# АНАЛІЗ КРИПТОГРАФІЧНИХ СИСТЕМ І ПЕРСПЕКТИВА ВИКОРИСТАННЯ ПРОТОКОЛІВ У ГРУПАХ КОС

Кавуненко Я.О.
Науковий керівник – к.т.н., доц. Єпішкін С.О.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Інфокомунікацій, тел. (057) 702-55-92)

The given work is about researching of general weaknesses of protocols in braid groups.

Протягом декількох останніх років помітно зріс інтерес до криптографічних додатків, заснованим на перетвореннях в некомутативних групах. Групи КОС зокрема представляють особливий інтерес в силу своєї ефективності при забезпеченні трудомістких обчислювальних процесів. Різними групами дослідників були запропоновані протоколи з перетвореннями в групі КОС. У той же час можливості практичного застосування перетворень в групах КОС обмежені через недостатнє їх аналізу, як раз в криптографічних додатках. Метою цієї статті є розгляд і аналіз основних криптографічних перетворень і криптографічних протоколів в КОС групах, а також розгляду проблемних питань [1].

Коса з n-ламаних ниток – об'єкт який складається з двох паралельних площин $P_0$ і $P_1$ в трьохвимірному просторі $R^3$, який складається з впорядкованої множини точок $a_1, a_2, \ldots a_n \in P_0$, $b_1, b_2, \ldots b_n \in P_1$ і з n - простих ламаних $l_1, l_2, \ldots l_n$, які не перетинаються між собою, перетинаючи кожну площину $P_t$ між $P_0$ і $P_1$ і з'єднують точки $\{a_i\}$ з точками $\{b_i\}$ (рис. 1).

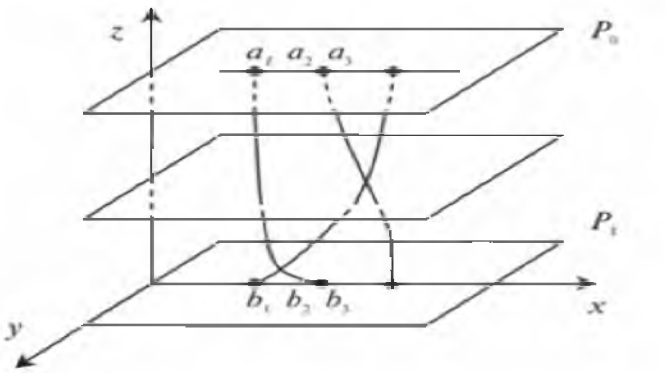


Рисунок 1 – Графічне представлення КОС

Фундаментальною в теорії КОС є теорема Артіна: група КОС $B_n$, ізоморфна абстрактнії групі, породженої утворювальними $b_1, b_2, \ldots b_{n-1}$, які задовольняють певним співвідношенням.

Грунтуючись на отриманих знаннях, були розглянуті наступні види криптографічних перетворень в КОС групах:

1. системи обміну ключами;

2. схеми шифрування / дешифрування;
3. протоколи аутентифікації;
4. механізм електронного цифрового підпису.

Стійкість криптосистем ґрунтується на наступних проблемах:

1. **Завдання пошуку сполучень (CSP)**: нехай (x, y) ∈ $B_nB_n$ такі, що y = $a^{-1}$xa, де a ∈ $B_n$ або однієї з підгруп $B_n$. Завдання знайти таке b, що y = $b^{-1}$xb.

2. **Завдання одночасного пошуку безлічі сполучень (MSCSP)**: нехай ($x_1$, $a^{-1}x_1a$)...($x_r$, $a^{-1}x_ra$) ∈ $B_nB_n$ такі, що y = $a^{-1}$xa, де a ∈ $B_n$ або однієї з підгруп $B_n$. Завдання знайти таке b, що y = $b^{-1}x_1b = a^{-1}x_1a$, ..., $b^{-1}x_rb = a^{-1}x_ra$.

3. **Завдання декомпозиції (BDP)**: нехай (x, y) ∈ $B_nB_n$ такі, що y = $a_1xa_2$ для ($a_1$, $a_2$) ∈ $LB_nLB_n$. Завдання знайти ($b_1$, $b_2$) ∈ $LB_nLB_n$ таку, що y = $b_1xb_2$.

4. **Завдання одночасної множинної декомпозиції (MSBDP)**: Нехай ($x_1$, $a_1x_1a_2$) ... ($x_r$, $a_1x_ra_2$) ∈ $B_nB_n$ для ($a_1$, $a_2$) ∈ $LB_nLB_n$. Завдання знайти пару ($b_1$, $b_2$) ∈ $LB_nLB_n$ таку, що y = $b_1x_1b_2 = a_1x_1a_2$, ..., $b_1x_rb_2 = a_1x_ra_2$.

5. **Завдання пошуку кореня (RP)**: Нехай x =, де a, x ∈ $B_n$ та p ∈ N. Завдання пошуку для експоненти *p* знайти таку косу b ∈ $B_n$, щоб = x.

6. **Завдання вибору пов'язаних елементів (CDP)**: Нехай (x, y) ∈ $B_nB_n$. Завдання встановити, чи є x і y сполученими, тобто встановити, чи існує таке a ∈ $B_n$ або однієї з підгруп $B_n$, що y = $a^{-1}$xa.

Виходячи з вищенаведеного, існує три основні різновиди атак:

1) використання рішення задачі пошуку сполучень;

2) використання імовірнісного підходу в $B_n$;

3) використання допоміжної групи, як правило, в уявленні Бурау [2].

Аналіз розглянутих криптографічних систем показує, що розробка алгоритмів, що використовують групи КОС є перспективним напрямком у розвитку криптографії. Основні характеристики систем наведені в таблиці 1.

Таблиця 1 – Основні характеристики криптографічних систем, що використовують групи КОС

| | |
|---|---|
| Вхідне повідомлення, біт | pnlog(n) |
| Зашифроване повідомлення, біт | 4pnlog(n) |
| Швидкість шифрування, операцій | $O(p^{2n}log(n))$ |
| Швидкість розшифрування, операцій | $O(p^{2n}log(n))$ |
| Довжина персонального ключа, біт | 0.5pnlog(n) |
| Довжина відкритого ключа, біт | 3pnlog(n) |
| Складність атаки «груба сила» | $((n/2)!)^p = exp(0.5pnlog(n))$ |

Перелік посилань:

1. D. Garber, S. Kaplan, M. Teicher, B. Tsaban and U. Vishne, Length-based conjugacy search in the braid group, Contemp. Math. 418 (2006), 75–87.

2. E. Artin, Theory of Braids, Ann. of Math. 48 (1947) 101–126.