КРИТЕРІЇ КВАНТОВИХ ОБЧИСЛЕНЬ У ЗАДАЧАХ КРИПТОАНАЛІЗУ

Котух Є.В., кандидат технічних наук, доцент,
Воєнна академія імені Євгена Березняка, Київ, Україна

У доповіді будуть розглянуто наступні питання:

1. Вплив розвитку квантових обчислень на криптоаналіз: етапи еволюції технологій (NISQ-ера з обмеженими шумними системами, EFTQC як ранні відмовостійкі системи та FTQC з повноцінною корекцією помилок).
2. Обмеження NISQ-ери: низька масштабованість, високий рівень шуму, необхідність тисяч коректованих кубітів; приклади задач, таких як факторизація 2048-бітного RSA-ключа.
3. Загрози для криптографічних систем: сильніший вплив на асиметричні алгоритми (RSA, DSA, еліптичні криві) через алгоритм Шора; квадратичне прискорення для симетричних схем за допомогою алгоритму Гровера (з $O(N)$ до $O(\sqrt{N})$).
4. Математичні моделі еволюції: параметр масштабованості α ($\alpha < 2$ для NISQ, $2 \leq \alpha \leq 3.5$ для EFTQC, $\alpha > 3.5$ для FTQC); чинники, такі як ізоляція кубітів, crosstalk, декогеренція.
5. Еволюція квантових обчислень (табл. 1): порівняння критеріїв за часовими рамками, класами складності, теоремою про поріг помилки, моделлю масштабованості та принципами корекції помилок.
6. Оцінки характеристик кубітів (табл. 2): кількість фізичних та логічних кубітів, формула для фізичних кубітів на логічний ($O(d^2)$), рівні фізичної та логічної помилок для NISQ, EFTQC та FTQC.
7. Порівняння квантових обчислювальних підходів (табл. 3): VQE/QAOA (гібридні для NISQ з $O(p)$), RFE (робастні для EFTQC з $O(K)$), QPE (для FTQC з $O(1/\varepsilon)$).

8. Показники якості квантових операцій (табл. 4): точність двокубітного гейта, кількісна формула для Quops (від KiloQuops до TeraQuops), час когерентності відносно часу операції.
9. Порівняльний аналіз EFTQC та FTQC у криптоаналізі (табл. 5): кількість операцій на схему (O(T_FTQC / 100) для EFTQC), запусків схеми (O(10^4) · R_FTQC), загальний час виконання, розмір задач (збільшення на 40–50%, від ~90 до ~130 логічних кубітів).
10. Наслідки для криптоаналізу: трансформація від гібридних атак у NISQ до робастних у EFTQC та повномасштабних у FTQC; необхідність переходу до постквантових стандартів для оновлення криптографічної інфраструктури.