Московский государственный университет имени М. В. Ломоносова и «СФБ лаб» разработали устойчивый к опасным атакам протокол квантового шифрования.

Протокол устойчив к атакам навязывания квантового состояния. Разработка относится к типу распредления «точка-точка». Стойкость протокола квантового распределения ключей в случае идеальной реализации была доказана в ходе тестирования.

Также было подтверждено, что новый протокол квантового шифрования остаётся защищённым от атак навязывания. При этом практическая реализация не требует больших изменений оборудования.

Как сообщает пресс-служба МГУ, протокол квантового шифрования может быть полезным для доставки ключа до конечного пользователя.

«Также отмечается перспективность использования данного протокола для космических систем квантового распределения ключей, где постоянное вращение спутника относительно передатчика может приводить к необходимости постоянной калибровки базисов <…>. В предложенном решении <…> дополнительная калибровка не требуется», — отмечается в сообщении.