

## Лекция 13

Коротко о применениях неклассического света:  
метрология (калибровка фотоприемников), криптография (секретная передача ключа).

### *Применение неклассических полей.*

Сейчас можно говорить только о применениях в метрологии (фотометрии) и секретной передаче информации.

#### **1. Абсолютная калибровка фотоприемников – то есть абсолютное измерение квантовой эффективности.**

(1980)

Пусть свет – бифотонный;  $N$  пар фотонов регистрируются двумя фотоприемниками.

За определенное время число отсчетов первого  $N_1 = \eta_1 N$ , второго  $N_2 = \eta_2 N$ , совпадений

$N_c = \eta_1 \eta_2 N$ , где  $\eta_{1,2}$  - квантовые эффективности. Тогда

$$\eta_1 = \frac{N_c}{N_2}$$

На самом деле, все несколько сложнее, надо вычитать шум, а главное – обеспечить, чтобы первый детектор заведомо регистрировал все моды (частотные и угловые), которые «видит» детектор 2. То есть детектор 1 должен быть *более широкополосным*. Это легко понять так: все «просчеты» детектора 1 должны быть связаны только с его неединичной квантовой эффективностью. При  $\eta_1=1$  должно быть  $N_c = N_2$ .

#### **2. Секретная передача ключа – квантовая криптография.**

Давно известно, что передаваемое сообщение (например, из  $n$  цифр в двоичном коде, 010101010101),

можно абсолютно секретно зашифровать, если использовать ключ той же длины – некую последовательность

01110001010001.

Тогда шифруют так: складывают сообщение и ключ по модулю 2:

00100100000100.

А уже те, кто знают ключ, могут это сообщение прочитать. Ключ должен быть одноразовым.

Поэтому единственная задача криптографии – как передать ключ, чтобы знали его только 2 человека (обычно их зовут Алиса и Боб).

1984 – Bennett, Brassard (BB84). Идея: так как поляризацию фотона нельзя измерить, не уничтожив его, да и уничтожив, тоже нельзя, кроме выделенных случаев, - ключ можно передать в виде последовательности поляризованных фотонов.

Алиса передает последовательность, шифруя нули горизонтально поляризованными фотонами, а единицы – вертикально поляризованными. Это в половине случаев. В другой половине случаев (случайно выбираемых) она делает то же в базисе, повернутом на 45 градусов.

Боб также измеряет поляризацию то в том, то в другом базисе – случайно. Потом они сравнивают базисы. Оставляют только те переданные биты, где базисы совпали.

Присутствие подслушателя обнаруживают, сравнивая отдельные биты ключа. Если было подслушивание, будут ошибки.