18. Bong-Huan, Jun. Manipulability analysis of underwater robotic arms on ROV and application to task-oriented joint configuration. [Text] / Jun Bong-Huan, Lee Pan-Mook, Kim Seungmin // Journal of Mechanical Science and Technology. – 2008. – №22. – P. 887-894.
19. Костенко, В. В. Исследование влияния кабеля связи на маневренность телеуправляемого подводного аппарата [Текст] / В. В. Костенко, И. Г. Мокеева // Подводные исследования и робототехника. – 2009. – №1(7). – С. 22-27.
20. Govindarajan, R. Underwater Robot Control Systems. [Text] / R. Govindarajan, S. Arulselvi, P. Thamarai // International Journal of Scientific Engineering and Technology. – 2013. – Vol. 2, Issue 4. – P. 222-224.
21. Moore, S. Underwater Robotics: Science, Design & Fabrication [Text] / Steven W. Moore, Harry Bohm, Vickie Jensen. – Publisher: Marine Advanced Technology Education (MATE) Center, 2010. – 770 p.
22. Вагущенко, Л. Л. Системы автоматичнского управления движением судов. [Текст] / Л. Л. Вагущенко, Л. Л. Цымбал. – Одесса: Латстар, 2002. – 310 с.
23. Харазов, В. Г. Интегрированные системы управления технологическими процессами [Текст] / В. Г. Харазов. – М.: Изд-во «Профессия», 2009. – 591 с.
24. Бойков, В. И. Интегрированные системы проектирования и управления[Текст] / В. И. Бойков, Г. И. Болтунов, О. К. Мансурова. – СПб: СПбГУ ИТМО, 2010. – 162 с.
25. Вагущенко, Л. Л. Интегрированные системы ходового мостика [Текст] / Л. Л. Вагущенко. – Одесса: Латстар, 2003. – 169 с.
26. Блінцов, В. С. Сучасні задачі автоматизації керування самохідними прив'язними підводними системами з начіпним обладнанням [Текст] / В. С. Блінцов, В. А. Надточій // «Збірник наукових праць НУК». – Миколаїв: НУК, 2012. – №2. – С. 79-83.

Представлено алгебраїчну задачу про приховану дію абелевої групи, до якої зводяться питання стійкості використання локально комутативних відображень в якості криптографічних односторонніх функцій. Показано зведення цієї задачі до відомої в квантовій моделі обчислень задачі про прихований зсув, що дозволяє використовувати вже відомі часткові розв'язки навіть при відсутності ефективного загального методу рішення

Ключові слова: квантова модель обчислень, задача про прихований зсув, одностороння функція

Представлена алгебраическая задача о скрытом действии абелевой группы, к которой сводятся вопросы стойкости использования локально коммутативных отображений в качестве криптографических односторонних функций. Показано сведение этой задачи к известной в квантовой модели вычислений задаче о скрытом сдвиге, что позволяет использовать уже известные частичные решения даже при отсутствии эффективного общего метода решения

Ключевые слова: квантовая модель вычислений, задача о скрытом сдвиге, односторонняя функция

УДК 004.056

СКЛАДНІСТЬ ЗАДАЧІ ПРО ПРИХОВАНУ ДІЮ АБЕЛЕВОЇ ГРУПИ В КВАНТОВІЙ МОДЕЛІ ОБЧИСЛЕНЬ

А. В. Фесенко
Асистент
Кафедра математичних методів захисту інформації
Фізико-технічний інститут
Національний технічний університет України «Київський політехнічний інститут»
пр. Перемоги, 37, м. Київ, Україна, 03056
E-mail: andrey.fesenko@gmail.com

1. Вступ

Значний поштовх у розвитку квантової моделі обчислень відбувся в 1994 році після відкриття ефективного алгоритму Шора [1] 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 із цим, а також у світлі останніх технологічних досягнень при побудові досить потужного квантового комп'ютера стає актуальним пошук нових односторонніх функцій і примітивів, які будуть стійкими навіть до атак з використанням квантового комп'ютера.

2. Квантова модель обчислень

Квантовий комп'ютер складається із квантово-механічної системи, обов'язково ізольованої від навколишнього середовища таким чином, щоб її поведінкою можна було ззовні керувати, але щоб жодна подія, яка

не пов'язана з процедурами контролю, не змогла змінити цю поведінку. Певний набір постулатів [2] створює модель для такої системи. Не вдаючись в деталі, переваги та обмеження такої системи, підкреслимо, що в квантовій моделі обчислень можна ефективно змоделювати довільне обчислення, що є ефективним в класичній моделі обчислень, використовуючи стандартний підхід з оракулом.

Але, як виявилося, знайшлися задачі, які в квантовій моделі обчислень мають якісно більш ефективні алгоритми розв'язку. Так, задача факторизації вважається дуже важкою, і на цьому припущенні базується багато криптографічних систем, включаючи відому систему RSA. І незламність системи RSA за три десятиліття використання підтверджує це припущення. Тому стає зрозумілим сплеск уваги до квантової моделі обчислень після знаходження поліноміального розв'язку для задачі факторизації в цій моделі обчислень. Після достатньої кількості досліджень виявилося, що квантові комп'ютери не стануть панацеєю від усіх проблем.

Зокрема, більшість дослідників вважають, що стандартна модель квантових обчислень з оракулом не зможе розв'язати NP-повну задачу, більш того на даний момент існує думка, що й деякі задачі з класу NPI, який належить NP, але не перетинається з класом NP-повних задач, не знайдуть швидкого вирішення на квантовому комп'ютері [3].

Алгебраїчна задача про приховану підгрупу вдало об'єднує приклади задач, які можна ефективно розв'язати за допомогою квантового комп'ютера на відміну від існуючих алгоритмів для класичного комп'ютера [2].

Задача 1. Задача про приховану підгрупу.

Постановка задачі: Нехай задано множину твірних елементів групи G, деяку скінченну множину S і функцію $f: G \to S$ з додатковою умовою, що існує така підгрупа $H \subset G$ така, що для $\forall g_1, g_2 \in G$ справджується рівність $f(g_1) = f(g_2)$ тоді і тільки тоді, коли $g_1 H = g_2 H$. Необхідно знайти множину твірних елементів підгрупи H, використовуючи обчислення функції f.

Для будь-якої скінченної групи G класичний алгоритм може послідовно обчислити значення $f(g)$ для кожного елемента $g \in G$ і таким чином визначити підгрупу H, використовуючи $|G|$ обчислень функції f. Головним завданням квантової моделі обчислень при розв'язку задачі про приховану підгрупу є зменшення складності до $O(\text{poly}(\log|G|))$ з урахуванням кількості запитів до оракула і будь-якої класичної обробки результатів. Цього можна досягти для достатньої великої кількості груп, що й спричиняє експоненційне зменшення використовуваних ресурсів і призводить до ефективних квантових алгоритмів. Так, як вже згадувалося раніше, майже всі відомі квантові алгоритми, які мають якісну перевагу над своїми класичними варіантами (під якісною перевагою вважається наявність поліноміального квантового алгоритму попри відсутність поліноміального класичного алгоритму для цієї ж задачі) можуть бути описані як часткові випадки задачі про приховану підгрупу. Так, до цих часткових випадків відносяться алгоритм Шора для факторизації цілих чисел, ефективний алгоритм для дискретного логарифму, алгоритм Саймона та інші [2]. Більш того, Кітаєв зі своїм алгоритмом для знаходження стабілізатора в групі фактично розв'язав цю задачу в квантовій моделі обчислень для скінченних абелевих груп [4]. Однак, існують значні проблеми з використанням некомутативних груп в задачі про приховану підгрупу – деякі речі, що здавалися досить простими й зрозумілими в абелевих групах, насправді, в узагальненому випадку вже такими не виглядають. Після успіху алгоритма Шора задача про приховану підгрупу для неабелевих груп розглядалася з метою узагальнення такого вдалого результату. Але, не зважаючи на існування ефективних розв'язків для деяких обмежених неабелевих випадків, в загальному випадку ця задача вважається складною в квантовій моделі обчислень.

Для того, щоб краще усвідомлювати можливу потужність квантових обчислювальних пристроїв було запропоновано цілий клас задач подібних до задачі про приховану підгрупу, і як наслідок пов'язаних з нею.

Задача про прихований зсув (англ. Hidden Shift Problem) розглядається в квантовій моделі обчислень як модель, що може допомогти в пошуку нових ефективних квантових алгоритмів. Задача була вперше сформульована і проаналізована в статті Дама, Холгрена та Іпа [5], де також було представлено декілька часткових розв'язків цієї задачі. Це було першим доказом того, що в квантовій моделі обчислень можливе більш ефективне відновлення як структури підгрупи так і зсуву деякої структури.

Задача 2. Задача про прихований зсув.

Постановка задачі: Нехай задано дві ін'єктивні функції f_1 і f_2, які відображають скінченну групу G в деяку множину S та мають ефективні алгоритми обчислення значень в класичній моделі обчислень, з додатковою умовою, що існує такий елемент $s \in G$, який називається зсувом, що для будь-якого значення $g \in G$ виконується співвідношення $f_1(g) = f_2(g \circ s)$, де $\circ$ - операція, яку визначено на групі G. Задача полягає в пошуку невідомого значення зсуву s, використовуючи твірні елементи групи G.

У випадку, коли група G є абелевою, групову операцію, зазвичай, позначають через '+' і співвідношення функцій прийме вигляд $f_1(g) = f_2(g+s)$. Такий частковий випадок будемо називати абелевою задачею про прихований зсув.

Значна гнучкість постановки задачі про прихований зсув дозволяє використовувати її при розв'язанні досить великої кількості різноманітних задач, починаючи від алгебраїчних проблем, таких як символ Лежандра із зсувом, геометричних задач, таких як пошук центра зсунутих сфер і решіток із зсувом, до комбінаторних задач, таких як ізоморфізм графів [6].

Хоча на даний момент не знайдено ефективного загального алгоритму розв'язку для абелевої задачі про прихований зсув навіть в квантовій моделі обчислень, алгоритм Куперберга [7], який ще називають "ситом Куперберга", дозволяє вирішити цю проблему за час $2^{O(\sqrt{\log|G|})}$, в той час, коли повний перебір вимагає $2^{\Omega(\log|G|)}$, тобто є субекспоненційним. Відзначимо, що алгоритм Куперберга використовує не тільки субекспоненційний час, а й також субекспоненційний об'єм пам'яті, оскільки вимагає $2^{\Theta(\sqrt{n})}$ квантових станів спеціального вигляду одночасно. Однак, як показав Реджев в [8],

можна використовувати значно меншу кількість кубітів за один раз і комбінувати їх відповідно до розв'язку класичної задачі суми підмножини (нажаль, відомо, що задача про суму підмножини належить класу NP - повних задач).

Треба також відзначити, що Реджев в [9] зробив оцінку часової складності лише для випадку циклічної групи, порядок якої є степенем 2, і без обчислення константи. І тільки в [10] було отримано чітку оцінку, що задача про прихований зсув для скінченної абелевої групи G може бути розв'язаною в квантовій моделі обчислень за час $L_{|G|}\left(\frac{1}{2},\sqrt{2}\right)$, використовуючи лише поліноміально обмежений розмір пам'яті.

3. Використання локально комутативних відображень для побудови односторонніх функцій

В роботі [11] розглянуто можливість використання певного класу комутативних та локально комутативних відображень виду $E: K\times X\to X$ в якості односторонніх функцій і побудовано цілу низку відомих протоколів з використанням таких відображень. Представлений в [11] клас відображень є прямим узагальненням математичної моделі симетричного шифру. Оскільки, більшість дослідників вважає, що майже всі сучасні стійкі симетричні шифри залишаться невразливими навіть в разі появи потужнього квантового комп'ютера, то запропонований підхід дає реальний шанс побудувати стійкі односторонні функції за квантової моделі обчислень, що в даний момент є досить актуальною задачею в криптографії.

Для такого використання симетричних шифрів та їх відображень необхідно, щоб вони були стійкими до атак на основі відкритого тексту [11] як в класичній так і в квантовій моделях обчислень. З формальної точки зору, така вимога зводиться до пошуку ефективних рішень алгебраїчної задачі, яку можна описати, використовуючи термінологію абстрактних груп та дії групи на множину.

Задача 3. Задача про приховану дію абелевої групи.

Постановка задачі: Нехай задано множину твірних елементів абелевої групи G, яка діє на множину X, причому 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. За заданими значеннями $x_0, x_1\in X$ необхідно знайти такий елемент $u\in G$, що $ux_0 = x_1$ з додатковою умовою, що такий елемент $u\in G$ - існує та є єдиним, і дія групи G на орбіту елемента x_0 є вільною.

Існування ефективного розв'язку задачі 3 для конкретного відображення означатиме порушення односторонності такої конструкції, і як наслідок, неможливість використання її для побудови криптографічних примітивів.

Оскільки основною метою є пошук односторонніх функцій в квантовій моделі обчислень, то з метою кращого розуміння перспективності використання запропонованої конструкції [11] є аналіз існуючих розв'язків та можливих методів вирішення задачі 3 в квантовій моделі обчислень.

4. Зведення задачі про приховану дію абелевої групи до задачі про прихований зсув

З метою усвідомлення можливої складності задачі про приховану дію абелевої групи покажемо яке місце займає ця задача в ієрархії алгебраїчних задач, що є добре відомими в квантовій моделі обчислень, та які було представлено вище.

Лема 1. Задача про приховану дію абелевої групи ефективно зводиться до задачі про прихований зсув.

Доведення.

Нехай задано множину твірних елементів абелевої групи G з операцією '+', яка діє на множину X. Також, нехай, задано деякий елемент $x_0\in X$ такий, що група G діє вільно на множину $G_{x_0}\subseteq X$, орбіту елемента x_0. За заданим значенням $x_1\in G_{x_0}$ необхідно знайти такий елемент $u\in G$, що $ux_0 = x_1$ (за таких умов елемент $u\in G$ завжди існує і він є єдиним).

Визначимо дві функції $f_1: G\to X$ та $f_2: G\to X$ наступним чином: $f_1(g) = gx_1$ і $f_2(g) = gx_0$. Оскільки група G діє вільно на орбіту елемента x_0, то різним значенням $g\in G$ будутьвідповідатирізнізначення $gx\in X$ для будь-якого фіксованого значення $x\in G_{x_0}$. Так як і x_0, і x_1 належать цій орбіті G_{x_0}, то обидві визначені функції, f_1 і f_2, є ін'єктивними і мають ефективний алгоритм знаходження значення функції в класичній моделі обчислень.

Для будь-якого значення $g\in G$ має місце співвідношення $f_1(g) = gx_1 = g(ux_0) = (g+u)x_0 = f_2(g+u)$. Таким чином визначено дві ін'єктивні функції f_1 і f_2, і існує деяке єдине значення прихованого зсуву $u\in G$, $u\neq 0$, яке збігається із шуканим елементом комутативної групи. Отже, задачу про приховану дію абелевої групи можна ефективно звести до задачі пошуку прихованого зсуву в комутативній групі.

Лему доведено.

Наслідок: Задача про приховану дію абелевої групи є частковим випадком відомої в квантовій моделі обчислень задачі про прихований зсув. Використовуючи зведення до відомих ефективних часткових розв'язків задачі пошуку прихованого зсуву для комутативних груп, можна отримати ефективні розв'язки задачі про приховану дію абелевої групи в квантовій моделі обчислень. Більш того, завдяки субекспоненційному алгоритму Куперберга для розв'язку задачі про прихований зсув для абелевої групи, можна стверджувати, що задача 3 також має загальний субекспоненційний алгоритм розв'язку в квантовій моделі обчислень.

Також виявляється, що достатньо дещо послабити обмеження до задачі про приховану дію абелевої групи, щоб побудувати еквівалентну задачу до задачі про прихований зсув для абелевої групи. При формулюванні задачі 3 було вказано, що має існувати ефективний алгоритм обчислення дії будь-якого елемента абелевої групи на довільний елемент множини, що повністю відповідає меті використання досліджуваних конструкцій. Але припустимо, що такий алгоритм буде вимагатися лише для двох заданих умовою елементів x_0 та x_1.

Лема 2. Задача про прихований зсув для абелевої групи поліноміально еквівалентна задачі про приховану дію абелевої групи, якщо ефективний алгоритм обчислення такої дії вимагається лише для двох заданих елементів x_0 та x_1.

Доведення.

Нехай за допомогою твірних елементів задано скінченну комутативну групу G (для зручності опису - з груповою операцією '+' та нейтральним елементом '0'), скінченну множину X і дві ін'єктивні функції $f_1: G \to X$ та $f_2: G \to X$ такі, що існує єдине значення "зсуву" $s \in G$, $s \neq 0$, для якого виконується умова $\forall g \in G \;\; f_1(g) = f_2(g+s)$. Функції f_1 та f_2 повинні мати ефективний алгоритм обчислення в класичній моделі обчислень для будь-якого значення аргумента.

Розглянемо дію групи G на множину X, визначену наступним чином:

$$\text{для } \forall g \in G \text{ і } r \in X \text{ - } gr = \begin{cases} f_2(g + f_2^{-1}(r)), \exists f_2^{-1}(r) \\ r, \nexists f_2^{-1}(r) \end{cases}.$$

Оскільки, за умовою, функція f_2 є ін'єктивною, то для будь-якого значення $g \in G$ визначене вище відображення буде автоморфізмом множини X. Більш того, для

$$\forall g_1, g_2 \in G \text{ і } \forall x \in X$$

$$g_1(g_2 x) = \begin{cases} f_2(g_1 + g_2 + f_2^{-1}(x)), \exists f_2^{-1}(x) \\ x, \nexists f_2^{-1}(x) \end{cases} := g_2(g_1 x) = (g_1 + g_2)x.$$

Отже підмножина елементів множини X, для яких існує прообраз функції f_2 формуватиме торсор над абелевою групою G (тобто, визначена дія групи G на цю підмножину буде вільною та транзитивною), а всі інші точки будуть нерухомими відносно дії групи G. Оскільки за умовою існує прихований зсув $s \in G$, $s \neq 0$, то елементи $f_1(0) = f_2(s)$ та $f_2(0)$ будуть належати торсору і не будуть нерухомими, що означає для $\forall g_1, g_2 \in G$, $g_1 \neq g_2 \;\; g_1 f_1(0) \neq g_2 f_1(0)$ і $g_1 f_2(0) \neq g_2 f_2(0)$.

Відзначимо, що в загальному випадку обчислення чи побудова оберненої функції $f_2^{-1}(r)$ для довільного значення $r \in X$ є складною як у класичній так і в квантовій моделях обчислень. Так, наприклад, розв'язок задачі про прихований зсув можна отримати як $s = f_2^{-1}(f_1(0))$. Тому побудована дія групи G на множину X не матиме ефективного алгоритму обчислення результату дії для будь-яких елементів як в класичній так і в квантовій моделях обчислень.

Але розглянемо результат дії групи G на елементи $f_1(0), f_2(0) \in X$. Для будь-якого $g \in G$ $gf_2(0) = f_2(g + f_2^{-1}(f_2(0))) = f_2(g+0) = f_2(g)$, а $gf_1(0) = gf_2(s) = f_2(g + f_2^{-1}(f_2(s))) = f_2(g+s) = f_1(g)$. Тобто, за умови наявності ефективного алгоритму обчислення функцій f_1 та f_2 можна також ефективно обчислити значення $gf_1(0)$ та $gf_2(0)$ для будь-якого елемента $g \in G$.

І $sf_2(0) = f_2(s + f_2^{-1}(f_2(0))) = f_2(s) = f_1(0)$, більш того $s \in G$ - це єдиний елемент, що переводить $f_2(0)$ в $f_1(0)$. Тому можна припустити, що $x_0 = f_2(0) \in X$, $x_1 = f_1(0) \in X$ і звести пошук значення зсуву $s \in G$ до задачі про приховану дію абелевої групи (задача 3) за заданими значеннями x_0 та x_1 і визначеною дією комутативної групи G на множину X, але за умови, що в задачі про приховану дію абелевої групи вимагатиметься ефективний в класичній моделі обчислень алгоритм обчислення дії лише для заданих елементів x_0 та x_1.

З іншого боку, розглядаючи задачу про приховану дію абелевої групи, за умови, що ефективний алгоритм обчислення дії має бути лише для елементів x_0 та x_1, та визначені функції в лемі 1 - $f_1: G \to X$, $f_2: G \to X$: $f_1(g) = gx_1$ і $f_2(g) = gx_0$, відзначимо, що побудовані функції f_1, f_2, навіть за такого припущення, залишаються ефективно обчислюваними в класичній моделі обчислень. А, отже, ефективне зведення до задачі про прихований зсув з леми 1 залишається справедливим і для такої модифікації задачі про приховану дію абелевої групи.

Таким чином, задача про прихований зсув для комутативної групи поліноміально еквівалентна задачі про приховану дію абелевої групи, в якій ефективний алгоритм обчислення дії групи на множину вимагається лише для двох заданих елементів x_0 та x_1.

Лему доведено.

Наслідок: Таким чином, задача 3, про приховану дію абелевої групи, є частковим випадком задачі про прихований зсув для абелевої групи з досить суттєвими обмеженнями. І хоча ефективного загального розв'язку задачі про прихований зсув не існує на даний момент в квантовій моделі обчислень, ці додаткові обмеження залишають більше шансів задачі про приховану дію абелевої групи на загальний розв'язок. Не дивлячись на цей факт, задача про приховану дію абелевої групи навряд чи буде мати ефективний загальний розв'язок в квантовій моделі обчислень, оскільки складність цієї задачі є порівнянної із відомої задачею про прихований зсув, яка загально визнана складною на даний момент.

5. Висновки

В результаті дослідження складності задачі про приховану дію абелевої групи в квантовій моделі обчислень було показано зведення цієї задачі до відомої абелевої задачі про прихований зсув, що дозволяє використовувати відомі часткові рішення та субекспоненційний алгоритм загального розв'язку Купербера. Вперше було показано схожість та відмінності між цими задачами, що дозволяє сподіватися на те що, задача про приховану дію абелевої групи також буде складної для загального розв'язку в квантовій моделі обчислень, що в свою чергу означає можливість побудови стійкої односторонньої функції в квантовій моделі обчислень на основі локально комутативних відображень. Але для цього необхідно досліджувати кожну таку конструкцію окремо і більш детально з урахуванням зазначених часткових рішень.

Література

1. Shor, P. W. Algorithms For Quantum Computation: Discrete Logs and Factoring [Текст] / P. W. Shor // Proceedings of the 35th Symposium on the Foundations of Computer Science. - 1994. - С. 124-134.

2. Nielsen, M. A. Quantum Computation and Quantum Information [Текст] / M. A. Nielsen, I. L. Chuang - Cambridge University Press, Cambridge, 2000. - 702 С. - ISBN 978-1107002173.
3. Aaronson, S. NP-complete problems and physical reality [Текст] / S. Aaronson // ACM SIGACT News. - 2005. - Т. 36(1). - С. 30-52.
4. Kitaev, A. Quantum measurements and the Abelian stabiliser problem [Електронний ресурс] / A. Yu Kitaev // Режим доступа: www/ URL: http://arxiv.org/abs/quant-ph/9511026, 1995.
5. Van Dam, W. Quantum algorithms for some hidden shift problems [Текст] / W. van Dam, S. Hallgren, L. Ip // In: Proceedings of the 14th annual ACM-SIAM symposium on Discrete algorithms. - 2003. - С. 489-498.
6. Gavinsky, D. Quantum algorithm for the Boolean hidden shift problem [Текст] / D. Gavinsky, M. Roetteler, J. Roland // Proceedings of the 17th annual international conference on Computing and combinatorics. - 2011. - С. 158-167.
7. Kuperberg, G. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem [Текст] / G. Kuperberg // SIAM Journal on Computing. - 2005. - Т. 35(№1). - С. 170-188.
8. Regev, O. A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space [Електронний ресурс] / O. Regev // Режим доступа : \www/ URL: http://arxiv.org/abs/quant-ph/0406151, 2004.
9. Regev, O. On the complexity of lattice problems with polynomial approximation factors [Текст] / O. Regev // In Phong Q. Nguyen and Brigitte Valle, editors, The LLL Algorithm, Information Security and Cryptography. - 2010. - С. 475-496.
10. Childs, A. M. Constructing elliptic curve isogenies in quantum subexponential time [Електронний ресурс] / A. M. Childs, D. Jao, V. Soukharev // Режим доступа : \www/ URL: http://arxiv.org/abs/1012.4019, 2010.
11. Савчук, М. М. Симетричні комутативні та локально комутативні шифри для побудови класичних та постквантових криптографічних протоколів [Текст] / М. М. Савчук, А. В. Фесенко // Інформаційні технології та комп'ютерна інженерія. - 2008. - Т. №2(12). - С. 43-51.

Дана стаття присвячена проблемі пошуку оптимальних параметрів тимчасової дискретизації випадкових стаціонарних процесів. На основі відомого методу дискретизації випадкових процесів формується алгоритм пошуку оптимального інтервалу між вимірами термогазодинамічних параметрів карбюраторних двигунів внутрішнього згоряння. Алгоритм реалізований з використанням прикладного програмного забезпечення Matlab

Ключові слова: оптімальна дискретизація, аналого–цифрове перетворення, термогазодинамічні параметри двигуна внутрішнього згоряння

Данная статья посвящена проблеме поиска оптимальных параметров временной дискретизации случайных стационарных процессов. На основе известного метода дискретизации случайных процессов формируется алгоритм поиска оптимального интервала между измерениями термогазодинамических параметров карбюраторных двигателей внуреннего сгорания. Алгоритм реализован с использованием прикладного програмного обеспечения Matlab

Ключевые слова: оптимальная дискретизация, аналого–цифровое преобразование, термогазодинамические параметры двигателя внутреннего сгорания

УДК 621.002:681.324

ИЗМЕРЕНИЕ СОДЕРЖАНИЯ ОКСИДА УГЛЕРОДА В ОТРАБОТАВШИХ ГАЗАХ ДВИГАТЕЛЯ ВНУТРЕННЕГО СГОРАНИЯ

И. С. Тимофеев
Аспирант
Кафедра информационных систем
Севастопольский национальный
технический университет
ул. Университетская, 33,
г. Севастополь, Украина, 99053
E-mail: timofieiev@gmail.com

1.Введение

Ужесточение требований к контролю состояния современных сложных двигателей внутреннего сгорания [1 – 8], их воздействия на окружающую среду, а также необходимость замены большей части натурных экспериментов вычислительными экспериментами на ЭВМ определяет актуальность задачи достоверного математического описания процессов изменения их параметров во времени. Возникающие при этом погрешности описания объясняются, в том числе, преобразованием непрерывных процессов изменения параметров в цифровые последовательности. Снижение погрешностей может быть достигнуто выбором шага временной дискретизации $\tau_д$, который должен быть таким, чтобы в результате обратного, цифро-аналогового преобразования, можно было восстановить исходный процесс с наименьшими ошибками, а полученные данные не были бы избыточными.