Российские математики узнали, как взламывать данные, защищённые квантовым шифрованием

Учёные из Математического института имени В. А. Стеклова РАН представили новый алгоритм, который позволяет выявить уязвимости в протоколах квантовой криптографии. Эти уязвимости ранее не учитывались существующими методами безопасности, что даёт возможность повысить надёжность квантового шифрования. Этот алгоритм может стать ключом к созданию более защищённых систем, обеспечивая безопасность банковских транзакций, защищённых линий связи и критической инфраструктуры.

Квантовая криптография используется для защиты данных с помощью законов квантовой механики. Протокол когерентного одностороннего шифрования (COW), популярный в коммерческих системах, теоретически устойчив к взломам. Однако нынешние методы защиты не могут учесть все возможные виды атак, например, комбинированные атаки, когда злоумышленник использует сразу несколько способов одновременно. Это делает такие атаки трудными для обнаружения.

Учёные предложили комбинированную атаку, которая объединяет два существующих метода: PNS-атаку и USD-атаку. PNS-атака позволяет злоумышленнику перехватывать только определённые фотонные импульсы, что раньше считалось невозможным с точки зрения защиты COW. В свою очередь, USD-атака позволяет точно определить квантовое состояние импульсов. Новый алгоритм, объединяющий оба подхода, способен обходить защиту и эффективно маскировать свои действия, что делает его особенно опасным для современных систем квантового шифрования.