УДК 004.056

В.С. Бурковський

Харківський національний університет радіоелектроніки, Харків

ОГЛЯД АЛГОРИТМІВ КРИПТОАНАЛІЗУ СИСТЕМ ВІДКРИТОГО РОЗПОДІЛУ КЛЮЧІВ ТИПУ ДІФФІ-ХЕЛЛМАНА, ЯКІ ЗАСНОВАНІ НА НЕКОМУТАТИВНИХ ГРУПАХ

Розглянути алгоритми криптоаналізу систем відкритого розподілу ключів типу Діффі-Хеллмана, які засновані на некомутативних групах.

***Ключові слова**: криптосистема Діффі-Хеллмана, криптоаналіз, некомутативні групи, групи кос, постквантова криптографічна платформа.*

Вступ

Сучасні Криптосистеми відкритого розподілу ключів типу Діффі-Хеллмана (Diffie-Hellman) [1] широко використовується в різних модифікаціях і вдосконаленнях для розподілу ключів. Крипостійкість їх перших варіантів ґрунтувалася на проблемі дискретного логарифмування (discrete logarithm problem (DLP)) в циклічних підгрупах абелевих (комутативних) груп. При цьому в якості груп G обиралися мультиплікативні групи кінцевих полів і кілець вирахувань та ін.

Класична платформа над полем F_q з елементом, що породжує $q = p^r$, де p – просте число, будувалася за наступною схемою.

Відкриті дані:

G – група з визначеною на ній нормальною формою nf ( ) її елементів;

$g \in G$ – виділений елемент.

Особисті секретні ключі:

Аліса вибирає секретне число $k \in Z$;

Боб вибирає секретне число $l \in Z$.

Передача даних для обчислення загального ключа здійснюється наступним чином. Аліса обчислює нормальну форму $nf(g^k)$ елементу g^k і посилає її Бобу, Боб аналогічно обчислює $nf(g^l)$ і посилає її Алісі:

Надалі для скорочення запису позначення nf( ) опускається, але мається на увазі оскільки відкритий ключ являє собою несверхзростаючу (нормальну) послідовність (наприклад, в якості функції нормалізації використовується mod p).

Скорочено будемо записувати

$A: g^k \rightarrow \leftarrow g^l :B$

Скорочена запис обчислення загального ключа:

$$A: \left(g^l\right)^k = K = g^{k \cdot l} = \left(g^k\right)^l :B$$

При цьому висувалися дві основні вимоги до платформи і параметрів протоколу. Перша вимога – помірні обчислювальні витрати при використанні протоколу, яке забезпечується за рахунок такого конструктивного завдання групи G , яке дає можливість ефективного (тобто з невеликими обчислювальними витратами) проводити обчислення групових операцій, нормальних форм елементів і групових операцій над нормальними формами.

Друга вимога – забезпечення стійкості за рахунок складності обчислення по (нормальній формі) g^k степеню k обраного елементу g , тобто проблеми дискретного логарифмування.

Найбільш ефективні алгоритми криптографічного аналізу класичної платформи мають субекспоненціальну часову складність за рахунок використання факторної бази. В роботі таких алгоритмів розрізняються два основних етапи. На першому, підготовчому, формується факторна база та на її основі генерується система лінійних рівнянь в кільце Z_{p-1}. Вид факторної бази (множина простих чисел багаточленів, що не приводяться, або інших об'єктів) і способи отримання матриці системи залежать від обраного алгоритму. На другому етапі (який є загальним для цих алгоритмів) отримуються рішення цієї системи.

Еліптична платформа над полем F_q з елементом, що породжує $q = p^r$, де p – просте число будувалася за наступною схемою.

Відкриті дані:

E: $y^2 + x \cdot y = x^3 + x^2 + 1$ – еліптична крива над полем, G(E) – відповідна група, P – фіксована точка еліптичної кривої (елемент $P \in G(E)$, що має великій порядок $|P|$).

Особисті секретні ключі:

Аліса вибирає секретне число $k \in Z$;

Боб вибирає секретне число $l \in Z$.

Передача даних:

A: $kP \rightarrow \leftarrow lP$:B

Обчислення загального ключа:

A: $k(lP) = klP = lkP = l(kP)$:B

Ефективність обчислень з нормальними формами забезпечується відомими формулами додавання в $G(E)$. Криптографічна стійкість базується на проблеми дискретного логарифмування в групі точок загальної еліптичної кривої (Elliptic Curve Discrete Logarithm Problem (ECDLP)).

Побудувати субекспоненціальні алгоритми на тих принципах, використання яких призвело до успіху у вирішення задачі дискретного логарифмування в полі (кольці), неможливо, оскільки для еліптичних кривих не знайдено факторної бази (немає аналогів простих чисел або багаточленів, що не приводяться). Тому складність рішення ECDLP на класичному комп'ютері є експоненціальною визначається складністю λ-методу Полларду.

Як показав огляд [2], DLP та ECDLP при використанні квантових комп'ютерів мають лише поліноміальну залежність складності від довжини ключа. Цей факт робить актуальним розвиток алгоритмів ЕЦП, протоколів відкритого розподілу ключів і відкритого шифрування, які б забезпечили потрібну стійкість в разі створення квантового комп'ютера з достатньою кількістю елементів пам'яті (кубіт). Тому для забезпечення достатньої стійкості алгоритмів і протоколів двохключової криптографії потрібно покласти в основу їх стійкості обчислювальне важку задачу, для якої складність вирішення мала б, як мінімум, субекспоненціальну залежність від довжини ключа, як для класичних, так і для квантових комп'ютерів.

Так Агентство національної безпеки ЗША вже поновило свої рекомендації, що до використання алгоритмів шифрування даних у зв'язку з необхідністю поступового переходу до криптографічних методів, які є стійкими до злому з використанням квантових комп'ютерів. Інженери Google вже працюють над змінами в браузері Chrome, завдяки яким стане можливо використання так званих постквантових алгоритмів.

В кінці 20-го століття відбувається поширення протоколу Діффі-Хеллмана на некомутативні групи і пропонуються нові платформи. В якості групи G пропонувалися матричні групи над полями [3; 4], модульні групи (modular group) [5], групи B_n кос Артіна [6], поліциклічні групи (група, що використовує поліциклічний ряд, тобто субнормальний ряд з циклічними факторами) [7], та ін.

Великий інтерес до матричних груп обумовлений тим, що вони добре підходять для впровадження і роботи з ними в криптосистемах. Так групи кос містять багато великих абелевих (комутативних) підгруп, що дає широку можливість вибору ключових просторів. Крім того, групи кос наділені нормальними формами записи елементів, операції з якими досить ефективні. Те ж саме можна сказати і про поліциклічні та інші матричні групи.

Криптосистема на групах кос, є окремим випадком систем, якої її автори далі назву MOR – системам [8; 9]. Стійкість цих систем заснована на проблемі спряженості (Conjugacy search problems (CSP)). Можливі атаки на групи кос були запропоновані вже в [10]. Однак в роботі [11] автори вважають, що встановлення певних обмежень на ключі, дозволять зробити неефективними відомі атаки і вважають за необхідне докласти зусиль для побудови доказовою стійких криптоалгоритмів на основі груп кос або ж для надання доказів того, що побудова подібних крипто алгоритмів неможливо. Тому становить інтерес отримати такі докази.

В [12] запропонована схема відкритого розподілу ключів, заснована на комбінації двох проблем теорії груп: проблеми спряженості (Conjugacy search problems (CSP)) і проблеми дискретного логарифмування (Discrete logarithm problem (DLP)). Коротко схема побудови запропонована в [12] записується наступним чином.

G – некомутативна група, $G1$ – її комутативна підгрупа. Відкритим ключем є елемент $\theta \in G$ та матричне представлення ϕ групи G над конечним полем F.

Особисті секретні ключі:

Аліса вибирає випадково секретні елементи $\alpha \in G1$ та $r \in N$;

Боб вибирає випадково секретні елементи $\beta \in G1$ та $s \in N$.

A: $AQ^rA^{-1} \rightarrow \leftarrow BQ^sB^{-1}$:B

де $A = \phi(\alpha)$, $Q = \phi(\theta)$, $B = \phi(\beta)$.

Обчислення загального ключа:

A: $A\left(BQ^sB^{-1}\right)^r A^{-1} = K = B\left(AQ^rA^{-1}\right)^s B^{-1}$:B

Ряд схем аналогічних схемі наведеної в [12] пропонується в [13–16]. Їх особливістю є вибір некомутативних груп, які визначаються на векторах лінійних просторів невеликої розмірності n над кінцевим полем. Автор [13] припускає, що задача знаходження логарифма в такої некомутативної групі має експонентну складність.

Мета статті полягає в огляді алгоритмів криптоаналізу систем відкритого розподілу ключів типу Діффі-Хеллмана, які засновані на некомутативних групах. Формування пропозицій щодо їх використання.

Основна частина

Розглянемо деякі аналоги класичного протоколу Діффі-Хеллмана, які використовуються в криптографії, що базується на теорії груп і в якій в якості платформ побудови систем, схем і протоколів розглядаються абстрактні матричні групи, як скінчені, так і нескінченні. Матричні групи стали використовуватися в криптографії вже в [6]. В якості відкритих даних в [6] використовувалися: G – група, U_1 и U_2 такі, що $[U_1,U_2]=1$ – кінцеві поелементно перестановочні підмножини G; $A=gp(U_1)$; $B=gp(U_2)$; фіксований елемент $g\in G$.

Короткий запис алгоритму має наступний вигляд.

Аліса вибирає секретний елемент $a\in A$, обчислює g^a и передає її Бобу. Боб надходить аналогічно щодо $b\in B$, g^b.

$A: g^a \rightarrow \leftarrow g^b : B$

Обчислення загального ключа:

$A: (g^b)^a = g^{ab} = g^{ba} = (g^a)^b : B$

В оригінальній версії в якості G пропонувалася група кос Артіна B_n на n нитках. В [17] автор, використовуючи вкладення Крамера-Лоуренса $\phi: B_n \rightarrow GL_{n\cdot(n-1)/2}\left(Z\left[t^{\pm1},q^{\pm1}\right]\right)$, побудував точне матричне зображення для будь-якої групи кос, коефіцієнтами матриць якого є поліноми від двох змінних. З класичних теорем теорії чисел випливає, що існує пара реальних чисел, при підстановці яких замість змінних ми отримаємо точне матричне зображення з реальними коефіцієнтами. Отже, все групи кіс B_n лінійні. За аналогією з підходами, які використовують факторну базу для криптографічного аналізу в цьому випадку достатньо знайти рішення системи лінійних рівнянь. Крім того, в [18] зазначено, що прообрази елементів $\phi(B_n)$ обчислюються ефективно. Значить, існує поліноміальний алгоритм обчислення по $\phi(K)$ ключа K за відкритими даними.

Алгоритм, запропонований в [18], складається з трьох основних кроків.

1. Використовуючи вкладення: $\phi: B_n \rightarrow GL_{n\cdot(n-1)/2}\left(Z\left[t^{\pm1},q^{\pm1}\right]\right)$ Лоуренса-Крамера групи кос в групу матриць, обчислити образи $\phi(g)$, $\phi\left(a^{-1}\cdot g\cdot a\right)$.

2. Знайти спряжений елемент $\phi(a)$ в матричної групі такий, що $\phi(a)^{-1}\cdot\phi(g)\cdot\phi(a)=\phi(g^a)$.

3. Знайти прообраз $a\in B_n$ елементу $\phi(a)$.

Однак при реалізації цього алгоритму виникають дві істотні труднощі, які роблять такий підхід обчислювальне нереальним.

По-перше, пряме застосування алгоритму Гауса призводить до великих (близько 2^{2^n}) коефіцієнтів.

По-друге, рішення слід шукати в образі $\phi(B_n)$ та матриця $\phi(a)$ повинна бути оборотною.

Тому було запропоновано наступний алгоритм, в якому замість пошуку спряженого елементу здійснюється знаходження загального ключа.

1. Використовуючи вкладення: $\phi: B_n \rightarrow GL_{n\cdot(n-1)/2}\left(Z\left[t^{\pm1},q^{\pm1}\right]\right)$ Лоуренса-Крамера групи кос в групу матриць, обчислити образи $\phi(g)$, $\phi(g^a)$, $\phi(g^b)$.

2. Вирішити рівняння $\phi(g^a)\cdot Y = Y\cdot\phi(g)$ та $\phi(\sigma_i)\cdot Y = Y\cdot\phi(\sigma_i)$, де σ_i – породжувальні елементи підгрупи B.

3. Знайти прообраз $a\in B_n$ елементу $\phi(a)$.

Однак і при реалізації цього алгоритму ми зустрічаємо подібні труднощі. Велике число рівнянь і невідомих. Якщо рішення, що знайдено $\phi(a)$, необоротне, потрібно повернутися і знову запустити процес його пошуку. Таким чином, цей алгоритм імовірнісний, час обчислення хоч і поліноміальний, але нереальний.

В [19] описаний аналіз методом лінійного розкладання криптографічних систем, схем і протоколів, заснованих на групах.

Для короткого опису методу лінійного розкладу використовуємо такі позначення.

V – простір кінцевої розмірності над полем F з базисом $B=\{v_1,\dots v_r\}$. $End(V)$ – напівгрупа ендоморфізмів простору V. Елементи $v\in V$ – вектори відповідно базису B. Ендоморфізми $a\in End(V)$ матриці відносно B, v^a – образ v відносно a.

Для підмножин $W\subseteq V$ и $A\subseteq End(V)$ позначимо $W^A=\left\{w^a \mid w\in W, a\in A\right\}$.

Вважаємо: $Sp(W)$ – підпростір V, породжене W, $\langle A\rangle$ – підмоноїд, породжений A в $End(V)$.

Припускаємо, що елементи поля F задані в деякій конструктивній формі, причому визначений розмір їх завдання.

Операції в F ефективні, представляються за поліноміальний час від розмірів нормальних форм.

Для $a\in F$ через $|a|$ позначається його розмір.

Для $v=(\alpha_1,\dots\alpha_r)\in V$ вважаємо $|v|=\max|\alpha_i|$.

Для матриці $a=(\alpha_{i,j})\in End(V)$ вважаємо

$|a| = \max\{|\alpha_{i,j}|\}$.

Основна лема методу стверджує що існує алгоритм знаходження для даних скінченних підмножин $W \subseteq V$ и $U \subseteq End(V)$ базису підпростору $Sp(W^{\langle U\rangle})$ у вигляді $w_1^{a_1},\dots w_t^{a_t}$, де $w_i \in W$ і a_i – добуток елементів з U. Число використаних операцій над елементами поля поліноміальне по $r = \dim_F V$ та кількостей елементів W та U.

Доказом цієї леми служить наступний алгоритм знаходження базису підпростору $Sp(W^{\langle U\rangle})$:

1. Методом винятків Гауса знаходимо максимальне лінійно незалежне (л.н.) підмножину L_0 для W. Зазначимо, що $Sp(L_0^{\langle U\rangle}) = Sp(W^{\langle U\rangle})$.

2. Додаємо до L_0 елементи v^a; $v \in L_0$; $a \in U$; перевіряючи кожного разу л.н. отриманої підмножини. Таким чином буде побудовано максимальне л.н. підмножина L_1 підмножини $L_0 \cup L_0^U$, що розширює L_0. Зазначимо, що $Sp(L_0^{\langle U\rangle}) = Sp(L_1^{\langle U\rangle})$, и елементи в L_1 мають форму w чи w^a, де $w \in W$ та $a \in U$. Тому, якщо $L_0 = L_1$, то L_0 – базис в $Sp(W^{\langle U\rangle})$.

3. Якщо $L_0 \neq L_1$, то повторюємо процедуру для використовуючи замість L_0 підмножину L_1 и повертаючись до кроку №2 цього алгоритму знаходимо максимальне л.н. підмножину L_2 підмножини $L_1 \cup L_1^U$, що розширює L_1. Будуємо $L_0 < L_1 < L_2 \dots < L_i$ в V. Так як розмірність r простору V скінченна, послідовність стабілізується на $i \le r$. Тоді L_i – базис в $Sp(W^{\langle U\rangle})$, який складається з елементів необхідного виду.

При оцінці складності методу лінійного розкладання врахуємо, що число операцій в методі виключення Гауса для матриці розміру $n \times r$ оцінюється як $O(n^2 \cdot r)$. Отже, потрібно не більше $O(n^2 \cdot r)$ кроків для побудови L_0 з W, де $n = |W|$ – число елементів W. Так як $L_j \le r$ для любого j, то знаходження L_{j+1} використовує матрицю відповідну $L_j \cup L_j^U$ розміру не більше $r + r|U|$. Таким чином, Верхня межа оцінки складності $O\left(r^3|U|^2\right)$. Так як число ітерацій $i \le r$, то алгоритм знаходження базису підпростору $Sp(W^{\langle U\rangle})$ працює за поліноміальний час $O\left(r^3|U|^2 + r|W|^2\right)$.

Таким чином, загальний алгоритм по методу лінійного розкладу для криптоаналізу протоколів запропонованих в [6] буде мати наступний вигляд.

1. З U_1, та V з використанням наведеного вище алгоритму знаходження базису підпростору, знаходимо базис $v^{a_1}, v^{a_2}, \dots, v^{a_t}$; $a_i \in A$; простору $Sp(v^A)$.

Методом виключення Гаусса розкладаємо g^a по цьому базису:

$$g^a = \sum_{i=1}^{t} \alpha_i \cdot g^{a_i}, \text{ де } \alpha_i \in F.$$

2. Знаходимо ключ $g^{a\cdot b}$:

$$g^{a\cdot b} = \left(g^a\right)^b = \left(\sum_{i=1}^{t} \alpha_i \cdot g^{a_i}\right)^b =$$

$$= \sum_{i=1}^{t} \alpha_i \cdot g^{a_i \cdot b} = \sum_{i=1}^{t} \alpha_i \cdot \left(g^b\right)^{a_i}.$$

У цьому методі немає необхідності в знаходженні ні a, ні b; щоб обчислити ключ $g^{a\cdot b}$. Крім того, немає необхідності знати U_2. Мало того, що для деякого $b \in End(V)$ маємо $\forall(u \in U1)\ ub = bu$. Алгоритм методу повністю детермінований. Він дозволяє використовувати значно менше число рівнянь в порівнянні з раніше розглянутими алгоритмами. Він ефективний для всіх платформ, які використовують лінійні групи або допускають (як у випадку з групами кос) вкладення в лінійні групи.

При цьому якщо група нелінійна, то мистецтво криптоаналізу є в її вкладанні и в матричну групу з найменшим числом параметрів такого вкладання.

Вже в [20] було зазначено, одним з найбільш ефективним способом криптоаналізу є приведення матриці g до жорданової формі: $tgt^{-1} = J(g)$. Матриця $J(g)$ – клітково діагональна, в якої по діагоналі розташовані клітки Жордана:

$$J(g) = J_{r_1}(\lambda_1) \oplus \dots \oplus J_{r_t}(\lambda_t);\ \sum_{i=1}^{t} r_i = n.$$

Діагональні елементи $\lambda_1, \dots, \lambda_t$ (не обов'язково різні) – корні (в розширеннях, що підходять $F_{q^{n_i}}$ основного поля) характеристичного рівняння матриці g: $p_g(x) = |g - \lambda \cdot E| = (x-\lambda_1)^{r_1} \dots (x-\lambda_t)^{r_t} = 0$.

Алгоритм обчислення жорданової формі матриці має наступні кроки.

1. Алгоритмом Гессенберга знайти характеристичний багаточлен $p_g(x)$.

2. Алгоритмом Бен-Ора розкласти характеристичний багаточлен в добуток степенів різних бага-

точлен, що не розкладуються над F_q:

$$p_g(x) = f_1^{e_1} \dots f_s^{e_s},$$

де f_i – багаточлен степені n_i, що не розкладуються. Нехай корни f_i в $F_{q^{n_i}}$ дорівнюють $\alpha_{i,j}$ при $1 \le j \le n_i$. Можливо визначити

$$F_{q^{n_i}} = F_q[x] / \text{ideal}(f_i(x)).$$

Тоді $\alpha_{i,1} = x$ та $\alpha_{i,j} = x^{q^{i-1}} \bmod(f_i(x))$ при $2 \le j \le n_i$.

3. Визначити розміри всіх кліток Жордана.

4. Получити форму Жордана: $J(g) = J_1 \oplus \dots \oplus J_t$.

Тоді матриці g^k та g^l можуть бути визначені відповідними степенями цієї жорданової форми. У випадку, якщо розмір хоча б однієї клітки жорданової форми матриці g виявляється більш одиниці, а степені k и l були менш характеристики основного поля, ці числа знаходяться дуже просто. У випадку, якщо матриця g мала діагональну жорданову форму обчислення параметрів k и l зводилось до рішення кратних проблем дискретного логарифма для відповідних друг другу наборів діагональних елементів отриманих матриць.

В [21] на основі [20] автор запропонував ефективний криптоаналіз, який може бути застосований до всіх систем з некомутативними групами, що запропоновані в [12–16] на 4-мірних векторах над полем Z_p. Такій підхід ефективний тому, що в усіх варіантах, що описані в [12–16], використовують групи, що ізоморфні підходящим групам матриць розмірів 4×4 над полем Z_p, причому характеристичні багаточлени матриць, що використовуються, можна розкласти над полем Z_p в добуток багаточленів не вище другої степені. Друга степінь обумовлена тим, що в деяких випадках матриця g не має жорданової форми над Z_p, однак вона буде мати жорданову форму над розширенням F другої степені поля Z_p.

Оскільки для еліптичних кривих не знайдено факторної бази (немає аналогів простих чисел або багаточленів, що не приводяться) то можна припустити, що наведені вище алгоритмі кріптааналізу будуть не ефективні якщо буде запропонована схема відкритого розподілу ключів, яка заснована на комбінації двох проблем теорії груп: проблеми спряженості (Conjugacy search problems (CSP)) і проблеми дискретного логарифмування в групі точок еліптичної кривої (Elliptic Curve Discrete Logarithm Problem (ECDLP)).

Висновки

В статті розглянути алгоритмів криптоаналізу систем відкритого розподілу ключів типу Диффи-Хелмана, які засновані на некомутативних групах.

Проведений огляд показав, що як і у випадку з комутативними групами, найбільшу ефективність при виконанні криптоаналізу на класичних комп'ютерах показують методи, що засновані на розкладені по деякої базі (базису) з наступним рішенням системи лінійних рівнянь. Для комутативних груп ця база мала назву факторної та складалася або з простих чисел або з багаточленів, що не приводяться.

Для некомутативних груп найбілішу ефективність показують дві групи методів.

Перша група методів заснована на приведенні матриці g до жорданової формі за рахунок використання характеристичних чисел.

Друга група методів заснована на знаходження базису підпростору $Sp(W^{\langle U \rangle})$ для метода лінійного розкладання.

Доцільно нові протоколи для некомутативних груп перевіряти на стійкість до зазначених методів криптоаналізу.

Доцільно провести дослідження щодо схеми відкритого розподілу ключів, яка заснована на комбінації двох проблем теорії груп: проблеми спряженості (Conjugacy search problems (CSP)) і проблеми дискретного логарифмування в групі точок еліптичної кривої (Elliptic Curve Discrete Logarithm Problem (ECDLP)).

Список літератури

1. Diffie W. New directions in cryptography / W. Diffie, M.E. Hellman // IEEE Trans. Information Theory/ – 1976. – Vol.22. – P. 644-654.

2. Бурковський В.С. Огляд можливостей квантового криптоаналізу та криптографічних платформ, що є стійкими до нього та можуть бути основою для систем електронного цифрового підпису / В.С. Бурковський // Наука і техніка Повітряних Сил Збройних Сил України. – Х.: ХНУПС, 2016. – №3(24). – С. 119-126.

3. Сидельников В.М. Системы открытого распределения ключей на основе некоммутативных полугрупп / В.М. Сидельников, М.А. Черепнев, В.В. Ященко // Докл. РАН. – 1993. – Том. 332, №5. – С. 566-567.

4. Сидельъников В.М. Системы распределения ключей на основе «экспоненциального представления» линейной группы GLn (Fp) / В.М. Сидельников // Проблемы передачи информации. – 1994. – Том 30, Вип. 4. – С. 25-32.

5. Yamamura A. Public-key cryptosystems using the modular group / A. Yamamura // In: Public Key Cryptography. Springer Berlin Heidelberg, 1998, – P.203-216. (Ser. Lecture Notes in Computer Science. – Vol. 1431). DOI: 10.1007/BFb0054026.

6. Ko K.H. New Public-Key Cryptosystem Using Braid Groups / K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang, C. Park // Advances in Cryptology - CRYPTO 2000 / Lecture

Notes and Computer Science. Springer-Verlag, 2000. – Vol. 1880. – P. 166-184.

7. Shpilrain V. An authentication scheme based on the twisted conjugacy problem / V. Shpilrain, A. Ushakov // ACNS'2008. LNCS. 2008. – Vol. 5037. – P. 366-372.

8. Paeng S.H. New public key cryptosystem using finite non abelian groups / S.H. Paeng, K.C. Ha, J.H. Kim, S. Chee, C. Park // CRYPTO'2001, Lect. Notes Comput. Sci., 2001. – Vol. 2139. – P. 470-485.

9. Paeng S.H. Improved public key cryptosystem using finite non abelian groups [Електронний ресурс] / S.H. Paeng, D. Kwon, K.C. Ha, J.H. Kim. – Режим доступу до ресурсу: http://eprint.iacr.org/2001/066.

10. Myasnikov A. A practical attack on a braid group based cryptographic protocol / A. Myasnikov, V. Shpilrain, A. Ushakov // Advances in Cryptology - CRYPTO 2005 / Lecture Notes and Computer Science. – Springer-Verlag, 2005. – Vol. 3621. – P. 86-96.

11. Паршина Д.А. Анализ криптографических систем в группах КОС / Д.А. Паршина, И.А. Митяева, И.Д. Горбенко // Прикладная радиоэлектроника. – 2012. – Том 11, №2. – С. 210-215.

12. Sakalauskas E. Key agreement protocol (KAP) using conjugacy and discrete logarith ms problems in group representation level / E. Sakalauskas, P. Tvarijonas, A. Raulynaitis // Informatica. – 2007. – Vol. 18, №1. – P. 115-124.

13. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи / Н.А. Молдовян. – СПБ.: БХВ-Петербург. 2010. – 304с.: ил. – (Учебное пособие). ISBN 978-5-9775-0585-7.

14. Молдовян Д.Н. Задание некоммутативных конечных групп векторов для синтеза алгоритмов цифровой подписи / Д.Н. Молдовян, А.И. Куприянов, А.А. Костина, Д.В. Захаров // Вопросы защиты информации. – 2009. – № 4. – С. 12-18.

15. Дернова Е.С. Конечные группы матриц как примитив алгоритмов цифровой подписи / Е.С. Дернова, А.А. Костина, Н.А. Молдовян // Вопросы защиты информации. – 2008. – № 3(82). – С. 8-12.

16. Молдовян Д.Н. Задание некоммутативных конечных групп векторов для синтеза алгоритмов цифровой подписи / Д.Н. Молдовян, А.И. Куприянов, А.А. Костина, Д.В. Захаров // Вопросы защиты информации. – 2009. – № 4. – С. 12-18.

17. Мантуров В.О. Экскурс в теорию кос / В.О. Мантуров // Сборник серии «Математическое просвещение». – М.: МЦНМО, 2010. – Серия 3, № 14. – 288 с.

18. Cheon J. A polynomial time algorithm for the braid Diffie-Hellman conjugacy problem / J. Cheon, B. Jun // Proc. CRYPTO2003, LNCS, 2729, Springer-Verlag, 2003. – P. 212-215.

19. Романьков В.А. Алгебраическая криптография: монография / В.А. Романьков. – Омск : ОмГУ, 2013. – 136 с.

20. Menezes A.J. The discrete logarithm problem in GL(n; q) / A.J. Menezes, Y.-H. Wu // Ars Combinatoria. – 1997. – Vol. 47. – P. 23-32.

21. Глухов М.М. К анализу некоторых систем открытого распределения ключей, основанных на неабелевых группах / М.М. Глухов // Математические вопросы криптографии. – 2010. – Том 1, №4. – С. 5-22.

Надійшла до редколегії 31.10.2016

Рецензент: д-р техн. наук ст. наук. співробітник В.О. Василець, Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків.

ОБЗОР АЛГОРИТМОВ КРИПТОАНАЛИЗА СИСТЕМ ОТКРЫТОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ТИПА ДИФФИ-ХЕЛЛМАНА, КОТОРЫЕ ОСНОВАНЫ НА НЕ КОММУТАТИВНЫХ ГРУППАХ

В.С. Бурковский

Рассмотрены алгоритмы криптоанализа систем открытого распределения ключей типа Диффи-Хелмана, которые основаны на не коммутативных группах.

***Ключевые слова**: криптосистема Діффі-Хеллмана, криптоанализ, некоммутативные группы, группы кос, постквантовая криптографическая платформа.*

OVERVIEW CRYPTANALYSIS ALGORITHMS OF PUBLIC DISTRIBUTION KEYS SYSTEMS SUCH AS THE DIFFIE-HELLMAN, WHICH ARE BASED ON NON-COMMUTATIVE GROUPS

V.S. Burkovsky

Overview cryptanalysis algorithms of public distribution keys systems such as the Diffie-Hellman, which are based on non-commutative groups.

***Keywords**: Diffie-Hellman cryptosystem, cryptanalysis, noncommutative group, braid groups, post quantum cryptographic platform.*