APPLICATION OF NON-ASSOCIATIVE STRUCTURES FOR CONSTRUCTION OF HOMOMORPHIC CRYPTOSYSTEMS

First examples

- RSA, 1978; (partially homomorphic)
- El-Gamal, 1985; (partially homomorphic)

Main point

- Rivest R., 1978 (the first idea);
- Goldwasser S., 1982 (The first attempt);
- Feigenbaum J., 1991 (Definition FHE);
- Gentry C., 2009 (The first strong);
- Brakerski Z., 2011 (LWE);
- Burtyka F., 2014 (Matrix equations);
- Trepacheva A., 2014 (Known plaintexts attack).
- Gribov A. 2017 (Partially homomorphic on quasigroup)

Before

D-H algorithm on group $(G, +) \mapsto$ Algorithm El-Gamal

Homomorphic with respect to the group operation $+$.

Then

D-H algorithm on quasigroup $(G, *) \mapsto$ Our algorithm

Homomorphic with respect to the group operation $+$ and quasigroup operation $*$.

$(\Omega, *)$ — finite groupoid. $g \in \Omega$.
The right r-th power is defined as:

$$g^{[r]} = \underbrace{(\ldots((g * g) * g)\ldots)}_{r \text{ factors}}.$$

An element g is ***an element with commutating right powers*** (***CRP-element***) if

$$\forall m, n \in \mathbb{N}: \quad \left(g^{[m]}\right)^{[n]} = \left(g^{[n]}\right)^{[m]}.$$

If this identity holds for all $g \in \Omega$, then the groupoid $(\Omega, *)$ is called ***a CRP-groupoid***.
Respectively, define the left l-th power:

$${}^{[l]}g = \underbrace{(\ldots(g * (g * g))\ldots)}_{l \text{ factors}}.$$

Algorithm №1.

$(\Omega, *)$ — finite groupoid, $g \in \Omega$ — CRP-groupoid.

$$\begin{array}{ccc} A\ (r_A) & & B\ (r_B) \\ g^{[r_A]} & \longrightarrow & \\ & \longleftarrow & g^{[r_B]} \\ (g^{[r_B]})^{[r_A]} & = & (g^{[r_A]})^{[r_B]} \end{array}$$

The right discreet logarithm problem

$$g^{[x]} = h.$$

$(\Omega, *)$ is a ***groupoid with commuting powers*** (***CP-groupoid***) if it is a CLP- and CRP-groupoid and:

$$\forall g \in G, \quad \forall l, r \in \mathbb{N}: \quad {}^{[l]}(g^{[r]}) = ({}^{[l]}g)^{[r]} = {}^{[l]}g^{[r]}.$$

g is a *CP-element* if it generates a CP-groupoid.

Algorithm №2.

$$\underset{[a_1]\ldots[a_r]}{A}\ (r \le m)\ (a_1, \ldots, a_m) \quad \underset{\longleftarrow}{\overset{\longrightarrow}{g}} \quad B\ (s \le n)\ (b_1, \ldots, b_n)\ \underset{[b_1]\ldots[b_s]}{g}\ [b_{s+1}]\ldots[b_n]$$

Shared secret key — ${}^{[a_1]\ldots[a_r][b_1]\ldots[b_s]}g^{[b_{s+1}]\ldots[b_n][a_{r+1}]\ldots[a_m]}$.

The generalized discreet logarithm problem

Finding $u, v \in \mathbb{N}$ and $(x_1, \ldots, x_v)$ $x_i \in \mathbb{N}$, $i \in \overline{1, v}$, satisfying:

$${}^{[x_1]\ldots[x_u]}g^{[x_{u+1}]\ldots[x_v]} = h.$$

Let $(\Omega,+)$ be an abelian group. Fixing two commuting (anti-)automorphisms

$$\sigma, \tau \in \mathrm{Aut}(G), \quad \sigma\tau = \tau\sigma,$$

we define a new operation on Ω by the following condition:

$$\forall\, x, y \in \Omega \quad x * y = \sigma(x) + \tau(y).$$

we will call $(G, *)$ a ***medial quasigroup***.

Theorem

The groupoid $(G, *)$ is a CP-groupoid.

Cryptosystem 1

1. ***Public key generation.*** A chooses $g \in \Omega$, secret $r_A \in \mathbb{N}$ and computes the public key (g, g_A):
$$g_A = g^{[r_A]}.$$
2. ***Encryption.*** If $m \in \Omega$ – plaintext, B generates secret r_B and computes ciphertext (g_B, m_{AB}):
$$g_B = g^{[r_B]}, \qquad m_{AB} = m + g_A^{[r_B]}.$$
3. ***Decrypting.*** In order to decrypt a ciphertext A computes
$$m = m_{AB} - g_B^{[r_A]}.$$

Theorem

The Cryptosystem 1 operates correctly, the complexity of a message encryption is estimated by $O(AUT(\sigma, |\Omega|)\log_2(|\Omega|))$ *operations in the group* $(\Omega, +)$.

Cryptosystem 2

1. ***Public key generation.*** A chooses $g \in \Omega$, $r \leqslant n$ and $a_1, \ldots, a_n \in \mathbb{N}$, computes the public key (g, g_A):
$$g_A = {}^{[a_1]\ldots[a_r]}g^{[a_{r+1}]\ldots[a_n]}.$$
2. ***Encryption.*** If $m \in \Omega$ – plaintexts, B generates $t \leqslant k$ and $b_1, \ldots, b_k \in \mathbb{N}$, computes ciphertext (g_B, m_{AB})
$$g_B = {}^{[b_1]\ldots[b_t]}g^{[b_{t+1}]\ldots[b_k]}, \quad m_{AB} = m + {}^{[b_1]\ldots[b_t]}g_A^{[b_{t+1}]\ldots[b_k]}.$$
3. ***Decrypting.*** In order to decrypt a ciphertext A computes
$$m = m_{AB} - {}^{[a_1]\ldots[a_r]}g_B^{[a_{r+1}]\ldots[a_n]}.$$

Theorem

The Cryptosystem 2 operates correctly. The complexity of message encryption is estimated by $O(N \cdot AUT(\sigma, |\Omega|) \log_2(|\Omega|))$ *operations in the group* $(\Omega, +)$, *where* $N = \max(n, k)$.

Theorem

The cryptosystems 1 and 2 are homomorphic with respect to the group operation $+$.

Theorem

The cryptosystems 1 and 2 are homomorphic with respect to the group operation $*$.

Modification of Gelfond–Shank's algorithm

In last paper we presented modification of Gelfond–Shank's algorithm, and its realization requires $O(\sqrt{\Omega})$ operations in the group $(\Omega, +)$ and storage area of size $O(\sqrt{\Omega} \cdot \log_2(\sqrt{\Omega}))$.

A generalization of the method of reduction to proper subgroups

Fundamental difference in the complexity of the right logarithm problem on the medial quasigroup occurs only at the stage of calculating logarithms in the medial quasigroup built over a group isomorphic to $\mathbb{Z}_p + ... + \mathbb{Z}_p$

Let $(\Omega, *)$ be a CP-groupoid.
$K = \left\{(u, v, a_1, ..., a_v) \middle| \ u, v \in \mathbb{N}, a_i \in \mathbb{N}, i \in \overline{1, v}\right\}$ — set of powers (set of secret keys in Cryptosystem 2).

On K we define the relation ϵ by the rule:
$(u, v, a_1, ..., a_v) \overset{\epsilon}{\sim} (u', v', a'_1, ..., a'_v) \Leftrightarrow$
$\Leftrightarrow {}^{[a_1]...[a_u]}g^{[a_{u+1}]...[a_v]} = {}^{[a'_1]...[a'_{u'}]}g^{[{}'a_{u'+1}]...[a'_v]}$.

Denote $K_\epsilon = \frac{|K|}{[\vec{x}]_\epsilon}$, where $[\vec{x}]_\epsilon$ — is a equivalence class that containing element $\vec{x}$.

Theorem

Considered algorithm based on Hellman's method allows to find a shares secret key with complexity $K_\epsilon^{2/3}$ and requires $K_\epsilon^{2/3}$ memory cells.

We say that a map δ of the groupoid $(G, *)$ onto itself **imitates a secret key** $(r, n, a_1, ..., a_m)$ of user A if for any secret key $(s, n, b_1, ..., b_n)$ of user B the following equality holds:

$$\delta\left({}^{[b_1]...[b_s]}g^{[b_{s+1}]...[b_n]}\right) = {}^{[a_1]...[a_r][b_1]...[b_s]}g^{[b_{s+1}]...[b_n][a_{r+1}]...[a_m]},$$

For instance if $g^{[r]} = {}^{[a_1]...[a_r]}g^{[a_{r+1}]...[a_m]}$, then the operation of right exponentiation into power r is an imitating map.

Theorem

Maximal security of Algorithm open key distribution against Imitating map ($g^{[r]}$) is achieved and it is equal to $O(|\Omega|^{\frac{3}{4}})$.

(15) Example – practical encryption

If we take the cyclic group $(\mathbb{Z}_p, +)$ $(p > 2)$, the identical automorphism σ, and $\tau(x) = -x$, then we can prove that the proposed cryptosystems are homomorphic for an n-ary operation $*(a_1, ..., a_n)$ if and only if the operation $*$ is given by a linear function of $a_1, ..., a_n$ from $(\mathbb{Z}_p, +)$.