Назва:

Квантові алгоритми для розв'язку алгебраїчних задач

та можливості їх застосування в криптоаналізі.

Короткий опис:

Наводяться базові відомості щодо математичного апарату квантових обчислень. Коротко проаналізовано відомі квантові алгоритми для розв'язку алгебраїчних задач, їхні оцінки складності та особливості використання. Розглядаються алгебраїчні задачі про приховану підгрупу і прихований зсув, а також можливості використання квантових алгоритмів для їхнього розв'язку, включаючи поточні ефективні розв'язки. Наведено ефективний розв'язок узагальненої задачі про дискретне логарифмування, а також показано можливості застосування подібних алгоритмів для криптоаналізу.

Окремо розглянута задача Саймона та її узагальнення, а також застосування квантового алгоритму розв’язку цієї задачі для квантового криптоаналізу як окремого інструменту, так і в поєднанні з іншими алгоритмами.

Наводяться особливості реалізації алгоритму Шора та наявні можливості для його застосування. Приводяться відомості про останні практичні спроби і результати розв’язку математичних задач на існуючих реалізаціях квантових комп’ютерів. Робиться оцінка щодо заявлених результатів факторизації цілих чисел та можливості використання цього алгоритму для практичного криптоаналізу.

Відомості про доповідачів:
д. ф.-м. н. Савчук Михайло Миколайович,
к. ф.-м. н. Фесенко Андрій В’ячеславович,
організація – Навчально-науковий Фізико-технічний інститут
КПІ ім. Ігоря Сікорського.