АРХИТЕКТУРА МНОГОКАНАЛЬНЫХ КВАНТОВЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

К.В. МЕЛЬНИКОВ, С.Б. БИРЮЧИНСКИЙ

Одним из основных недостатков современных систем квантовой криптографии является низкая скорость передачи данных, что обусловлено как техническими ограничениями для существующих систем, так и ограничениями, вызванными применяемыми алгоритмами. Использование систем с малой скоростью передачи данных не позволяет полностью реализовать все возможные методы криптографической защиты.

Для обеспечения наивысшего уровня секретности в симметричных криптосистемах необходимо формировать последовательность криптографического ключа с длиной, равной длине передаваемого сообщения.

Поскольку скорость передачи данных в существующих системах квантовой криптографии низка, устойчивость систем к шумовым воздействиям является слабой.

Одним из способов повышения скорости передачи информации является переход к многоканальным системам. Авторами предложены варианты архитектуры различных многоканальных систем связи, использующих квантовую криптографию.

Одним из методов перехода к многоканальности в квантовых криптографических системах является одновременное использование на передающей стороне нескольких источников фотонов с различными длинами волн, передаваемых по одному и тому же каналу связи. Разделение фотонов по частоте в этом случае осуществляется классическими методами спектральной селекции. Преимуществами являются простота реализации системы.

Возможным направлением развития является использование псевдо-квантовокриптографических систем. Реализация такой системы основана на использовании традиционных каналов связи, как волоконно-оптических, так и атмосферных оптических линий связи.

Разработана оптическая схема детектирования направления поляризации фотона, позволяющая определить поляризацию единичного фотона с вероятностью выше 50%. Предложен способ повышения точности определения поляризации фотона.

ИССЛЕДОВАНИЕ ВЛИЯНИЯ НЕДОКУМЕНТИРОВАННОГО ОТЛАДОЧНОГО РЕЖИМА ПРОЦЕССОРОВ ФИРМЫ AMD НА БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ

Е.Е. ОРЛОВ, О.К. БАРАНОВСКИЙ

Аппаратное обеспечение современных компьютерных систем создается путем интеграции большого числа базовых компонент (модулей). Сложность таких систем является причиной того, что выполняемые аппаратным обеспечением функции могут не соответствовать заявленным в спецификации. Эти отличия могут вноситься преднамеренно, например, недокументированные возможности, внедряемые для послепроизводственного тестирования компаниями-производителями, или для проведения вредоносной деятельности, либо быть вызванными ошибками в технологиях разработки и производства.

Характерным примером ошибки в аппаратном обеспечении может являться проблема с когерентностью L1 кэша многоядерных процессоров Intel Core 2 Duo [1].