Moldovyan D.N., Moldovyan N.A.

St.etersburg, Russia, SPIIRAS

A New Hard Problem over Non-Commutative Finite Groups for Cryptographic Protocols

Reporter: Moldovyan N.A.

Structure of the report

1. Hard problems used as cryptographic primitives.
2. Hard problems over non-commutative groups.
3. The MOR cryptosystem.
4. A new hard problem
5. Construction of finite non-commutative groups.
6. Cryptoschemes for post quantum cryptography

Hard problems used as cryptographic primitives

1. Factorization problem
(Given *n*. Find two large primes *p* and *q* such that $pq=n$).

2. Disceret logarithm problem
(Given *y*, *g* and *p*. Find *x* such that $y=g^x \bmod p$).

Both of these problems can be computed in polynomial time on a quantum computer

Hard problems over non-commutative groups (Γ)

1. The conjugacy search problem over Γ.
(Given $G \in \Gamma$, $Y \in \Gamma$, $\Gamma_{sub} \subset \Gamma$. Find $X \in \Gamma_{sub}$ such that $Y = XGX^{-1}$).

2. The decomposition search problem over Γ.
(Given $G \in \Gamma$, $Y \in \Gamma$, $\Gamma_{sub1} \subset \Gamma$, and $\Gamma_{sub2} \subset \Gamma$. Find $X \in \Gamma_{sub1}$ and $W \in \Gamma_{sub2}$ such that $Y = XGW$).

3. The membership search problem over Γ.
(Given the subgroup $\Gamma_{sub} \subset \Gamma$ generated by elements $H_1, H_2, \ldots, H_k$, and element Y. Find an expression of Y in terms of $H_1, H_2, \ldots, H_k$).

The MOR cryptosystem

1. The public key represents two inner automorphisms $\varphi(\Gamma)$ and $\varphi^{m}(\Gamma)$, where integer m is the secrete key.

2. To encrypt a message a user generates a random number r and computes $\varphi^{r}(\Gamma)$, $\varphi^{mr}(\Gamma)$, $\varphi^{mr}(G)$, where G – is a specified element, and cryptogram $C = KMK^{--1}$, where $K = \varphi^{mr}(G)$.

The MOR cryptosystem is broken, if one solves the DLP in the group of inner automorphisms of the group Γ or CSP in the group Γ.

Analysis of the known variants of the MOR cryptosystem have shown the DLP in the inner automorphisms group can be reduced to the DLP in Γ.

The MOR cryptosystem analysis results

Analysis of the known variants of the MOR cryptosystem have shown the DLP in the inner automorphisms group can be reduced to the DLP in Γ. The MOR cryptosystem is usually constructed using the finite groups of matrices.

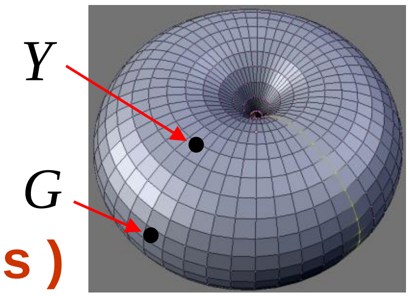
The DLP in the finite groups of matrices is reduced to the DLP in the fields *GF*(p^k) for sufficiently small integers *k* [*Menezes A. J., Wu Yi-H.* The Discrete Logarithm problem in *GLn*(*q*) // Ars Combinatorica. 1997. Vol. 47. P. 23-32].

Thus, the MOR cryptosystem give no security advantage over the cryptoschemes defined over the finite field.

The known variants of the public key formation

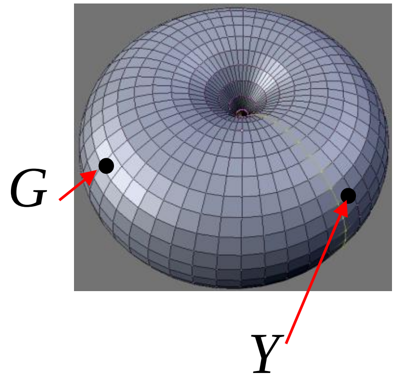
$$Y = G^{x}, \qquad x - \text{private key}$$

(computing in finite fields and commutative finite groups)



$$Y = XGX^{-1}, \qquad X - \text{private key}$$

(computing in finite non- commutative groups)



The proposed hard problem

$$Y = XG^{x}X^{-1},$$

where the pair (x, X) represents the private key, X is an element from some specified commutative subgroup possessing sufficiently large prime order

Correctness proof for public key agreement protocol

$$K_{12} = X_1 \circ Y_2^{x_1} \circ X_1^{-1} = X_1 \circ \left(X_2 \circ G^{x_2} \circ X_2^{-1} \right)^{x_1} \circ X_1^{-1} =$$

$$= X_1 \circ X_2 \circ G^{x_2 x_1} \circ X_2^{-1} \circ X_1^{-1}$$

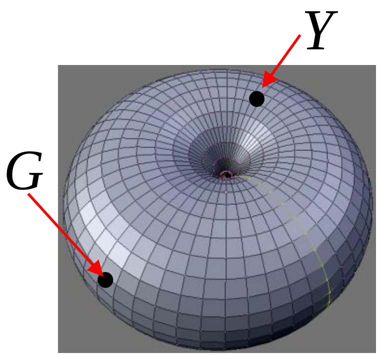
$$K'_{12} = X_2 \circ Y_1^{x_2} \circ X_2^{-1} = X_2 \circ \left(X_1 \circ G^{x_1} \circ X_1^{-1} \right)^{x_2} \circ X_2^{-1} =$$

$$= X_2 \circ X_1 \circ G^{x_2 x_1} \circ X_1^{-1} \circ X_2^{-1} = K_{12}.$$

Particular implementation

$$Y = Q^{x} G^{w} Q^{-x},$$

where $QG \neq GQ$



Theorem:

For all x = 1,2,…,q and w = 1,2,…,g, where q and g are the prime orders on the non-commutative elements Q and G, the Elements $Z_{x,w} = Q^{x} G^{w} Q^{-x},$ ***are pairwise different.***

Construction of the non-commutative finite groups of *m*-dimension vectors

To extend the class of the non-commutative groups with computationally efficient group operation it is proposed to construct the finite groups of vectors with associative and non-commutative multiplication.

The finite non-commutative groups of the different dimension vectors provides alternative variants of the construction of the cryptosystems based on the hidden subgroup DLP.

Defining the finite vector spaces

Description of the vectors:

$$(a,b,\ldots,c) \equiv a\cdot e + b\cdot i + \ldots + c\cdot j$$

a,b,…,c – elements of some finite field

e,i,…,j – formal basis vectors

Operations over vectors:

Addition is performed as addition of the corresponding coordinates of the operands

Multiplication is performed as multiplication of each component of the first operand with each component of the second operand

Defining the non-commutative finite groups of four-dimension vectors

Basis vector multiplication table

×	e	i	j	k			
e	e	i	j	k			
i	i	– e	k	– j			
j	j	– k	– e	i			
k	k	j	– i	– e			

Associativity property of the BVMT defines associativity of the vector multiplication operation. The order of the vector group is defined by formula

$$\Omega = p(p-1)(p^2-1).$$

The used non-commutative finite groups

- Groups of the matrices over finite fields

- Groups of the matrices over finite fields

Homomorphism into the underlying finite field

$$\Gamma \to GF(p) \; : \quad \varphi(A) = \Delta(A) \quad \forall \;\; A \in \Gamma$$

The homomorphism provides possibility to part the hidden subgroup DLP into two independent problems, namely the DLP and CSP.

To avoid such attacks the element G should be selected so that its order is mutually prime with the number *p* – 1:

$$\gcd\left(p-1, \omega(G)\right) = 1$$

Types of the proposed cryptoschemes for the “postquantum” cryptography

- **Public key agreement protocols**
- **Public key distribution protocols**
- **Commutative encryption algorithms**
- **Zero knowledge protocols**
- **Digital signature schemes (*probably it will be required a new type of the “hidden” difficult problems*)**

Advantages of the cryptoschemes based on the new hard problem

- Security against attacks using computations on a quantum computer
- Higher performance
- Cheaper implementation in hardware

Thanks for your attention !