decomposition of an element $\ell \in L$ as $\ell = a_{1,j_1} \cdot a_{2,j_2} \cdots a_{s,j_s}$ with an unknown arrangement of parentheses is not less complex than the similar task in a finite group.

A cryptoscheme based on Moufang loops

1. A chooses two Moufang loops L, M such that there exist sufficiently many epimorphisms from L to M and randomly selects one of them $f : L \to M$. A keeps f secret.
2. A forms some $[s, r]$-cover $\alpha = (a_{ij})$ of L and computes its image $\beta = (b_{ij}) = (f(a_{ij}))$. α and β are published.
3. B randomly chooses a product $y_1 = a_{1,j_1} \cdot a_{2,j_2} \cdots a_{s,j_s}$ with some arrangement of parentheses, computes $y_2 = b_{1,j_1} \cdot b_{2,j_2} \cdots b_{s,j_s}$ with the same arrangement of parentheses as in y_1 and $y_3 = m \cdot y_2$, where $m \in M$ is the message.
4. B sends to A the cryptogram (y_1, y_3). A uses the secret epimorphism f to find $y_2 = f(y_1)$ and then deciphers m as $m = y_3 \cdot y_2^{-1}$.

Remarks to the described cryptoscheme

Remark (1)

L and M may be any two quasigroups such that the right division in M is easy to compute.

Remark (2)

Since the elements of the cover α by definition generate L, α and β uniquely define the epimorphism f, but again the example of the discreet logarithm map $f : \mathbb{F}_q^* \to \mathbb{Z}_{q-1}$ shows that formal knowledge of f is not sufficient for simple calculation of the images. Of course A must have some other presentation of f.

Remark (3)

In particular, it is possible that $L = M$ and thus $f \in \mathrm{Aut}(L)$. To make this scheme efficient one must have quasigroups with many automorphisms.

A loop with many automorphisms

Here we show a loop that has more automorphisms that any group of the same order. Define a loop L of order 6 by the multiplication table

0	1	2	3	4	5
1	0	3	2	5	4
2	4	0	5	1	3
3	5	4	0	2	1
4	3	5	1	0	2
5	2	1	4	3	0

Then $|\operatorname{Aut}(L)| = 20$, but $|\operatorname{Aut}(\mathbb{Z}_6) = 2|$ and $|\operatorname{Aut}(S_3)| = 6$.
In general the problem of existence of such loops for other values of order is still open.

Secret key exchange protocol based on a Moufang loop

History. In 1976г. W.Diffie и M.Hellman suggested key exchange protocol (DH protocol) based on finite fields.
In 2000г. K. H. Ko, S. J. Lee and et. al. developed protocol based on noncommutative groups with large commutative subgroups .
In 2005г. E. Stickel presented protocol based on noncommutative groups.

Let L be a generally known Moufang loop, and a, b, c its generally known elements such that $ab \neq ba$.

1. A chooses random positive integers $m < M, k < K, n < N$ and sends to B the pair $(u_1, u_2) = (a^m b^k, b^k c^n)$.
2. B chooses random positive integers $r < M, l < K, s < N$ and sends to A the pair $(v_1, v_2) = (a^r b^l, b^l c^s)$.
3. A computes $K_A = ((a^m v_1)b^k)((b^k v_2)c^n)$.
4. B computes $K_B = ((a^r u_1)b^l)((b^l u_2)c^s)$.

Then $K_A = K_B = (a^{m+r} b^{k+l})(b^{k+l} c^{n+s})$ is the common secret key.

Key exchange protocol: remarks

Remark 1.

Knowledge of one secret number implies that of the secret key. Consequently, the protocol complexity does not exceed the complexity of defining one secret key.

Remark 2.

To define the common key, the adversary has to solve the discrete logarithm problem in the subgroup $< a, b > \in L$ or $< b, c > \in L$ or to find the key as a loop element in L.

Key exchange protocol: an example

Paige loops

Consider the following finite, simple, non associative Moufang loop

The set of matrices $\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}$, where $a, b \in F_q$ и $\alpha, \beta \in F_q^3$, with operation

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \cdot \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac + \alpha \cdot \delta & a\gamma + d\alpha - \beta \times \delta \\ c\beta + b\delta + \alpha \times \gamma & \beta \cdot \gamma + bd \end{pmatrix}$$

is the Paige loop $M^*(q)$.

Thus, elements a, b, c might have the following form:

$$\begin{pmatrix} \eta & e_1 \\ 0 & \eta^{-1} \end{pmatrix}, \begin{pmatrix} \theta & e_2 \\ 0 & \theta^{-1} \end{pmatrix}, \begin{pmatrix} \zeta & e_3 \\ 0 & \zeta^{-1} \end{pmatrix},$$

where η, θ, ζ are some primitive elements of the field F_q.

Order of these elements is equal to $(q-1)/2$.

Key exchange protocol: an attack

A. Myasnikov, V. Shpilrain, A. Ushakov (2008) described attack to Stickel's protocol based on group of invertible $k \times k$ – matrices. The main idea is reduction problem to system of linear equations:

$$\begin{cases} xa = ax \\ yb = by \\ u = xy \end{cases}$$

Transform this system:

$$\begin{cases} x_1 a = a x_1 \\ yb = by \\ x_1 u = y \end{cases}$$

There are $3k^2$ equations and $2k^2$ unknowns.

But this attack doesn't work in nonassociative case, even in Paige loops.

Linearly optimal codes

Definition

A linear $[n, k, d]_q$-code is called *linearly optimal*, if it has maximal possible dimension k among all linear codes over the field $\Omega = \mathbb{F}_q$ having length n and distance d.

Evidently any linear MDS-code is linearly optimal.
Denote by $m(k, q)$ the maximal length of a linear MDS-code over $\mathbb{F}_q$ having dimension k. This notion is used to give another class of linearly optimal codes.

Proposition

Let n, k be positive integers and q a prime power such that $n > m(k+1, q)$. Then any linear $[n, n-k, k]_q$-code is linearly optimal.

Quasigroup codes

Definition

For any finite quasigroup $L = \{\ell_1, \ldots, \ell_n\}$ consider a *quasigroup algebra* $A = \mathbb{F}_q L$ and for any left ideal $I \leq {}_A A$ define the *quasigroup code*

$$\mathcal{C} = \mathcal{C}(I) = \left\{ (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n : \sum_i \alpha_i \ell_i \in I \right\}.$$

Example

Any quasigroup algebra contains 2 *trivial MDS-codes*: $[n, 1, n]$-code $\mathcal{C}(I_0)$ defined by the ideal $\mathbb{F}_q(\sum_{\ell \in L} \ell)$, and $[n, n-1, 2]$-code $\mathcal{C}(\Delta)$ defined by the fundamental ideal

$$\Delta(A) = \left\{ \sum_{\ell \in L} \alpha_\ell \ell : \sum_{\ell \in L} \alpha_\ell = 0 \right\}.$$

Commutator groupoids

Definition

Let G be a finite group. For fixed integers c, d we define a new multiplication on G be the rule:

$$x *_{c,d} y = x^{1-d} y^c x^d y^{1-c} = x[x^{-d}, y^c]y, \quad x, y \in G.$$

The resulting groupoid we denote by $(G)_{c,d}$ and call it the *commutator groupoid*, or the *commutator quasigroup* if it is a quasigroup.

In general we do not know for which G, c, d the groupoid G, c, d is a quasigroup. But if $G = D_n$ is a dihedral group, we have the following classification.

Commutator quasigroups for dihedral groups

Proposition

Let D_n be the dihedral group. Denote by $U(n)$ the set of integers k such that $2k-1$ is invertible modulo n and consider the four sets:
$M_0^n = 2\mathbb{Z} \cap U(n)$, $M_1^n = 2\mathbb{Z} \cap (\mathbb{Z} \setminus U(n))$,
$M_2^n = (2\mathbb{Z}+1) \cap U(n)$, $M_3^n = (2\mathbb{Z}+1) \cap (\mathbb{Z} \setminus U(n))$.
The following table shows the values of c and d for which $(D_n)_{c,d}$ is a quasigroup (and thus a loop):

	$d \in M_0^n$	$d \in M_1^n$	$d \in M_2^n$	$d \in M_3^n$
$c \in M_0^n$	$+$	$+$	$+$	$+$
$c \in M_1^n$	$+$	$+$	$-$	$-$
$c \in M_2^n$	$+$	$-$	$+$	$-$
$c \in M_3^n$	$+$	$-$	$-$	$-$

where $+$ means that the groupoid $(D_n)_{c,d}$ is a loop.

Associativity and isomorphisms of $(D_n)_{c,d}$

Proposition

If $c, d \in \overline{1, exp(D_n/Z(D_n)) - 1}$ *then* $(D_n)_{c,d}$ *is a semigroup iff* $c = d = 1$ *(in this case* $(D_n)_{c,d} = (D_n)^{op} \cong D_n$*) or both* c *and* d *are even (in this case* $(D_n)_{c,d} = D_n$*).*

Proposition

For different pairs $c, d \in \overline{1, exp(D_n/Z(D_n)) - 1}$ *such that* $c \in M_2^n$ *and* $d \in M_2^n$
(i.e. both c *and* d *are odd and both* $2c - 1, 2d - 1$ *are invertible modulo* n*) the corresponding loops* $(D_n)_{c,d}$ *are non-isomorphic.*

Linearly optimal codes in quasigroup algebras $\mathbb{F}_p(D_p)_{c,d}$

The following two statements (below and on the next slide) show that in some cases the loop algebras of the commutator loops contain left ideals which give linearly optimal quasigroup codes.

Theorem

Let $p > 2$ be a prime, $P = \mathbb{F}_p$. Suppose that $(D_p)_{c,d}$ is a non-associative loop and one of the following conditions holds

- *c is odd, d is odd, $\exists x \in \mathbb{Z}: \ x^2 \equiv 2c - 1 \pmod{p}$;*
- *c is even, d is odd, $\exists x \in \mathbb{Z}: \ x^2 \equiv 1 - 2c \pmod{p}$;*
- *c is odd, d is even.*

Then the quasigroup algebra $P(D_p)_{c,d}$ contains at least two ideals corresponding to linearly optimal $[2p, 2p-3, 3]_p$-codes.

Linearly optimal codes in quasigroup algebras $\mathbb{F}_q(D_{q-1})_{c,d}$

Theorem

Let p be a prime, l a positive integer, $q = p^l$ and $n = q - 1$. Suppose that $(D_n)_{c,d}$ is a non-associative loop and one of the of the following conditions holds:

- *c is odd, d d is odd, $2c \equiv 2 \pmod{n}$;*
- *c is even, d is odd, $2c \equiv 0 \pmod{n}$;*
- *c is odd and d even.*

If $p > 2$ (resp. if p=2) then the quasigroup algebra $\mathbb{F}_q(D_n)_{c,d}$ contains at least $2\varphi(q-1)$ (resp. $\varphi(q-1)$) left ideals a defining linearly optimal $[2q-2, 2q-5, 3]_q$-codes.

Bibliography

- Росошек, С.К. Криптосистемы групповых колец. Вестник Томского государственного университета. - 2003. - № 6. - С.57-62.
- Myasnikov, A., Shpilrain, V., Ushakov, A., Group-based Cryptography, Birkhauser Basel, Berlin, 2008.
- Грибов, А. В., Золотых, П. А., Михалёв А. В. Построение алгебраической криптосистемы над квазигрупповым кольцом, Матем. вопросы криптографии. - 2010. - Том 1, № 4. - С. 23-33.
- Марков В.Т., Михалёв А.В., Грибов А.В., Золотых П.А., Скаженик С.С. Квазигруппы и кольца в кодировании и построении криптосхем. Прикл. дискр. матем. - 2012. - № 4. -С. 31-52.
- С. Гонсалес, Е. Коусело, В. Т. Марков, А. А. Нечаев. Групповые коды и их неассоциативные обобщения. Дискр. матем. - 2004. - Том 14, №1. С. 146–156.
- Couselo E., Gonzalez S., Martinez C., Markov V., Nechaev A. Some constructions of linearly optimal group codes. Lin. Alg. Appl. - 2010. V. 433, № 2. - P. 356–364.

THANK YOU VERY MUCH

FOR YOUR ATTENTION!