УДК 004.056

АНАЛІЗ СТІЙКОСТІ ПОПУЛЯРНИХ КРИПТОСИТЕМ ПРОТИ КВАНТОВОГО КРИПТОАНАЛІЗУ НА ОСНОВІ АЛГОРИТМУ ГРОВЕРА

Юрій Горбенко, Роман Ганзя

Проблема стійкості популярних криптосистем проти квантового криптоаналізу є актуальною і важливою задачею, враховуючи темпи розвитку квантових технологій. Стійкість всіх сучасних криптосистеми базується на складності вирішення певних математичних задач. Такі математичні задачі, як правило, мають субекспоненціальну або експоненціальну складність вирішення, використовуючи квантові алгоритми, які були запропоновані Шором та Гровером, складність вирішення таких задач зменшується до поліноміальної. Так, алгоритм Шора зменшує складність криптоаналізу перетворень в кільці, полі та в групі точок еліптичних кривих. У статті показана можливість використання алгоритму Гровера для криптоаналізу популярних симетричних блокових шифрів. Розглянуто методи квантового криптоаналізу криптосистем NTRU, основані на комбінації класичної атаки зустріч посередині і квантового алгоритму Гровера. У роботі запропоновано наші оцінки стійкості популярних блокових шифрів і криптосистем NTRU з різними розмірами загальносистемних параметрів проти квантового криптоаналізу, що базується на використанні квантового алгоритму Гровера. Також у статті показано характеристики, якими повинен володіти квантовий комп'ютер, для проведення успішного криптоаналізу певної криптосистеми.

Ключові слова: *алгоритм Гровера, блоковий симетричний шифр, NTRU, кільця зрізаних поліномів, стійкість.*

Вступ. Зважаючи на проблеми та необхідність розв'язання задач криптоаналізу вчені особливу увагу приділили вивченню можливостей розв'язання задач криптоаналізу з використанням квантових комп'ютерів та, в першу чергу, розроблення відповідних алгоритмів для квантових комп'ютерів. Внаслідок таких досліджень у 1994 році Шором [1] були розроблені перші квантові алгоритми - факторизації та дискретного логарифмування в скінченному полі, які призначались для реалізації на квантовому комп'ютері. Пізніше Гровером [2] було запропоновано квантовий алгоритм пошуку у неупорядкованій базі даних. З цих пір почала приділятися велика увага дослідженням у квантовій сфері. Нині, незважаючи на особливу складність практичного розроблення «істинно квантового» комп'ютера [3], в цьому напряму ведуться інтенсивні дослідження і отримано ряд важливих результатів. В першу чергу необхідно відмітити роботи математиків з розроблення методів та алгоритмів криптоаналізу [1].

Алгоритм Гровера, що пропонує вичерпний пошук у великій базі даних та використовується у квантовому комп'ютері, зменшує обчислювальну складність поточного вичерпного пошуку з O(2n) до O(2n/2), таким чином збільшуючи занепокоєння станом безпеки сучасних криптосистем [2].

Постановка проблеми. Досягнення фізики останніх років (бозе-ейнштейнівська конденсація атомів газу [4], квантовий ефект Хола, штучні періодичні структури – квантові точки, колодязі, тощо), а також розвиток лазерних та оптоволоконних технологій дали надію на можливість реалізації найближчим часом квантового комп'ютера. Такі реалізації в початковому стані вже з'являються [3]. Так, за створення проривних технологій маніпулювання квантовими системами, які зробили можливими вимір окремих квантових систем і керування ними, француз Серж Арош (Serge Haroche) і американець Девід Джей Вайнленд стали лауреатами Нобелівської премії 2012 року.

На наш погляд у випадку появи квантового комп'ютера, що може реалізувати уже розроблені квантові алгоритми, зокрема алгоритми криптоаналізу Шора [1] та Гровера [2], можуть виникнути великі загрози у інформаційній сфері відносно забезпечення криптографічної стійкості для симетричних та асиметричних криптоперетворень. При цьому важливим є не тільки сам факт побудови такого комп'ютера, а й технічні характеристики, якими буде володіти квантовий комп'ютер. Вказане необхідно враховувати, так як існуючі квантові алгоритми для своєї «роботи» потребують значних технічних ресурсів, особливо просторових у вигляді кількості кубітів.

Метою цієї статті є аналіз стійкості симетричних криптосистем та систем на базі решіток при використанні алгоритму Гровера для проведення криптоаналізу таких криптосистем. Важливість цих проблемних задач пояснюється тим, що при появі квантових комп'ютерів їх застосування скоріше всього буде направлене на сучасні криптосистеми.

Сучасні криптографічні системи можна поділити на симетричні та асиметричні. У свою чергу асиметричні криптосистеми у відповідності до застосування можна в основному поділити на системи направленого шифрування (НШ) та системи електронного цифрового підпису (ЕЦП).

На сьогодні вже існують квантові алгоритми, які дають змогу проводити атаки на такі асиметричні криптосистеми:

– системи, що базуються на складності факторизації великого цілого числа (RSA) [5];

– системи, що базуються на складності вирішення дискретного логарифму в скінченному полі Галуа (DSA) [5];

– системи, що базуються на складності вирішення дискретного логарифму в групі точок еліптичної кривої (ECC) [5];

– системи на базі решіток (NTRU) [6].

Усі вказані криптосистеми відносяться до класу ймовірно-стійких. А ця ймовірна стійкість як раз і визначається можливостями появи відповідних квантових комп'ютерів, і,як наслідок, вирішення задачі повного розкриття [5].

В даній статті буде показано як з використанням алгоритму Гровера можна провести квантову атаку зустріч посередині на NTRU, а також буде запропоновано аналіз стійкості системи NTRU та деяких популярних симетричних шифрів.

Використання алгоритму Гровера для квантового криптоаналізу симетричних криптосистем. Проблема, на вирішення якої спрямовано метод Гровера, може бути сформульована наступним чином. Нехай дана неупорядкована база даних (список) з N елементів, і нехай в ній існує один елемент, що володіє деякою властивістю (яка легко перевіряється). Потрібно знайти цей елемент.

Таким чином, ми будемо формулювати проблему пошуку наступним чином в термінах експоненційно великої неупорядкованої бази даних з N=2n елементами, серед яких один елемент пронумерований спеціальним чином. Проблема полягає у тому, що необхідно знайти цей елемент. Елементарна теорія ймовірностей показує, що якщо ми переглянемо k елементів, то ми маємо ймовірність k/N знаходження необхідного нам елемента. Отже, необхідно створити O(N) запитів до бази, щоб знайти необхідний елемент з будь-якою константною (не залежної від N) ймовірністю [2].

Існує безліч класичних алгоритмів, в яких процедура повторюється багато разів для досягнення кращого результату. Повторення квантової процедури може покращувати результат деякий час, але після достатньої кількості повторень результат знову стає гіршим. Квантова процедура це унітарне перетворення, яке здійснює поворот в комплексному просторі. Тому, в той час як повторне застосування квантового перетворення може повертати поточний стан все ближче і ближче до потрібного нам стану протягом якогось часу, подальше застосування квантового перетворення може пройти повз потрібного стану і віддалить правильне рішення. Тому, для того, щоб отримати добрий результат при повторюваних квантових перетвореннях, дуже важливо знати, коли потрібно зупинитися [7].

Таблиця 1

Стійкість популярних симетричних шифрів проти квантового крипто аналізу при атаці на ключ та на блок повідомлення

№ п/п	Шифр	Розмір блока/ключа, біт	Кількість необхідної пам'яті для атаки на блок повідомлення/ ключ, кубіт	Стійкість при атаці на	
				блок повідомлення, квантових операцій	ключ, квантових операцій
1	AES-128	128/128	128/128	2^{64} ($10^{19,2}$)	2^{64} ($10^{19,2}$)
2	AES-256	128/256	128/256	2^{64} ($10^{19,2}$)	2^{128} ($10^{38,4}$)
3	DES	64/56	64/56	2^{32} ($10^{9,6}$)	2^{28} ($10^{8,4}$)
4	TDES	64/168	64/168	2^{32} ($10^{9,6}$)	2^{134} ($10^{40,2}$)
5	ГОСТ-28147	64/256	64/256	2^{32} ($10^{9,6}$)	2^{128} ($10^{38,4}$)
6	Калина-128	128/128	128/128	2^{64} ($10^{19,2}$)	2^{64} ($10^{19,2}$)
7	Калина-256	256/256	256/256	2^{128} ($10^{38,4}$)	2^{128} ($10^{38,4}$)
8	Калина-512	512/512	512/512	2^{256} ($10^{76,8}$)	2^{256} ($10^{76,8}$)
9	Blowfish	64/448	64/448	2^{32} ($10^{9,6}$)	2^{224} ($10^{67,2}$)

З використання алгоритму Гровера можна знайти секретний ключ симетричного шифрування за час $\sqrt{K}$, де K – розмір ключа. Детальний опис стійкості симетричних систем проти квантового криптоаналізу наведено в табл. 1. З табл. 1 чудово видно, що стійкість симетричних шифрів при атаці з використанням квантового алгоритму суттєво зменшується. Це означає, що DES буде повністю скомпрометований і не можливо буде вважати його стійким, його стійкість буде дорівнювати 2^{28}. Навіть при AES-128 можна було б знайти секретний ключ за час, приблизно 2^{64}, що в наші дні вважається небезпечно. Що стосується AES-256

біт, то тоді час роботи алгоритму Гровера становить 2^{128}, що є допустимим в наші дні.

Атака зустріч посередині на NTRU. Нехай, *B* – множина булевих многочленів ступеня *N*. *B(d)* – підмножина *B*, многочлен якого має *d* коефіцієнтів *1*, і *N-d* коефіцієнтів *0*. *T(d+,d-)* – множина многочленів, де число коефіцієнтів 1 дорівнює *d+*, а число коефіцієнтів *-1* дорівнює *d-*, а інші є *0*.

Атака дозволяє криптоаналітику отримати особистий ключ користувача обраного з простору 2^N елементів за час $O(2^{N/2})$. Запропонована атака реалізується наступним чином. Простір особистих ключів *f* розділяється на дві великі частини $f_1 \| f_2$, де f_1 та f_2 мають довжину $N/2$ з d/2 одиниць, який володіє властивістю ($\|$ – конкатенація частин):

$$\begin{aligned} & f \cdot h = g (\mathrm{mod}\, q), \\ & (f_1 \| f_2) \cdot h = g (\mathrm{mod}\, q), \\ & f_1 \cdot h = g - f_2 \cdot h (\mathrm{mod}\, q), \\ & (f_1 \cdot h)_i = \{0,1\} - (f_2 \cdot h)_i (\mathrm{mod}\, q)\ \forall i. \end{aligned} \quad (1)$$

Фактично для *f* може і не виконуватися умова, що половина одиниць попадає в перші $N/2$ записів. Як показано в роботі Олдижко [8] існує хоча б одне крутіння *f*, яке буде задовольняти цій властивості, а в якості особистого ключа буде будь-яке крутіння *f*.

Атака складається з наступних кроків:

1. Обирається число *k*, таке що $2^k \geq \binom{N/2}{d/2}$, після чого виділяється пам'ять під 2^k корзин для зберігання багаточленів. Чим більшим буде обрано *k*, тим швидше буде виконуватися алгоритм, але потрібно буде більше пам'яті.

2. Перебираються багаточлени f_1(до багаточленів додається $N/2$ нулів, щоб вони мали довжину *N*). Перебір займе $\binom{N/2}{d/2}$ кроків. Кожне значення f_1 записується до корзини таким чином, що номер корзини, в яку буде поміщатися багаточлен дорівнює найбільш значимим бітам перших *k* коефіцієнтів $f_1 \cdot h = g (\mathrm{mod}\, q)$. Позначимо цю корзину, як *label_f*$_1$. При цьому в деяких корзинах буде по декілька значень багаточленів.

3. Аналогічним чином перебираються вектори f_2 та помічаються як *label_* f_2, але нульові біти додаються до початку. Сформований багаточлен розміщується до корзин, номер яких визначається наступним чином найбільш значимі біти для перших *k* коефіцієнтів багаточлену $-f_2 * h (\mathrm{mod}\, q)$, а також найбільш значимі біти для перших *k* коефіцієнтів багаточлену $-f_2 * h (\mathrm{mod}\, q)$ до кожного коефіцієнту якого додається 1.

4. У випадку якщо при записі f_2, в корзині є багаточлен f_1, то він вважається добрим кандидатом для відновлення *f*. Криптоаналітик обчислює $(f_1 \| f_2) \cdot h = g (\mathrm{mod}\, q)$, складається з {0,1}, то особистий ключ знайдено.

Було встановлено, що цей алгоритм завжди може вернути результат, який, швидше за все може бути закритим ключем *f*, або циклічним зсувом *f*. Часова складність атаки зустріч посередині $O(\frac{C_{N/2}^{d/2}}{\sqrt{N}})$, а складність простору – $O(\frac{C_{N/2}^{d/2}}{\sqrt{N}})$ [8].

Атака Ванга на NTRU. Багато схем NTRU мають властивість $f = 1 + pF$ для закритого ключа *f*, де $f \in B(d_F)$. Ванг розглянув проблему закритого ключа NTRU [9], як задачу пошуку фіксованої ваги цілі. Ванг запропонував квантовий алгоритм пошуку цілі з фіксованою вагою, використовуючи квантовий алгоритм Гровера.

Для збільшення ефективності квантового алгоритму пошуку для вектора з фіксованою вагою не потрібно проводити пошук по усім n-кортежним булевим векторам. Замість цього потрібно знайти усі входи, які мають фіксовану вагу d а також, щоб класичні входи з фіксованою вагою d були представлені як t-кортежним вектори ($t<n$). Щоб досягти цього представимо визначення t-кортежного вектора, позначено як n-розмірний з фіксованою вагою *d*, а також з цим Ванг запропонував алгоритм відтворення векторної мітки [9].

Визначення 1: припустимо, що вага n-кортежного вектора *v* дорівнює *d,* і що на всіх позиціях *v* отримує значення *0*, крім позицій $i_1, i_2, ..., i_d$ для $i_1 \leq i_2 \leq ... \leq i_d \leq n$. Мітка для вектора *v* записується як I_v та має такий вигляд:

$$I_v = 1 + C_{i_1}^1 + C_{i_2}^2 + ... + C_{i_d}^d. \quad (2)$$

Відповідно до Визначення 1, ми можемо розрахувати мітки для усіх n-кортежних векторів з фіксованою вагою *d*, у цьому випадку вектора та їх мітки знаходяться в однозначній відповідності. Щоб оцінити необхідну кількість квантових бітів та діапазон пошуку, у статті Ванга було надано наступну лему [9]:

Лема 1. Для усіх міток n-кортежних векторів з фіксованою вагою *d*, максимальні та мінімальні їх значення є:

$$\min I_v = 1 + C_1^1 + C_2^2 + ... + C_d^d = C_{d+1}^d, \quad (3)$$

$$\max I_v = 1 + C_{n-d+1}^1 + C_{n-d+2}^2 + ... + C_n^d = C_{n+1}^d. \quad (4)$$

Комбінаторна Лема 1 може бути легко доведена, і на основі цієї леми, максимальне значення мітки з фіксованою вагою буде визначати число кубітів, необхідних для проведення пошуку. Тому, вважаючи

$$t = \min\{k \mid C_{n+1}^{d} \le 2^{k}\}. \quad (5)$$

Тоді кількість необхідних кубітів буде визначатися величиною *t*. Так, розмір області пошуку буде 2^t, а це набагато менше, ніж 2^n, що є число при проведенні пошуку над усіма n-кортежними векторами.

Тим не менш, результат пошуку по вектору міток з використанням алгоритму Гровера така мітка цілі, що відповідає вектору цілі з фіксованою вагою. У кінцевому рахунку ми повинні відновити вектор цілі з мітки цілі.

Процедури атаки Ванга наступні:

1. Розрахувати максимальну кількість міток $C_{N+1}^{d_f}$, нехай $t = \left\lceil \log_2^{C_{N+1}^{d_f}} \right\rceil$;

2. Знайти t-кортежний вектор, використовуючи квантовий алгоритм пошуку Гровера, отримати мітку цілі b_0;

3. Отримати вектор цілі v_0 з b_0, повернути v_0 як *F*.

Оскільки $C_{N+1}^{d_F} \le C_{N+1}^{\lceil (N+1)/2 \rceil} < 2^N$, та $d_F << N$, простір пошуку атаки Ванга менше, ніж 2^n [10].

Квантова атака зустріч посередині на NTRU. На даний момент атака зустріч посередині є найбільш ефективним методом проти NTRU, але часова складність до сих пір дуже велика. Метода Ванга [9] може розглядатися, як квантовий пошук «грубої сили», який зменшує часову складність з $O(C_N^{d_f})$ до $O(\sqrt{C_{N+1}^{d_f}})$. Це привабливо для комбінації квантових обчислень з атакою зустріч посередині. Такий метод наводиться у роботі Ксіонга та Ванга [10]. Суть алгоритму полягає у наступному [10].

Для того щоб не втратити загальності:

1. $f, N, d \in B(d)$;

2. Корзина, що складається з полінома f_1 буде помічена як *lable_*f_1, та *bin*(f_1)={*label_*f_1};

3. *bin*(f_2)={*label_*f_2}.

Базова ідея квантової атаки зустріч посередині проти NTRU така:

1. Обчислюємо усі {*label_* f_1, f_1} та розташовуємо їх у вигляді таблиці *L*, проіндексованої за допомогою *label_*f_1.

2. Знаходимо f_2 за допомогою алгоритму пошуку Гровера, з *label_*$f_1 \in$ bin(f_2), та $(f_1+f_2)*h(\text{mod } q) \in \{0,1\}^N$.

3. Знаходимо f_1 відповідний до lab*el_*f_1 в *L*.

4. Перевіряємо f_1+f_2 з іншими умовами.

Деталі пошуку f_2, що засновані на алгоритмі пошуку Гровера, наступні:

1. Обчислюємо максимальне значення мітки $C_{N/2+1}^{d_f/2}$ та нехай $n = \left| \log_2^{C_{N+1}^{d_f}} \right|$.

2. Ініціалізуємо квантову систему з $|0\rangle^{\otimes n} \otimes |0\rangle$. Застосуємо перетворення Адамара $H^{\otimes n}$ до першого регістру, щоб отримати рівноважну суперпозицію стану $|s\rangle$:

$$|s\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{2^{n/2}} \sum_{x=0}^{2^{n/2}} |x\rangle. \quad (6)$$

3. Деталі Оракула: $F_{f_2} : B(\frac{d_f}{2}) \to \{0,1\}$, де:

$$F_{f_2} = \begin{cases} 1, \exists label\_f_1 \in bin(f_2), (f_1 + f_2) \cdot h(\text{mod } q) \in \{0,1\}^N, \\ 0, others. \end{cases} \quad (7)$$

4. Застосуємо алгоритм Гровера $\frac{\pi}{4} 2^{n/2}$ разів. Існує 2 операції, що виконуються в алгоритмі Гровера:

а) застосування Оракула;

б) застосування одиничного (унітарного) оператора $I_\phi = 2|\phi\rangle\langle\phi| - I$ на суперпозиції стану $|s\rangle$, де $\phi = \frac{1}{2^{n/2}} \sum_{x=0}^{2^{n/2}-1} |x\rangle$.

5. Розраховуємо перший регістр, та повертаємо значення f_2 [10, 11].

Вдосконалена квантова атака зустріч посередині. Базова ідея цієї атаки – це знаходження ключа *f* у вигляді *f1* || *f2*, де || – це конкатенація. Довжина *f1* дорівнює $\lfloor N/3 \rfloor$ та *f2* дорівнює $N - \lfloor N/3 \rfloor$. Кожна з частин має відповідну кількість одиниць.

Відповідно до Леми 2, хоча *f* може і не мати відповідних властивостей, таких, що наведені у формулі (1), проте відомо, що деякі циклічні зсуви будуть мати такі властивості і такий циклічний зсув може ефективно використовуватися як параметри для закритого ключа [11].

Лема 2. Нехай $f = f1 || f2$, $\lfloor N/3 \rfloor$ та $N - \lfloor N/3 \rfloor$ є довжинами *f1* та *f2* відповідно. Тоді існую один циклічний зсув *f*, який задовольняє властивості: *f1* має $\lfloor d/3 \rfloor$ одиниць, та *f2* має $d - \lfloor d/3 \rfloor$ одиниць.

Доведення. Нехай *a, b>0*. Щоб не втратити загальності, нехай *f* має $\lfloor d/3 \rfloor + a$ одиниць в перших $\lfloor N/3 \rfloor$ записах, b кількість одиниць в сере-

дніх $\lfloor N/3 \rfloor$ записах, та $d-(\lfloor d/3 \rfloor + a)$ - b одиниць в останніх $N-2\lfloor N/3 \rfloor$ записах.

Тоді, зсуваючи F на одну позицію може змінюватися кількість одиниць в перших (середніх) записах на 0,1 чи -1. Можливі три випадки.

В першому випадку, якщо $b=\lfloor d/3 \rfloor$, тоді після $\lfloor N/3 \rfloor$ зсувів вліво все залишиться на своїх місцях відповідно.

У другому випадку, якщо $b<\lfloor d/3 \rfloor$, після $\lfloor N/3 \rfloor$ зсувів вліво, перші $\lfloor N/3 \rfloor$ записи будуть мати $b<\lfloor d/3 \rfloor$ одиниць в них. Тому в деякій точці кількість одиниць в перших $\lfloor N/3 \rfloor$ записах повинна буде мати точно $\lfloor d/3 \rfloor$ одиниць.

В останньому випадку, якщо $b>\lfloor d/3 \rfloor$, тоді $d-(\lfloor d/3 \rfloor + a)-b<\lfloor d/3 \rfloor$, так після $N-\lfloor N/3 \rfloor$ зсувів вліво перші $N-2\lfloor N/3 \rfloor$ записи будуть мати $d-(\lfloor d/3 \rfloor + a)-b<\lfloor d/3 \rfloor$ одиниць в них.

Нехай L та T позначають бінарні вектори, які визначаються найбільш значущими бітами перших k координат $h+f_1*2h(\bmod q)$ та $-f_1*2h(\bmod q)$, відповідно.

Кроки вдосконаленого алгоритму такі.

1. Вибираємо k таке, що

$$2^k \geq 100*C_{N-\lfloor N/3 \rfloor+1}^{d-\lfloor d/3 \rfloor}. \quad (8)$$

2. Обчислюємо кожне f_l, щоб отримати бінарний вектор T, та підготовляємо таблицю L проіндексовану T.

3. Застосовуємо Оракул, нехай F_2 пробігає по усьому підібраному простору, а тоді шукаємо збіги з квантовим алгоритмом Ванга [9]. Відповідні збіги зустрічаються в двох випадках.

Так, $S \in \{T\}$ чи $S' \in \{T\}$, де S' визначаються перестановкою деяких бітів з S, які отримуються додаванням 1 до $-f_1*2h(\bmod q)$, а в другому випадку $h+(f_1 \| f_2)*2h(\bmod q) \in \{0,1\}^N$.

4. Перевірка, що $f=1+2(f_1 \| f_2)$ з іншими умовами.

Детально 3 крок алгоритму можна представити наступними кроками.

1. Нехай мітка l відповідає вектору $f_{2,1}$. Оракул може бути представлений як:

$$O(l)=\begin{cases} 1, \textit{ якщо } f_{1,2} \textit{ зустрічає } 2 \textit{ стани на } 3 \textit{ кроці}, \\ 0, \textit{ у інших випадках.} \end{cases} \quad (9)$$

2. Обчислюємо максимальне значення мітки $C_{N-\lfloor N/3 \rfloor+1}^{d-\lfloor d/3 \rfloor}$, нехай $n=\left\lceil \log C_{N-\lfloor N/3 \rfloor+1}^{d-\lfloor d/3 \rfloor} \right\rceil$;

3. Ініціалізуємо квантову систему та виготовляємо рівномірно-зважену суперпозицію станів $\frac{1}{2^{n/2}}\sum_{l=0}^{2^n-1}|l\rangle|0\rangle$;

4. Використаємо алгоритм Гровера $\frac{\pi 2^{n/2}}{4}$ разів, отримаємо мітку l та вектор $F_{2,1}$, що відповідає мітці [10].

Порівняння квантових та класичних методів криптоаналізу NTRU. Атака може вернути рішення з високою ймовірністю, а ймовірність може бути збільшена зі збільшенням значенням k. Оракул є простою вирішальною функцією, тому часова складність квантового алгоритму Гровера залежить тільки від кількості ітерацій. Детальне порівняння алгоритмів криптоаналізу NTRU наведено у табл. 2.

В табл. 2, для останніх 2 стовпчиків, під $\bar{O}$ мається на увазі складність роботи квантової атаки зустріч посередині, а під O складність обрахунку таблиці передобчислень для виконання атаки. З таблиці чудово видно, що складність побудови таблиці передобчислень дуже велика і неможна її не враховувати при аналізі складності атаки.

Таблиця 2

Аналітична складність різних атак на NTRU

Складність	Груба сила	Класична атака зустріч посередині	Атака методом Ванга	Квантова атака зустріч посередині (метод Ксіонга)	Удосконалена квантова атака зустріч посередині (метод Ванга)
Часова складність	$O(C_N^d)$	$O(\frac{C_{N/2}^{d/2}}{\sqrt{N}})$	$O(\sqrt{C_{N+1}^d})$	$O(C_{N/2}^{d/2}\log C_{N/2}^{d/2})$ $+\bar{O}(\sqrt{C_{N/2+1}^{d/2}})$	$O(C_{\lfloor N/3 \rfloor}^{\lfloor d/3 \rfloor}\log C_{\lfloor N/3 \rfloor}^{\lfloor d/3 \rfloor})$ $+\bar{O}(\sqrt{C_{N-\lfloor N/3 \rfloor+1}^{d-\lfloor d/3 \rfloor}})$
Просторова складність	$O(1)$	$O(\frac{C_{N/2}^{d/2}}{\sqrt{N}})$	$O(1)$	$O(C_{N/2}^{d/2})$	$O(C_{\lfloor N/3 \rfloor}^{\lfloor d/3 \rfloor})$

Порівняльний аналіз часової складності для різних розмірів системних параметрів NTRU та різних атак наведено у табл. 3. Всі отримані чисельні результати – це кількість елементів кільця зрізаних поліномів, які необхідно перебрати. Тобто всі результати табл. 3 вимірюються у кількості значень з фактор-кільця, які необхідно перебрати.

Таблиця 3

Порівняльний аналіз часової складності різних атак на NTRU

Параметри NTRU	Груба сила	Класична атака зустріч посередині	Атака методом Ванга	Квантова атака зустріч посередині (метод Ксіонга)	Удосконалена квантова атака зустріч посередині (метод Ванга)
NTRU251	10^{52}	10^{24}	10^{26}	$3.3\cdot10^{27}+7\cdot10^{12}$	$3.5\cdot10^{18}+1.6\cdot10^{17}$
NTRU347	10^{72}	10^{34}	10^{36}	$4.6\cdot10^{37}+6.9\cdot10^{17}$	$9\cdot10^{25}+7.6\cdot10^{23}$
NTRU491	10^{100}	10^{48}	10^{50}	$3.2\cdot10^{52}+1.5\cdot10^{25}$	$3\cdot10^{35}+1.8\cdot10^{33}$
NTRU587	10^{120}	10^{58}	10^{60}	$4.5\cdot10^{60}+7.6\cdot10^{29}$	$3.8\cdot10^{41}+9\cdot10^{39}$
NTRU787	10^{159}	10^{77}	10^{79}	$1.5\cdot10^{81}+2.7\cdot10^{39}$	$4.6\cdot10^{54}+3.7\cdot10^{52}$

З наведеної таблиці видно, що удосконалений квантовий метод має набагато меншу складність, ніж класичний метод атаки зустріч посередині. Запропонований метод Ксіонга [10] має набагато більшу складність, ніж класичний метод атаки зустріч посередині (враховуючи складність обчислення таблиці передобчислень).

Порівняльний аналіз просторової складності для різних розмірів системних параметрів NTRU та різних атак наведено у табл. 4. Значення в табл. 4 вимірюються у кількості значень фактор-кільця, які необхідно зберігати в пам'яті для проведення криптоаналізу.

Таблиця 4

Порівняльний аналіз просторової складності різних атак на NTRU

Параметри NTRU	Груба сила	Класична атака зустріч посередині	Атака методом Ванга	Квантова атака зустріч посередині (метод Ксіонга)	Удосконалена квантова атака зустріч посередині (метод Ванга)
NTRU251	1	10^{24}	1	$3.5\cdot10^{25}$	$6\cdot10^{16}$
NTRU347	1	10^{34}	1	$3.5\cdot10^{35}$	$2.6\cdot10^{23}$
NTRU491	1	10^{48}	1	$4\cdot10^{49}$	$9.5\cdot10^{32}$
NTRU587	1	10^{58}	1	$4.2\cdot10^{59}$	$2.7\cdot10^{39}$
NTRU787	1	10^{77}	1	$4.9\cdot10^{78}$	$1.4\cdot10^{52}$

Квантові обчислення сильно впливають на криптографію. Комбінуючи атаку зустріч посередині і квантовий алгоритм пошуку Гровера, вище наведено квантовий метод атаки посередині на NTRU. Наші оцінки показують, що часова складність $O(C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}\log C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor})+\overline{O}\sqrt{C_{N/2+1}^{d/2}}$ різко скоротилася в порівнянні з класичним алгоритмом атаки зустріч посередині $O(\frac{C_{N/2}^{d/2}}{\sqrt{N}})$, з тією ж просторової складністю [10]. Наведений метод також на багато краще у часовій складності в порівнянні з методом Ванга та запропонованого у минулого році метода Ксіонга.

В наведених таблицях чудово видно, що системи на базі NTRU навіть з використанням потужних параметрів (великих розмірів) не мають суттєвої стійкості проти квантової атаки зустріч посередині.

Висновки. Незважаючи на особливу складність практичного розроблення «істинно квантового» комп'ютера, в цьому напряму ведуться інтенсивні дослідження і отримано ряд важливих результатів, що вимагає врахування при проектуванні та застосуванні можливостей здійснення ефективних атак як на асиметричні системи так і на симетричні криптосистеми.

Забезпечення необхідного рівня стійкість симетричних криптографічних систем при появі квантового комп'ютера можна тільки за допомогою збільшення розмірів довжини блока та довжини ключа. Але і за умови збільшення розмірів системних параметрів симетричні системи можуть бути, при певних параметрах, уразливими для квантового криптоаналізу.

Можливості реалізації квантових обчислень суттєво впливають на стійкість криптоперетворень в кільцях зрізаних поліномів. Так комбінуючи атаку зустріч посередині і квантовий алгоритм пошуку Гровера, можна здійснити квантову атаку зустріч посередині, що потребує значно менших затрат, ніж аналогічна класична атака на криптосистему типу NTRU.

Криптосистеми на базі NTRU можуть стати уразливими до квантового криптоаналізу, хоча ще не так давно зазначалося, що такі схеми будуть стійкі проти нього. Так квантова атака зустріч посередині у разі появи квантових комп'ютерів може скомпрометувати системи на основі фактор-кілець (NTRU).

ЛИТЕРАТУРА

[1]. Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quan-

tum Computer, SIAM J. Comput. – 1997. – 26 (5). – pp. 1484-1509.
[2]. Grover, L. K. A fast quantum mechanics algorithm for database search [Text] / L. K. Grover. // – Proceeding of the 28th ACM Symposium on Theory of Computation, New York: ACM Press. – 1996. – pp. 212-219.
[3]. Quantum computer built inside diamond [Electronic resource] / Futurity Research news from top universities- Режим доступа : http://www.futurity.org/ quantum-computer-built-inside-diamond/ .
[4]. Dalfovo, F. V. Theory of Bose-Einstein condensationin trapped gases [Text] / Dalfovo F., Giorgini S., Pitaevskii L. P., Stringari S. // Rev. Mod, Physics. – 1998 –71, No3. – pp. 463-510.
[5]. FIPS-186-3. Digital signature standard: 2009 [Text]. 2009 – 07 – 19 – Gaithersburg, MD 20899-8900 – 2009 – 120 p.
[6]. IEEE Std 1363.1-2008. IEEE Standard Specification for Public Key Cryptographic Tehniques Based on Hard Problems over Lattice [Text]. 2009 – 04 – 10 – NY: The Institute of Electrical and Electronics Engineers, Inc – 2009 – 69 p.
[7]. Гайнутдинова, А. Ф. Квантовые вычисления [Текст]: метод.пособие. А. Ф. Гайнутдинова. – Казань: Казанский государственный университет, 2009, – 272 с.
[8]. Silverman, J. A Meet-The Middle Attack on an NTRU Private Key [Text] / J. Silverman, J. Odlyzko // NTRU Cryptosysytems. – Technical Report, NTRU Report – 2003 - 004, Version 2. – 7 p.
[9]. Wang, X. A quantum algorithm for searching a target solution of fixed weight [Text] / Wang, X. W., S. Bao and X. Q. Fu// Chinese Sci Bull. - 2010.- Vol.55(29). – pp.484-488.
[10]. Xiong, Z. An Improved MITM Attack Against NTRU [Text] / Z. Xiong Wang J., Wang Y., Zhang T., Chen L. // International Journal of Security and Its Applications. – 2012. - Vol. 6, No. 2. – pp. 269-274.
[11]. Wang, H. An efficient quantum meet-in-the-middle attack against NTRU-2005 [Text] / Wang Hong, MA Zhi, MA ChuanGui // Chinese Science Bulletin. – 2013. Vol. 58, No.28-29. – pp.3514-3518.

REFERENCES

[1]. Shor, P. (1997), «Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer», SIAM J. Comput., 26 (5), pp.1484-1509.
[2]. Grover, L. (1996),. «A fast quantum mechanics algorithm for database search», Proceeding of the 28th ACM Symposium on Theory of Computation. New York: ACM Press, pp. 212-219.
[3]. Perkins, R. (2012), «Quantum computer built inside diamond», Futurity Research news from top universities. Mode of access: http://www.futurity.org/ quantum-computer-built-inside-diamond/.
[4]. Dalfovo, F. (1998), «Theory of Bose-Einstein condensationin trapped gases». Rev. Mod. Physics, 71, No3, pp. 463-510.
[5]. FIPS-186-3. (2009), Digital signature standard: 2009. Gaithersburg, MD 20899-8900, 120 p.
[6]. IEEE Std 1363.1-2008. (2009), IEEE Standard Specification for Public Key Cryptographic Tehniques Based on Hard Problems over Lattice. NY: The Institute of Electrical and Electronics Engineers, Inc., 69 p.
[7]. Gaynutdinova, A. (2009), «Quantum Computing», Kazan: Kazan State university, 272 p.
[8]. Silverman, J., Odlyzko, J. (2003), «Meet-The Middle Attack on an NTRU Private Key», NTRU Cryptosysytems: Technical Report, NTRU Report, Version 2, 7 p.
[9]. Wang, X., Bao, W., Fu, X. (2010), «A quantum algorithm for searching a target solution of fixed weight», Chinese Sci Bull, Vol.55(29), pp. 484-488.
[10]. Xiong, Z., Wang, J., Wang, Y., Zhang, T., Chen, L. (2012,. «An Improved MITM Attack Against NTRU», International Journal of Security and Its Applications, Vol. 6, No. 2, pp. 269-274.
[11]. Wang, H., Zhi, MA., ChuanGui, MA. (2013), «An efficient quantum meet-in-the-middle attack against NTRU-2005», Chinese Science Bulletin, Vol. 58, No.28-29, pp. 3514-3518.

АНАЛИЗ СТОЙКОСТИ ПОПУЛЯРНЫХ КРИПТОСИТЕМ ПРОТИВ КВАНТОВОГО КРИПТОАНАЛИЗА НА ОСНОВЕ АЛГОРИТМА ГРОВЕРА

Проблема стойкости популярных криптосистем против квантового криптоанализа является актуальной и важной задачей, учитывая темпы развития квантовых технологий. Стойкость всех современных криптосистем базируется на сложности решения определенных математических задач. Такие математические задачи, как правило, имеют субэкспоненциальную или экспоненциальную сложность решения, используя квантовые алгоритмы, которые были предложены Шором и Гровером, сложность решения таких задач уменьшается до полиномиальной. Так, алгоритм Шора уменьшает сложность криптоанализа преобразований в кольце, поле и в группе точек эллиптических кривых. В статье показана возможность использования алгоритма Гровера для криптоанализа популярных симметричных блочных шифров. Рассмотрены методы квантового криптоанализа криптосистем NTRU, основанные на комбинации классической атаки встреча посередине и квантового алгоритма Гровера. В работе предложено наши оценки стойкости популярных блочных шифров и криптосистем NTRU с различными размерами общесистемных параметров против квантового криптоанализа, основанного на использовании квантового алгоритма Гровера. Также в статье показано характеристики, которыми должен обладать квантовый компью-

тер, для проведения успешного криптоанализа определенной криптосистемы.
Ключевые слова: алгоритм Гровера, блочный симметричный шифр, NTRU, кольца срезанных полиномов, устойчивость.

ANALYSIS OF RESISTANCE POPULAR CRYPTOSYSTEMS AGAINST QUANTUM CRYPTANALYSIS BASED ON GROVER'S ALGORITHM

The problem of resistance the popular cryptosystems against quantum cryptanalysis is an urgent and important task, given the pace of development of quantum technologies. Resistance of all modern cryptosystems based on the complexity of solving certain mathematical problems. Such mathematical problems tend to have exponential complexity or subexponential solutions, using quantum algorithms that have been proposed Shore and Grover the complexity of solving such problems is reduced to a polynomial. So Shor's algorithm reduces the complexity of cryptanalysis transformations in the ring, field and in the group of points on elliptic curves. The article describes the using of Grover's algorithm for cryptanalysis popular symmetric block ciphers. The methods of quantum cryptosystems cryptanalysis NTRU, based on a combination of classical attacks and meeting in the middle of Grover's quantum algorithm. In this paper we proposed our estimates of resistance of block popular ciphers and cryptosystems NTRU with different sizes of the quantum system-wide parameters against cryptanalysis based on the use of Grover's quantum algorithm. The article also shows the characteristics that must have a quantum computer for successful cryptanalysis of certain cryptosystems.
Index Terms: Grover's algorithm, block symmetric cipher, NTRU, the ring of truncated polynomials, stability.

Горбенко Юрій Іванович, кандидат технічних наук, старший науковий співробітник Харківського національного університету радіоелектроніки, лауреат Державної премії в галузі науки та техніки.
E-mail: GorbenkoU@iit.com.ua
Горбенко Юрий Иванович, кандидат технических наук, старший научный сотрудник Харьковского национального университета радиоэлектроники, лауреат Государственной премии в области науки и техники.
Gorbenko Yuriy, Ph.D., senior research fellow of Kharkiv National University of Radio Electronics, Laureate of the State Prize in Science and Technology.

Ганзя Роман Сергійович, аналітик систем захисту інформації ЧАО «ІІТ».
E-mail: roman.ganzya@gmail.com
Ганзя Роман Сергеевич, аналитик систем защиты информации ПрАТ «ИИТ».
Ganzya Roman, analyst of security systems of JSC «IIT».

УДК 511.512

ПРОГРАММНО-МОДЕЛИРУЮЩИЙ КОМПЛЕКС SCSPS АЛГОРИТМА ПОТОЧНОГО ШИФРОВАНИЯ

Анатолий Белецкий, Денис Навроцкий, Александр Семенюк

Основу SCSPS алгоритма поточного шифрования образуют шенноновские примитивы нелинейной подстановки (Substitution) и перестановки (Permutation), или так называемые SP-сети, дополненные примитивами «скользящего кодирования» (SlideCode) и стохастического циклического сдвига (Shift). Поточное шифрование осуществляется поразрядным сложением по модулю 2 блоков шифруемого текста, размер которых составляет 128, 192 или 256 бит, с равными по длине блоками двоичных псевдослучайных чисел (ключами, или гаммами). Поток гамм вырабатывается совокупностью криптографических преобразований секретного базового ключа шифрования. Моделирующий комплекс допускает возможность исключения одного или нескольких примитивов из алгоритма шифрования. Проведен анализ эффективности SCSPS алгоритма.
Ключевые слова: *криптографические примитивы, поточные шифры, программно-моделирующий комплекс.*

I. Введение и постановка задачи. В тех случаях, когда шифрование данных необходимо осуществлять в реальном времени, когда требуется высокая скорость передачи информации (например, при трансляции «живого» видео, в системах сотовой связи и др.), или при передаче по каналам связи массивов данных большого объема зачастую применяют поточные шифры [1].

Различают два основных типа поточных шифров: *синхронные* и *асинхронные* шифры. В синхронных поточных шифрах (СПШ) ключевая (шифрующая) псевдослучайная последовательность (ПСП), называемая *гаммой шифра* (или просто гамма), формируется независимо как от входного (шифруемого) текста, так и шифротекста. При таком способе поточного шифрования от-