Канал связи с квантовым распределением ключа

УДК 621.391

Э.Ю. БУШУЕВ, ассистент МТУСИ, С.Е. ГРЫЧКИН, ассистент, Е.П. СТРОГАНОВА, профессор доктор технических наук

Канал связи с квантовым распределением ключа
Communication Channel with Quantum Key Distribution

В настоящее время защита информационных потоков от несанкционированного доступа в информационно-телекоммуникационных системах является важнейшим показателем качества функционирования, зависящим, в свою очередь, от применяемых криптографических средств. Среди методов криптографической защиты особое место занимает квантовая криптография, обеспечивающая высокую степень защищенности информационных потоков.

В данной статье описаны основные принципы и назначение квантового распределения ключа, рассмотрена структура канала связи с квантовым распределением ключа, дано описание процедуры квантового распределения ключа и видов кодирования фотонов в квантовом канале связи при квантовом распределении ключа. Приведено пояснение принципа фазового кодирования в интерферометре Маха-Цандера. Проведен сравнительный анализ схем распределения ключа при использовании фазового кодирования — на основе интерферометра Маха-Цандера и Plug&Play, и объяснены преимущества схемы Plug&Play.

Currently, the protection of information systems from unauthorized access to information and telecommunication systems is the most important factor in the quality of functioning, in turn, used by cryptographic means. Among the methods of cryptographic protection, a special place is occupied by quantum cryptography, a high degree of security of information streaming.

This article describes the basic principles and purpose of quantum key distribution, considers the structure of communication channel with quantum key distribution, describes the procedures for channel key distribution and coding photons in a quantum communication channel with quantum key distribution. An explanation of the principle of phase coding in the Mach-Zehnder interferometer is given. A comparative analysis of key distribution schemes using phase coding is carried out: schemes based on the Mach-Zehnder interferometer and Plug&Play schemes. The benefits of the Plug&Play scheme are explained.

Ключевые слова: квантовая криптография, квантово-криптографическая защита информации, квантовое распределение ключа, фазовое кодирование, поляризационное кодирование, квантовый канал связи.

Keywords: *quantum cryptography, quantum cryptographic information protection, quantum key distribution, phase encoding, polarization coding, quantum communication channel.*

Введение

К современным информационно-телекоммуникационным системам предъявляются все более высокие требования по качеству функционирования [1, 2]. Среди показателей качества функционирования одно из важнейших мест занимает защищенность информационно-телекоммуникационной системы, а именно информационных потоков, от несанкционированного доступа. Степень защищенности информационных потоков, в свою очередь, зависит от применяемых криптографических средств.

Применяемая для обеспечения конфиденциальности информационных потоков криптография имеет потенциальную уязвимость, так как криптостойкость используемых шифров обуславливается огромными вычислительными затратами, т. е. не исключается теоретическая возможность взлома. Для мощнейших классических компьютеров эти затраты исчисляются сотнями тысяч лет, однако с появлением квантовых компьютеров станет возможным осуществить взлом достаточно быстро. Таким образом, необходимо искать новые способы защиты информации. Одним из них и является квантовая криптография.

Под квантовой криптографией подразумевается квантовое распределение ключа (КРК). В отличие от обычных криптографических схем, безопасность которых основана на вычислительных трудностях, при КРК безопасность гарантируется законами квантовой механики [3].

КРК происходит между двумя удаленными узлами, соединенными оптическим квантовым каналом, используемым для передачи фотонов, и открытым каналом, используемым для обработки обмениваемой информации [4]. Далее в качестве оптического квантового канала рассматривается оптоволоконный квантовый канал.

Статью целиком читайте в бумажной версии журнала