XXX Юбилейная Неделя науки СПбГТУ.Материалы межвузовской научной конференции. Ч.VIII: С.9-10, 2002.
УДК 621.383.4

**А.В.Брылевский (6 курс, каф. РФ); В.Д.Купцов, к.т.н., доц.**

# СИСТЕМА КВАНТОВОЙ ПЕРЕДАЧИ КРИПТОГРАФИЧЕСКОГО КЛЮЧА: АВТОМАТИЧЕСКАЯ КОМПЕНСАЦИЯ НАБЕГА ФАЗЫ В ИНТЕРФЕРОМЕТРЕ

ABSTRACT: The experimental quantum key distribution (QKD) setup using phase-coding scheme was assembled and tested; the real-time phase drift compensation technique was developed, implemented and tested; results show that such a technique will work even on single-photon level, i.e. without adding components such as variable attenuator to the system.

В настоящее время является актуальным создание нового класса криптографических систем – систем квантовой передачи ключа. В отличие от широко распространённых на сегодня классических криптосистем, секретность которых основана на математических предположениях и не является строго математически доказанной (пример – алгоритмы с публичным ключом), секретность систем квантовой передачи ключа основана на фундаментальных законах квантовой механики, что при надлежащей практической реализации такой системы гарантирует абсолютную секретность передачи сообщений. Ключ представляет собой случайную последовательность бит, передающуюся по квантовому каналу (оптическому волокну) слабыми оптическими импульсами, вероятность появления фотона в каждом из которых много меньше единицы. Далее ключ используется для кодирования сообщений, которые затем передаются по любому открытому каналу (например, по сети Интернет) и декодируются принимающей стороной при помощи того же самого ключа.

Целью данной работы являлась сборка и настройка системы квантовой передачи ключа, что подразумевает настройку волоконно-оптического интерферометра, настройку источника фотонов (лазера), приёмника (ЛФД) и синхронизацию всей системы; разработку методики автоматической компенсации набега фазы в интерферометре.

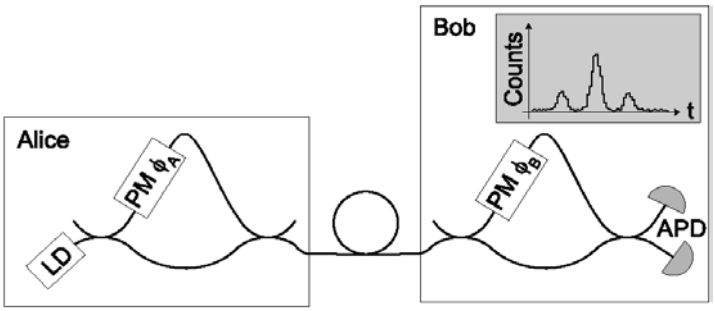


Рис. 1. Волоконно-оптический интерферометр
(LD – лазерный диод, PM – фазовые модуляторы, APD – ЛФД)

Экспериментальная установка принадлежит к системам с фазовым кодированием, то есть информация кодируется фазой передаваемых фотонов. Следует отметить, что в сути данной системы заложена передача по квантовому каналу именно ключа, то есть случайной и заранее неизвестной участникам последовательности бит. Основой системы является волоконно-оптический интерферометр (рис. 1), разбитый на две половинки, которые находятся у передающей стороны (Алисы) и у приёмной стороны (у Боба). Между ними протянут квантовый канал (предполагается использование уже существующих одномодовых волоконно-оптических коммуникационных линий).

Представленная зависимость числа отсчётов в единицу времени на одном из выходов (APD) состоит из 3-х пиков, первый и третий из которых соответствуют фотонам, прошедшим соответственно по обоим коротким и по обоим длинным плечам у Алисы и Боба; средний пик получается в результате интерференции фотонов, прошедших по длинному плечу у Алисы и по короткому у Боба и наоборот. В зависимости от состояния обоих фазовых модуляторов, возможно получение как конструктивной, так и деструктивной интерференции. Возможные варианты сведены в таблицу:

| Alice | | Bob | | |
|---|---|---|---|---|
| Bit value | $\varphi_A$ | $\varphi_B$ | $\varphi_A$-$\varphi_B$ | Bit value |
| 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | $\pi/2$ | $3\pi/2$ | ? |
| 1 | $\pi$ | 0 | $\pi$ | 1 |
| 1 | $\pi$ | $\pi/2$ | $\pi/2$ | ? |
| 0 | $\pi/2$ | 0 | $\pi/2$ | ? |
| 0 | $\pi/2$ | $\pi/2$ | 0 | 0 |
| 1 | $3\pi/2$ | 0 | $3\pi/2$ | ? |
| 1 | $3\pi/2$ | $\pi/2$ | $\pi$ | 1 |

Из-за случайного набега фазы, вызванного нестабильностями в обеих половинках интерферометра, становится невозможным правильная установка фазового сдвига модулятором, приводящая к стабильной интерференции. В связи с этим необходим метод определения постоянного смещения напряжения, подаваемого на модулятор Боба, в зависимости от текущего состояния набега фазы в системе.

Была разработана и воплощена такая методика, состоящая из двух этапов. На первом этапе Боб сканирует весь диапазон напряжений на своём модуляторе и выбирает такое ($V_{comp1}$), при котором был зарегистрирован максимум отсчётов на одном выходе и минимум – на другом. Для более точного определения $V_{comp}$ на втором этапе на модулятор Боба подаётся меандр с постоянным смещением, определённом на первом этапе, и с амплитудой, равной полуволновому напряжению модулятора. На каждом из двух выходов интерферометра подсчитываются количества отсчётов фотонов в точках $V_{comp1}+V_{\pi/2}$ и $V_{comp1}-V_{\pi/2}$, обозначаемые $N_1$ и $N_2$ для одного выхода и $N_3$, $N_4$ – для другого. Результаты для каждого выхода подставляются в заранее выведенную формулу уточнённой поправки к результату 1-го этапа:

$$\Delta\varphi_{comp2-1} = \frac{90^\circ}{\pi}(\arccos(2\frac{N_{dark}-N_1}{N_{\max}-N_{dark}}+1)-\arccos(2\frac{N_{dak}-N_2}{N_{\max}-N_{dark}}+1)),$$

($N_{max}$ и $N_{dark}$ – соответственно максимальное и минимальное количества отсчётов) усредняются для двух выходов и пересчитываются в напряжение смещения, которое затем подаётся на фазовый модулятор Боба и таким образом используется непосредственно при передаче ключа.

Преимуществом данного метода компенсации набега фазы является его работоспособность на квантовом уровне (с числом фотонов, передаваемых в единицу времени, равным таковому при передаче ключа), таким образом отпадает необходимость использования дополнительных дорогостоящих оптических компонентов (электрически управляемого переменного аттенюатора).

Работа выполнена на кафедре физической электроники в NTNU (Норвежском университете науки и технологии, г. Тронхейм).