Научно-исследовательский семинар ***«Математические вопросы кибернетики»***

В пятницу, **1 апреля 2022 г.**, состоится доклад:

**Аблаев Фарид Мансурович, Аблаев Марат Фаридович** (Казань, Казанский (Приволжский) федеральный унивеситет)

**«Квантовое хеширование: основные свойства, эффективные конструкции, реализация»**.

*Аннотация доклада*. Основной результат: метод генерации квантовых хеш-функций и как следствие задание конструкций семейств новых квантовых хеш-функций.

1. Квантовая хеш-функция – это обобщение понятия криптографической хеш-функции на квантовый случай. Напомним, что криптографическая хеш-функция – это функция: а) сжимающая, б) сложно обратимая и в) коллизия-устойчивая. Доказательство свойства «сложной обратимости» – открытая проблема. Доказательство свойства «сложной обратимости» для некоторой функции будет означать, что класс сложности P не совпадет с классом NP.

2. Квантовая хеш-функция отображает исходную информацию (последовательности длины n) в квантовые s-кубитовые состояния и должна удовлетворять следующим двум требованиям:

a) Величина s должна быть значительно меньше n. Это обеспечивает (в силу теоремы Холево) свойство сложной обратимости в случае квантовой хеш-функции.

b) Требование попарной epsilon-ортогональности квантовых состояний (образов исходных последовательностей). Это требование обеспечивает свойство коллизия-устойчивости.

3. Разработан метод генерации квантовых хеш-функций:

a) Определено понятие семейства функций — генератор квантовых хеш-функций.

b) Доказана теорема о композиции: если семейство H функций генерирует квантовую хеш-функцию, а семейство F является epsilon-универсальным хеш-семейством, то композиция G семейств F и H генерирует новую квантовую хеш-функцию.

c) В качестве следствия из теоремы о композиции получены новые конструкции квантовых хеш-функций.

4. Параметры функций семейства (генератора квантовых хеш функций) задают значения фаз квантовых состояний. Эксперимент по генерации таких квантовых состояний реализован в рамках совместной работы в лаборатории нелинейной оптики Казанского ФИЦ РАН:

a) Экспериментальная реализация квантовых хеш-функций выполнена с использованием последовательности однофотонных кубитов, генерируемых в процессе спонтанного параметрического рассеяния света. При этом управление состояниями кубитов в базисе орбитального углового момента света осуществлялось через пространственную модуляцию излучения накачки, что позволило достичь максимальной эффективности условного приготовления фотонов. Получено хорошее согласие теории и эксперимента при исследовании зависимости вероятности коллизии хеш-функции от числа кубитов s. Результат практически не зависит от величины орбитального момента света, что открывает перспективу использования мультиплексирования для повышения скорости обработки информации.

b) Публикация: D. A. Turaykhanov, D. O. Akat'ev, A. V. Vasiliev, F. M. Ablayev, and A. A. Kalachev. Quantum hashing via single-photon states with orbital angular momentum // Physical Review A, 104, 052606(1-8) (2021).