УДК 004.056

Фесенко А. В.

ЗВЕДЕННЯ ЗАДАЧІ ОБЕРНЕННЯ КУСКОВО-ЛІНІЙНОГО ВІДОБРАЖЕННЯ ДО ЗАДАЧІ ПРО ПРИХОВАНУ ДІЮ НА ТОРСОР НАД АБЕЛЕВОЮ ГРУПОЮ

У цій роботі, використовуючи загальні методи аналізу складності задачі обернення локально комутативних відображень, досліджено кусково-лінійне відображення. Як результат, задачу обернення кусково-лінійного відображення, яке використовується для побудови асиметричних криптосистем, зведено до часткового випадку задачі про приховану дію на торсор над абелевою групою, що має ефективне рішення в квантовій моделі обчислень.

Ключові слова: одностороння функція, локально комутативне відображення, квантова модель обчислень.

Поняття односторонньої функції є одним з ключових у сучасній криптографії. Хоча існування таких функцій теоретично не доведено, проте сформовано цілий набір претендентів, що витримали перевірку часом. Саме ці функції є необхідною умовою стійкості багатьох криптографічних систем. Значний поштовх у розвитку квантової моделі обчислень відбувся 1994 року після відкриття ефективного алгоритму Шора [7] для факторизації цілих чисел на квантовому комп'ютері завдяки його можливому застосуванню для атак на сучасні асиметричні криптосистеми, оскільки на складності задач факторизації та дискретного логарифму базується абсолютна більшість існуючих асиметричних криптографічних систем. У зв'язку з цим, а також з огляду на останні технологічні досягнення при побудові досить потужного квантового комп'ютера, стає актуальним пошук нових односторонніх функцій і примітивів, які будуть стійкими навіть до атак із використанням квантового комп'ютера.

У праці [3] вперше представлено нову властивість локальної комутативності для симетричних шифрів, відображень спеціального виду та підгруп перестановок. Використовуючи цю властивість, показано, як можна будувати нові односторонні функції на основі симетричних шифрів, що мають шанс бути стійкими в квантовій моделі обчислень.

У квантовій моделі обчислень розглядаються в першу чергу саме алгебраїчні задачі, тому для аналізу постквантової стійкості таких функцій є необхідними методи зведення алгебраїчних моделей шифрів до конструкцій, які використовуються у квантовій моделі обчислень (алгебраїчні задачі про приховану підгрупу, зсув тощо). Нині такі методи лише починають з'являтися, і найбільш загальний підхід запропоновано у праці [4], в якій поширено властивість локальної комутативності на дію груп, а також розроблено методи зведення довільного відображення.

Постановка задачі дослідження

Наведемо основні означення та твердження з [3; 4], що будуть використовуватися при аналізі та побудові зведення.

Означення 1. *Відображення* $E: K \times X \to X$ *назвемо комутативним, якщо для* $\forall k_1, k_2 \in K$, $\forall x \in X$ *виконується співвідношення* $E_{k_2}(E_{k_1}(x)) = E_{k_1}(E_{k_2}(x))$.

Означення 2. *Відображення* $E: K \times X \to X$ *назвемо локально комутативним, якщо існує така підмножина* $X_c \subseteq X$, $X_c \neq \emptyset$, *що для* $\forall k_1, k_2 \in K$, $\forall x \in X_c$ *виконується співвідношення* $E_{k_2}(E_{k_1}(x)) = E_{k_1}(E_{k_2}(x))$. *Множину* X_c *будемо називати множиною комутативності відповідного відображення. Позначимо через* C_L *клас локально комутативних відображень виду* $E: K \times X \to X$, *для яких існує ефективна процедура обчислення результату.*

Зауваження. Множини K і X мають бути скінченними, оскільки, по-перше, це відповідає більшості практичних реалізацій, а по-друге – є необхідним для аналізу оцінок складності алгоритмів. Відразу відзначимо, що в роботі [4] розглядається лише клас відображень $E: K \times X \to X$, для яких за будь-якого фіксованого значення $k \in K$ відображення $E(k,\cdot): X \to X$ є бієкцією (або автоморфізмом множини X). Саме до такого класу відображень призводить узагальнене поняття симетричного шифру. Для скороченого

позначення локально комутативного відображення $E: K \times X \to X$ із множиною комутативності $X_c \subseteq X$, $X_c \neq \phi$, будемо використовувати позначення $E_{[K,X;X_c]}$, а якщо немає необхідності точно вказувати множину комутативності, або вона відома з контексту, то також використаємо позначення $E_{[K,X]}$.

У праці [4] досліджується складність задачі обернення локально комутативного відображення $E_{[K,X]}$, тобто для заданого відображення $E_{[K,X]} \in C_L$ та заданих значень $x_0, x_1 \in X$ знайти значення $k \in K$ таке, що $E_k(x_0) = x_1$.

У результаті проведеного аналізу було сформовано набір припущень, присутніх у більшості випадків, і які є необхідними для проведення ефективного зведення задачі обернення таких відображень до алгебраїчних задач.

Припущення 1. *З опису відображення $E_{[K,X]} \in C_L$ можна отримати його характеристичну групу $G^{char}\left(E_{[K,X]}\right)$ (наприклад, твірні елементи групи), результат дії якої на множину X збігається з результатами відображення $E_{[K,X]}$ та його комбінацій.*

Припущення 2. *З опису відображення $E_{[K,X;X_c]} \in C_L$ та довільного значення $x \in X_c$ можна отримати його характеристичну групу (яка буде абелевою) відносно елемента x як факторгрупу $G^{char}\left(E_{[K,X;X_c]}, x\right) = G^{char}\left(E_{[K,X]}\right) / G_x^{char}\left(E_{[K,X]}\right)$ (наприклад, твірні елементи групи), де G_x^{char} – підгрупа стабілізатор елемента x.*

Припущення 3. *Кількість різних орбіт $\omega\left(E_{[K,X]}\right)$ дії характеристичної групи $G^{char}\left(E_{[K,X]}\right)$ дорівнює 1, або за заданим значенням $x \in X_c$ існує ефективний алгоритм виокремлення елементів орбіти Gx.*

Перевірка виконання наведених припущень відносно конкретного відображення розглядається як алгоритм аналізу відповідного локально комутативного відображення [4]. У випадку його ефективного застосування задачу обернення відповідного відображення можна звести до однієї з алгебраїчних задач.

Задача 1. ***Задача про приховану дію на торсор над абелевою групою.***

Постановка задачі. Нехай задано множину твірних елементів абелевої групи G і деякий торсор X над групою G. За заданими значеннями $x_0, x_1 \in X$ необхідно знайти такий елемент $g \in G$, що $gx_0 = x_1$.

Аналогічно до проблеми Діффі-Хеллмана, іноді достатньо мати результат дії шуканого елемента g групи G на довільний елемент $x \in X$, не знаючи g в явному вигляді.

Задача 2. ***Про прихований елемент торсора над абелевою групою.***

Постановка задачі. Нехай задано множину твірних елементів абелевої групи G і деякий торсор X над групою G. За заданими значеннями $x_0, x_1, x_2 \in X$ необхідно знайти такий елемент $x_3 \in X$, що коли $gx_0 = x_1$ для деякого $g \in G$, то $gx_2 = x_3$.

У випадку порушення припущення 3 було також запропоновано більш узагальнені задачі [4]: про приховану дію абелевої групи та прихований результат дії абелевої групи відповідно.

Зауваження. При виконанні оцінки складності обчислень для пошуку ефективних алгоритмів розв'язку для задач вважаємо, що алгоритм обчислення результата дії довільного елемента $g \in G$ на довільний елемент $x \in X$ має складність, обмежену деяким поліномом від значення $\log|X|$, тобто є ефективним відносно розмірів задачі.

У праці [4] представлено застосування такого аналізу до комутативного симетричного шифру Поліга-Хеллмана. А в роботі [6] показано зведення задач 1 і 2 до відомих задач у квантовій моделі обчислень, що дало змогу представити їхні часткові ефективні рішення.

З огляду на це, досить актуальним є поширення застосування таких методів до інших шифрів та відображень з метою вдосконалення методів та пошуку нових стійких екземплярів односторонніх функцій. У цій роботі об'єктом дослідження є криптосистема, що використовує кусково-лінійне відображення, яке використовується в системах детермінованого хаосу [1]. Цю систему нещодавно запропоновано, її основною частиною є кусково-лінійне відображення, яке є частково комутативним, що повністю відповідає нашим вимогам. Отже, спробуємо використати запропоновані в [4] методи аналізу і звести задачу обернення відповідного відображення до алгебраїчних задач 1–2.

Криптосистема на основі кусково-лінійного відображення з відсіканням молодших розрядів

Нові результати в більшості випадків отримують на стику кількох наукових областей, коли теоретична модель, яка вивчається в одній предметній області, переноситься в іншу та проявляє нові властивості, котрі можна ефективно використовувати. Зокрема, постійно робляться спроби знайти можливе застосування нових результатів із різних наукових напрямів у криптографії.

Одним із таких напрямів останнім часом є теорія детермінованого хаосу. Якоюсь мірою хаотичні та криптографічні системи дійсно взаємопов'язані навіть на концептуальному рівні. Як у криптографії, так і в нелінійній динаміці здійснюється нелінійне перетворювання інформації. Звичайно, такий взаємозв'язок між об'єктами вивчення не зміг залишитися непоміченим. Так, почали створюватися та вивчатися криптографічні примітиви, що використовують об'єкти хаотичної динаміки.

На жаль, у нашій країні цей напрям ще не отримав належної уваги криптографічного співтовариства, тому будь-які публікації в цій області викликають неабиякий інтерес.

Опис досліджуваної в цьому підрозділі криптосистеми, на яку будемо посилатися як на криптосистему, що використовує відсікання молодших розрядів, повністю взято з [1], включає такі етапи.

Криптосистема 1 (з відсіканням молодших розрядів).

Генерування ключів: нехай відоме достатньо велике значення $l_m \in N$, що описує рівень стійкості системи. Формування ключів користувачем A включає такі етапи:

1) генерування простого числа $2^{2l_m+2} < N < 2^{2l_m+3}$;
2) знаходження нестійкої нерухомої точки X_0 кусково-лінійного відображення $T_N(x) = \frac{1}{\pi}\arccos(\cos(N\pi x))$ порядку N на інтервалі $(2^{-l_m-1}, 2^{-l_m}]$, тобто $X_0 = T_N(X_0)$. Причому значення X_0 задається $4(l_m+1)$ бітами після коми;
3) генерування натурального числа Q, значення якого є близьким до $\sqrt{N}$, тобто $Q \approx 2^{l_m+1}$;
4) обчислення значення $P = N / Q$;
5) обчислення та опублікування відкритого ключа $Y = T_P(X_0)$. Причому значення Y задається $3(l_m+1)$ бітами після коми та повинно належати інтервалу $(2/3 - 0.25, 2/3 + 0.25)$. Якщо умова $Y \in (2/3 - 0.25, 2/3 + 0.25)$ не виконується, генеруються нові значення Q і P та процедура повторюється знову, починаючи з п. 3.

Значення X_0, P, Q і N є секретними. Пара значень (X_0, Q) складає секретний ключ користувача A. Значення P і N в подальших обчисленнях не використовуються.

Шифрування: для шифрування повідомлення M, де $M \in N$ і $M < 2^{l_m}$, користувач $Б$ діє таким чином:

1) отримує відкритий ключ Y користувача A.
2) Обчислює та відправляє користувачеві A шифр-текст $C = T_M(Y)$. Значення шифр-тексту задається $2l_m + 2$ бітами після коми.

Шифр-текст C є деяким дійсним числом, що належить інтервалу $(0,1)$ визначення відображення, та визначено наближеним раціональним значенням.

Розшифрування: процедура розшифрування повідомлення користувачем A складається з обчислення значення виразу $\hat{M} = \text{round}\left(\frac{T_Q(C)}{X_0}\right)$, яке є оцінкою повідомлення M, а (X_0, Q) є його секретним ключем. Функція round() округляє значення аргументу до найближчого натурального значення. Значення відображення $T_Q(C)$ обчислюється з точністю $l_m + 1$ біт після коми. У випадку коректної роботи криптосистеми та вибраних параметрів присутня тотожність $\hat{M} = M$.

Треба зазначити, що криптосистема 1 є модифікацією іншої криптосистеми на основі кусково-лінійного відображення тих самих авторів [2]. Попередня система відрізнялася тільки простішим представленням даних у вигляді раціональних чисел, що призвело до побудови ефективного алгоритму безключової атаки на повідомлення в роботі [5]. Після цього, з метою покращення стійкості авторами запропоновано модифікацію цієї системи в [1], яка представляє всі параметри та дані у вигляді дійсних чисел з плаваючою комою у двійковій системі числення (стандарт IEEE 754) та фіксованою кількістю знаків після коми.

Застосування розроблених методів аналізу локально комутативних відображень

У цьому підрозділі буде розглянуто можливість використання розроблених у [4] загальних методів аналізу комутативних та локально комутативних відображень у класичній та квантовій моделях обчислень до криптосистеми 1 на основі кусково-лінійного відображення.

Як зазначалося вище, криптосистема 1 має попередника, що відрізняється лише представленням чисел у практичній реалізації. Саме цей перехід від роботи з дійсними числами до практичних реалізацій, які працюють з цілими або раціональними числами, є характерним і найкритичнішим для всіх криптосистем, побудованих на об'єктах детермінованого хаосу. Щоб уникнути подальших спроб модифікацій криптосистеми 1, використаємо довільне однозначне представлення всіх даних криптосистеми у вигляді раціональних чисел (а не тільки відсікання молодших результатів).

Головним елементом такого узагальнення криптосистеми 1 залишається кусково-лінійне відображення, тому можна перейти до аналізу самого відображення та задачі його обернення, абстрагуючись від досліджуваної криптосистеми та використовуючи лише необхідні обмеження на значення, що продиктовані описом криптосистеми.

Твердження 1. *Кусково-лінійне відображення* $T: N \times R \to R$ *є комутативним і* $T_{(k_1 \cdot k_2)}(x) = T_{k_2}(T_{k_1}(x))$ *для* $\forall x \in R$ *і* $\forall k_1, k_2 \in N$.

Доведення.

Неважко перевірити, що для $\forall x \in R$, і $\forall k_1, k_2 \in N$, і кусково-лінійного відображення $T_k(x) = \frac{1}{\pi}\arccos(\cos(k\pi x))$ виконується співвідношення $T_{(k_1 \cdot k_2)}(x) = T_{k_2}(T_{k_1}(x))$, унаслідок чого таке відображення є комутативним відносно параметра $k \in N$, тобто $T_{k_1}(T_{k_2}(x)) = T_{k_2}(T_{k_1}(x)) = T_{(k_1 \cdot k_2)}(x)$ для довільних значень $k_1, k_2 \in N$.

Твердження доведено.

Нехай M – деяке ціле значення, $1 \le M < 2^{l_m}$, і $C = T_M(Y) = \frac{1}{\pi}\arccos(\cos(YM\pi))$, де Y – відкритий ключ деякого користувача. Для двох різних значень $k_1, k_2 \in N$ співвідношення $T_{k_1}(Y) = T_{k_2}(Y)$ виконується тоді і тільки тоді, коли $\begin{bmatrix} k_1 Y = k_2 Y + 2t \\ k_1 Y = -k_2 Y + 2t \end{bmatrix}$ для деякого $t \in N$. Останню сукупність можна переписати у вигляді $\begin{bmatrix} k_1 = k_2 + 2Y^{-1}t \\ k_1 = -k_2 + 2Y^{-1}t \end{bmatrix}$, оскільки $Y \neq 0$ (у цьому випадку не буде однозначного розшифрування). Якщо Y буде ірраціональним значенням, то будь-які різні значення $k_1, k_2 \in N$ призведуть до різних значень $T_{k_1}(Y)$ і $T_{k_2}(Y)$.

Але в дійсності, для практичної реалізації, як вже зазначалося вище, всі значення мусять бути представлені у вигляді раціональних чисел. У такому випадку повинні існувати такі значення $t \in N$, для яких $2Y^{-1}t \in N$. Мінімальне таке натуральне значення позначимо через $W(Y)$, $W(Y) \in N$, $W(Y) = \min\{t \mid t, 2Y^{-1}t \in N\}$, а також позначимо через $Z(Y)$, $Z(Y) \in N$, величину $2Y^{-1}W(Y)$. Маючи в розпорядженні довільне представлення раціонального значення Y, обчислення значень $W(Y)$ та $Z(Y)$ є досить легкою справою. Також треба зазначити, що для однозначного розшифрування всі параметри криптосистеми 1 мусять бути взаємно простими із значенням $Z(Y)$, більш того, має виконуватися нерівність $2^{l_m+1}Y < 1$.

Розглянемо мультиплікативну групу кільця лишків Z_n^* для деякого значення $n > 2$, $n \in N$. Ця група містить $\phi(n)$ елементів, де ϕ – функція Ейлера. Якщо для $\forall r \in Z_n^*$ додатково вважати класи лишків r та $n - r$ еквівалентними, то унікальними залишаться лише класи лишків, які при діленні на n дають лишок $r \in Z_n^*$, такий, що $0 < r < \left\lceil \frac{n}{2} \right\rceil$. Оскільки для будь-якого значення $r \in Z_n^*$ серед чотирьох чисел r, $(-r \bmod n) \in Z_n^*$, $r^{-1} \bmod n \in Z_n^*$ і $(-r^{-1} \bmod n) \in Z_n^*$ рівно два числа матимуть лишок при діленні на n такий, що він потрапляє в інтервал $\left(0, \left\lceil \frac{n}{2} \right\rceil\right)$, то кількість елементів у новоутвореній множині дорівнюватиме $\frac{\phi(n)}{2}$. Позначимо таку множину через $Z_n^{*/2}$. Якщо узагальнити множення за модулем n на випадок еквівалентності класів лишків r та $n - r$ для $\forall r \in Z_n^*$, то отримаємо таку операцію над елементами $Z_n^{*/2}$: $\forall r, q \in Z_n^{*/2}$ $r \cdot q = (-1)^{\left\lceil \frac{2rq}{n} \right\rceil} rq \bmod n$. З такою операцією множина $Z_n^{*/2}$ перетворюється на комутативну групу з нейтральним елементом 1. З іншого боку, групу $Z_n^{*/2}$ можна представити як факторгрупу $Z_n^* / \langle n-1 \rangle$, і оскільки група Z_n^* є комутативною, то $Z_n^{*/2}$ також буде комутативною групою.

Означення 3. *Для* $\forall n \in N$, $n > 2$, *через* $Z_n^{*/2}$ *позначимо комутативну факторгрупу* $Z_n^* / \langle n-1 \rangle$, *де* Z_n^* *– мультиплікативна група кільця лишків* Z_n.

Лема 1. *Маючи в розпорядженні раціональне представлення значення* Y *та значення* C, *де* $C = T_M(Y)$ *для невідомого значення* M, *існує ефективний алгоритм обчислення значення* $T_{M^n}(Y) = \underbrace{T_M(T_M \ldots T_M(Y))}_{n \text{ разів}}$ *для довільного* $m \in N$.

Доведення.

Припустимо, що раціональне представлення значення Y має вигляд $\frac{y_1}{y_2}$, де $y_1, y_2 \in N$. Використовуючи властивості відображення T, маємо $C = T_M(Y) = \frac{1}{\pi}\arccos(\cos(YM\pi)) = \frac{1}{\pi}\arccos\left(\cos\left(M\pi\frac{y_1}{y_2}\right)\right)$ $= T_M\left(T_{y_1}\left(\frac{1}{y_2}\right)\right) = T_{y_1}\left(T_M\left(\frac{1}{y_2}\right)\right)$. Тоді $T_{y_1^{-1}}(C) = T_M\left(\frac{1}{y_2}\right)$, і нехай $C_1 = T_{y_1^{-1}}(C)$. Оскільки $M < y_2$ (інакше не буде однозначного розшифрування в

криптосистемі 1), то $(C_1)^n = \frac{1}{\pi}\arccos\left(\cos\left(\frac{M\pi}{y_2}\right)^n\right) =$ $= T_{M^n}\left(\frac{1}{y_2^n}\right) = T_{y_2^{n-1}}\left(T_{M^n}\left(\frac{1}{y_2}\right)\right)$. Тобто, $T_{y_2^{1-n}}(C_1^n) =$ $= T_{M^n}\left(\frac{1}{y_2}\right)$, що можна переписати у вигляді $T_{y_1}\left(T_{y_2^{1-n}}(C_1^n)\right) = T_{y_1}\left(T_{M^n}\left(\frac{1}{y_2}\right)\right) = T_{M^n}\left(T_{y_1}\left(\frac{1}{y_2}\right)\right) =$ $= T_{M^n}\left(\frac{y_1}{y_2}\right) = T_{M^n}(Y)$. І остаточно: $T_{M^n}(Y)$ $= T_{y_1}\left(T_{y_2^{1-n}}\left(\left(T_{y_1^{-1}}(C)\right)^n\right)\right)$. Операції з параметрами відображення T виконуються в комутативній групі $Z_z^{*/2}$, де $z = Z(Y)$, а отже, можуть бути виконані ефективно.

Лему доведено.

Наслідок: раціональне представлення відкритого ключа Y може бути довільним, а от значення шифртексту C належить множині всіх можливих результатів відображення $\left\{\frac{1}{\pi}\arccos(\cos(k\pi Y)) \mid k \in N, 1 \le k \le 2^{l_m}\right\}$, або точніше – множині представлення таких чисел у вигляді раціональних значень задля можливості практичного використання подібної системи. Узагальнюючи цю множину на випадок послідовного використання відображення, можна показати, що всі результати належать множині $\left\{\frac{1}{\pi}\arccos(\cos(k\pi Y)) \mid k \in Z_z^{*/2}\right\}$, де $z = Z(Y)$. Таку множину позначимо через X. Через K позначимо множину всіх натуральних чисел з відрізку $[1; 2^{l_m}]$. З леми 1 виходить, що за довільними значеннями Y та $C = T_M(Y)$, $C \in X$ можна ефективно обчислити значення $D = T_{M \cdot M}(Y)$, $D \in X$ без знання невідомого значення $M \in K$. Таким чином, кусково-лінійне відображення можна розглядати як комутативне відображення виду $T : K \times X \to X$ (або $T_{[K,X]}$) із задачею обернення такого відображення: за відомими значеннями $C, D \in X$ відновити невідоме значення $M \in K$, що $D = T_M(C)$. Це цілком відповідає розробленим у [4] методам, а також рішення задачі такого обернення дозволить побудувати безключову атаку на повідомлення криптосистеми 1.

Лема 2. *Для фіксованого раціонального значення Y характеристична група $G^{char}\left(T_{[K,X]}\right)$ відображення $T_{[K,X]}$ ізоморфна $Z_z^{*/2}$, де $z = Z(Y)$.*

Доведення.

Нехай зафіксовано деяке раціональне значення Y (що є відкритим ключем одного з абонентів криптосистеми 1). Як було відзначено, множина всіх можливих результатів відображення має вигляд: $X = \left\{\frac{1}{\pi}\arccos(\cos(k\pi Y)) \mid k \in Z_z^{*/2}\right\}$, де $z = Z(Y)$. З огляду на це, а також на те, як зазначено в доведенні леми 1, що дії над параметрами відображення $T_{[K,X]}$ виконуються в групі $Z_z^{*/2}$, досить звичним виглядає введення дії групи $Z_z^{*/2}$ на множину X як для $\forall g \in Z_z^{*/2}$ і $\forall x \in X$ $gx = \frac{1}{\pi}\arccos(\cos(g\pi x))$, що є повністю еквівалентним результату відображення $T_{[K,X]}$ для відповідних елементів.

Лему доведено.

Наслідок: легко перевірити, що для довільного елемента $x \in X$ стабілізатор $G_x^{char}\left(T_{[K,X]}\right)$ є тривіальним, тобто містить лише нейтральний елемент характеристичної групи $G^{char}\left(T_{[K,X]}\right)$, а отже, характеристична група відносно будь-якого елемента $G^{char}\left(T_{[K,X]}, x\right)$ збігається з характеристичною групою. Крім того, при фіксованому значенні Y кількість різних орбіт $\omega\left(T_{[K,X]}\right) = 1$.

Таким чином, для кусково-лінійного відображення всі припущення 1–3 виконуються, що можна вважати вдалим застосуванням алгоритму аналізу (зведення). В результаті задача обернення кусково-лінійного відображення ефективно зводиться до екземплярів задач 1 та 2, де абелева група G – це введена група $Z_z^{*/2}$, а множина X – раціональні представлення набору чисел $\left\{\frac{1}{\pi}\arccos(\cos(k\pi Y)) \mid k \in Z_z^{*/2}\right\}$, де $z = Z(Y)$, і для $\forall g \in G$ і $\forall x \in X$ $gx = \frac{1}{\pi}\arccos(\cos(g\pi x))$.

Звідси випливає, що, як і у випадку шифру Поліга-Хеллмана [4], присутня деяка залежність при побудові торсора. В даному випадку – від виду раціонального представлення значення відкритого ключа Y.

Таким чином, за лемою 1 можна твердити, що з фіксованим раціональним значенням відкритого ключа Y та довільним невідомим значенням $g \in G$, маючи в розпорядженні результат відображення $C = gY$, завдяки виявленим властивостям відображення T можна ефективно в класичній моделі обчислити значення $D = gC$, причому $C, D \in X$, а також значення $D_k = \underbrace{g(g..gC)}_{k \text{ разів}}$ для довільного значення $k \in N$, використовуючи операції в межах групи $Z_z^{*/2}$.

Цей факт відповідає частковому ефективному рішенню [6] для задач 1 та 2 в квантовій моделі обчислень. Це означає, що у квантовій моделі обчислень існує ефективний алгоритм обернення кусково-лінійного відображення за будь-якого представлення даних у вигляді раціональних чисел, що відповідає безключовій атаці на повідомлення для криптосистеми 1. На жаль, ефективна безключова атака на повідомлення присутня і в класичній моделі обчислень для криптосистеми 1, що показано в [6], але для цього знадобилося більше зусиль, і результат було отримано лише для конкретної криптосистеми 1 без узагальнення щодо представлення даних.

Висновки

У цій праці використано методи аналізу локально комутативних відображень та зведення їх обернення до алгебраїчних задач до кусково-лінійного відображення. На основі цього відображення з теорії детермінованого хаосу нещодавно запропоновано криптосистему з відкритим ключем. В результаті застосування зазначених вище методів побудовано ефективне зведення задачі обернення кусково-лінійного відображення до задачі про приховану дію на торсор над абелевою групою $Z_n^{*/2} = Z_n^* / \langle n-1 \rangle$ для $n \in N$. Крім того, особливості кусково-лінійного відображення дали змогу застосувати часткове ефективне рішення задачі про приховану дію на торсор над абелевою групою в квантовій моделі обчислень. Для досліджуваної криптосистеми це означає наявність ефективного алгоритму безключової атаки на повідомлення в квантовій моделі обчислень.

Список літератури

1. Костенко П. Ю. Обеспечение стойкости криптосистемы с открытым ключом на основе кусочно-линейного отображения к атаке с LLL-приведением базиса решетки / П. Ю. Костенко, А. В. Антонов, С. И. Сиващенко // Прикладная радиоэлектроника. – 2007. – Т. 6, № 3. – С. 460–463.
2. Применение методов хаотической динамики для обеспечения информационной скрытности в коммуникационных системах и сетях / П. Ю. Костенко, С. И. Сиващенко, А. В. Антонов, Т. П. Костенко // Изв. Вузов. Радиоэлектроника. – 2006. – Т. 49, № 3. – С. 63–70.
3. Савчук М. М. Симетричні комутативні та локально комутативні шифри для побудови класичних та постквантових криптографічних протоколів / М. М. Савчук, А. В. Фесенко // Інформаційні технології та комп'ютерна інженерія. – 2008. – № 2 (12). – С. 43–51.
4. Фесенко А. В. Сведение атаки на основе открытого текста на локально коммутативный шифр алгебраическим задачам в классической и квантовой моделях вычислений / А. В. Фесенко // Проблемы управления и информатики. – 2014. – № 3. – С. 148–156.
5. Фесенко А. В. Построение бесключевой атаки на криптосистему на основе кусочно-линейного отображения / А. В. Фесенко // Проблемы управления и информатики. – 2008. – № 5. – С. 149–156.
6. Фесенко А. В. Складність задачі про приховану дію абелевої групи в квантовій моделі обчислень // Східно-Європейський журнал передових технологій. – 2013. – № 5 (65). – С. 45–49.
7. Shor P. W. Algorithms For Quantum Computation: Discrete Logs and Factoring / P. W. Shor // Proceedings of the 35th Symposium on the Foundations of Computer Science. – 1994. – P. 124–134.

A. Fesenko

A REDUCTION OF THE PIECEWISE LINEAR MAPPING INVERSION PROBLEM TO THE HIDDEN ACTION ON TORSOR OVER THE ABELIAN GROUP PROBLEM

In this paper, using the general methods of analyzing the inversion problem complexity for locally commutative mappings, investigated the piecewise linear mapping. As a result, the piecewise linear mapping inversion problem, that was used for constructing asymmetric cryptosystems, reduced to the particular case of the hidden action on torsor over the abelian group problem which has effective solution in quantum computing model.

Keywords: one-way function, locally commutative mapping, quantum computation model.

Матеріал надійшов 25.10.2013