Доповіді на Міжнародному науковому семінарі "Квантові обчислення" (2022-2023 рр.)

Сергій Шевченко, доктор фізико-математичних наук, Фізико-технічний інститут низьких температур ім. Б.І. Вєркіна Національної академії наук України, м. Харків.

"Квантовий комп'ютер – з точки зору фізика".

Проаналізовано сучасний стан проблеми, пов'язаної зі створенням квантового комп'ютера як реально працюючого приладу.

Введено основні поняття квантових обчислень, такі як логічні операції та наведено приклади сучасних досліджень фізичних реалізацій квантових бітів – кубітів.

Іван Горбенко, доктор технічних наук, ПАТ "Інститут інформаційних технологій", м. Харків.

"Концепція зниження ризиків для вразливих криптографічних систем, розробка, стандартизація та впровадження стійких постквантових криптопримітивів на міжнародному та національному рівнях".

Розглянуто процеси зниження ризиків для вразливих (існуючих) криптографічних систем, розробка, стандартизація та впровадження стандартизованих стійких постквантових криптопримітивів асиметричного шифрування, електронного підпису та протоколів інкапсуляції ключів на міжнародному та національному рівнях.

Євген Васіліу, доктор технічних наук, Державний університет інтелектуальних технологій і зв'язку, м. Одеса.

"Квантове розподілення таємних ключів шифрування – новітня технологія криптографічного захисту інформації".

Розглянуто основні переваги та недоліки квантових протоколів розподілення ключів.

Михайло Савчук, член-кореспондент НАН України, доктор фізико-математичних наук, **Андрій Фесенко** кандидат фізико-математичних наук, Навчально-науковий фізико-технічний інститут КПІ ім. Ігоря Сікорського, м. Київ.

"Квантові алгоритми для розв'язку алгебраїчних задач та можливості їх застосування в криптоаналізі" (2 засідання).

Розглянуто ефективний розв'язок узагальненої задачі про дискретне логарифмування.

Наведено 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.

Сергій Гнатюк, доктор технічних наук, Національний авіаційний університет, м. Київ.

“Квантова криптографія та квантовий зв’язок: останні досягнення, передові технології та галузі застосування”.

Основну увагу приділено технологіям квантової криптографії – квантовому розподілу ключів і квантовому прямому безпечному зв’язку. Розглянуто випадки, коли реалізація квантових алгоритмів може бути реальною загрозою традиційним криптографічним системам.

Андрій Терещенко, кандидат фізико-математичних наук, Інститут кібернетики імені В.М. Глушкова НАН України, м. Київ.

“Багаторозрядна арифметика для квантової моделі обчислень”.

Розглянуто квантову модель обчислень для реалізації операцій багаторозрядної моделі обчислень, розглянуто особливості реалізації алгоритмів для квантової моделі обчислень, наведено основні критерії ефективності у разі обчислення складності алгоритмів для квантової моделі обчислень.

“Квантова телепортація та надщільне кодування”.

Розглянуто протоколи квантової телепортації та надщільного кодування як засобів передачі інформації. Розглянуто покрокові алгоритми виконання протоколів.

Проведено покроковий аналіз протоколу квантової телепортації та надана реалізація на основі Qiskit. Коротко розглянуто загальний випадок, коли кубіт заплутаний з іншою системою.

На основі ресурсів IBM проведено симуляцію квантової схеми пересилки двох бітів класичної інформації на основі двох кубітів.

Василь Устименко, доктор фізико-математичних наук, Інститут телекомунікацій та глобального інформаційного простору НАН України та Royal Holloway of University of London, United Kingdom.

“Алгебраїчна геометрія та нові алгоритми постквантової криптографії”.

Представлено групи перетворень векторного простору довільної розмірності, визначені через символічні обчислення з використанням комірок Шуберта проективної геометрії.

“Проєктивні геометрії, постквантові криптосистеми від багатьох змінних та схеми типу Ель Гамаля”.

Запропоновано деякі схеми перетворення відкритих ключів багатовимірної криптографії у криптосистеми типу Ель Гамаля.

Андрій Фесенко, кандидат фізико-математичних наук, Навчально-науковий Фізико-технічний інститут КПІ ім. Ігоря Сікорського, м. Київ.

“Наявні можливості та перспективи побудови квантових обчислювальних пристроїв”.

Проаналізовано обчислювальні можливості сучасних квантових пристроїв. Розглянуто різні підходи до побудови таких обчислювальних пристроїв та фінансові ресурси, які довелося витратити, щоб досягнути мети.

Розглянуто наявні технічні перешкоди, які можуть завадити створенню потужних квантових обчислювальних пристроїв, та потенційні способи їх подолання.

Антон Кудін, доктор технічних наук, Національний банк України, Навчально-науковий Фізико-технічний інститут КПІ ім. Ігоря Сікорського, м. Київ.

“За межами постквантової криптографії або криптосистеми, стійкі в певних моделях обчислень”.

Розглянуто сучасний стан досліджень в галузі “релятивістської криптографії” та існування реальних моделей обчислень, в яких деякі сучасні криптоалгоритми є нестійкими, пропонуються підходи до побудови криптографічних перетворень, стійких в перспективних моделях обчислень.