## 3. Основні методи квантового криптоаналізу та можливості їх реалізації? Квантовий алгоритм факторизації RSA та які його можливості ?

37.3 Основні методи квантового криптоаналізу та особливості їх застосування.

Детальний аналіз дозволив виділити основні методи криптоаналізу, які можуть бути реалізованими на квантовому комп'ютерові( звичайно якщо він буде побудований). Усі вказані методи повинні бути орієнтовані на використання специфіки квантового комп'ютера та мову програмування на ньому. До основних задач, які можуть бути вирішені на квантовому комп'ютерові в першу чергу необхідно віднести такі:

- квантовий алгоритм факторизації Шора[178,78, 416, 417];
- квантовий алгоритм Гровера [ 164,100 ];
- квантовій алгоритм Шора вирішення дискретного логарифму в скінченному полі
- [178,8];
- квантовій алгоритм Шора вирішення дискретного логарифму в групі точок еліптичної кривої [ 8,388];
- квантовий алгоритм криптоаналізу для перетворень в фактор кільці[20, 21, 388, 187,185 ].

по суті, алгоритм Гровера дозволяє реалізувати алгоритм узагальненого парадоксу про день народження.

2.3.2 Квантовий алгоритм факторизації Шора

Цей квантовий алгоритм був запропонований одним з перших [178]. Він був запропонований для вирішення задачі факторизації модуля криптографічного перетворення в кільці, наприклад RSA криптографічного перетворення. Детальні оцінки складності атаки повного розкриття при застосуванні RSA для електронного цифрового підпису та направленого шифрування розглянуті детально в 2 та 4 розділах. Там показано, що вирішення вказаної задачі зводиться до факторизації модуля перетворення N[20,21]. Там показано, що нині відомі класичні алгоритми факторизації мають або експоненційну, або субекспоненційну складність. При цьому вважається, що найкращим по критерію мінімуму складності факторизації – є алгоритм загального решета числового поля та при деякиз обмеженнях його модифікації - спеціальні решета числового поля. Але застосування алгоритму загального або спеціального решета числового поля для реальних значень загальних параметрів, наприклад $N \geq 2^{2048}$, не можуть бути за нинішніх поглядів реалізованими. Дійсно [162], часова складність таких алгоритмів, оцінюється як субекспоненційна, наприклад у вигляді оцінки:

$$O(exp((c+o(1))(\ln n)^{1/3}(\ln \ln n)^{2/3})). \qquad (2.9)$$

В той же час алгоритм Шора, що орієнтований на квантовий комп'ютер, має поліноміальну складність. При його застосуванні факторизацію можна буде здійснити [178] зі складністю

$$O(n^3) \qquad (2.10)$$

та з використанням $O(n)$ кубітів.

Розглянемо алгоритм на якісному рівні дещо детальніше.

Алгоритм Шора, що запропонований ним в 1994 році, дозволить факторизувати N - значне число на квантовому комп'ютері з певною ймовірністю та з обмеженою помилкою. В алгоритмі Шора для зменшення складності факторизації використано ефект здійснення квантового паралелізму, який може бути реалізованим знаходженням суперпозиції всіх значень функції за один крок. Після цього необхідно виконати квантове перетворення Фур'є функції. Подальші обчислення дозволяють визначити з великою ймовірністю період N, при знанні якого виконується факторизація. Попередньо замітимо, що з точки зору складності найбільшу трудність становить перетворення Фур'є, хоча воно і ґрунтується на алгоритмі швидкого перетворення Фур'є.

У цілому Шор показав, що такий алгоритм дозволяє розкласти число N з часовою складністю

$$O(\log^2 N \log^3(\log N)) \qquad (2.11)$$

з використанням $O(\log N)$ логічних кубітів [4].

Це був перший алгоритм, орієнтований на квантовий комп'ютер, його значимість полягає в тому, що при використанні квантового комп'ютера з декількома сотнями логічних кубітів, він дозволяє , наприклад, зламати RSA крипто перетворення, розклавши модуль перетворення N, тобто знайти множники модуля $N$. Уже при $N \geq 2^{1024}$ це зробити практично неможливо зробити, якщо використовувати відомі класичні алгоритми.

Зроблені попередні оцінки показують, що з використанням квантового алгоритму Шора задачу факторизації модуля $N$ можна звести до вирішення еквівалентної проблеми, сутність етапів якої є у наступному:

- вибрати випадково й рівномірно ціле число a взаємно просте з N*;*
- для вибраного числа *a*, що є взаємно простим з *N*, знайти порядок *r* елемента
- *a mod N.*

Взаємну простоту числа та *N* виконати використовуючи Алгоритм Евкліда[20,21]. Якщо *a* не є взаємно простим з *N*, то потрібно повторно вибрати *a* , взаємно просте з N. Якщо *a* є взаємно простим з *N*, то порядок *r* елемента *a mod N* буде дільником числа *N*.

Порівняльний аналіз складності факторизації для класичного та квантового алгоритмів наведено у табл.2.4.

Таблиця 2.4 - Порівняльний аналіз класичного та квантового алгоритмів факторизації (RSA)

| Розмір модуля N, бітів | Кількість необхідних кубітів 2n | Складність квантового алгоритму $4n^3$ | Складність класичного алгоритму |
|---|---|---|---|
| 512 | 1024 | $0.54 \cdot 10^9$ | $1.6 \cdot 10^{19}$ |
| 3072 | 6144 | $12 \cdot 10^{10}$ | $5 \cdot 10^{41}$ |
| 15360 | 30720 | $1.5 \cdot 10^{13}$ | $9.2 \cdot 10^{80}$ |

Аналіз даних таблиці 2.4 показує, що для зламу RSA криптосистеми з розміром модуля у 15360 бітів (а це розмір відкритого ключа сертифікату США, необхідно лише $1.5 \cdot 10^{13}$ операцій на квантовому комп'ютері, тоді як з використання існуючих класичних обчислювальних систем потрібно виконати порядку $10^{80}$ операцій.

Таким чином, якщо появиться квантовий комп'ютер з відповідними характеристиками та параметрами, RSA система буде зламана за поліноміальний час. Крім того, як слідує із таблиці 2.4, навіть суттєве збільшення модуля, наприклад $2^{3072}$ та більше не врятовує RSA криптосистему від її злому. Детально алгоритм Шора розглядається аналізується в розділі 2.4.