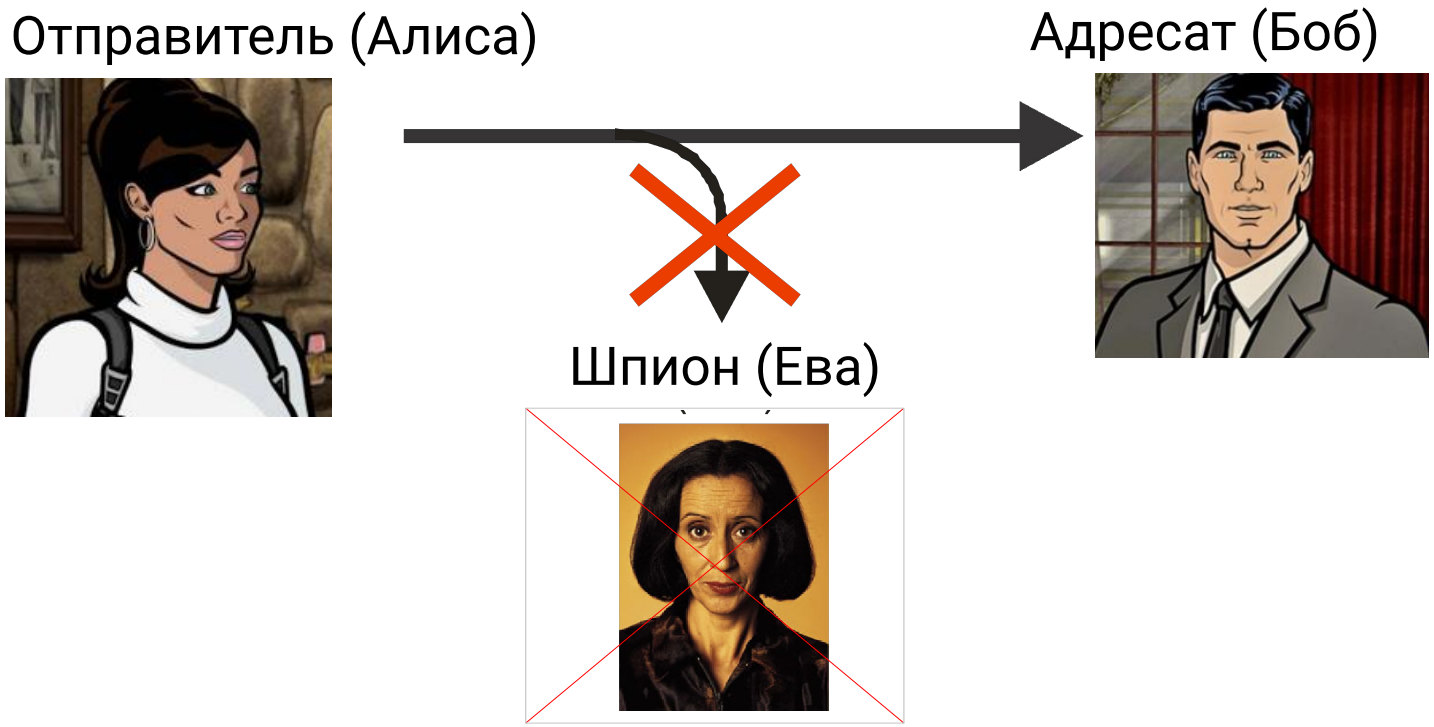
Что такое криптография?

Искусство обмена секретными сообщениями посредством несекретных каналов



Криптография

сообщение 01101000..

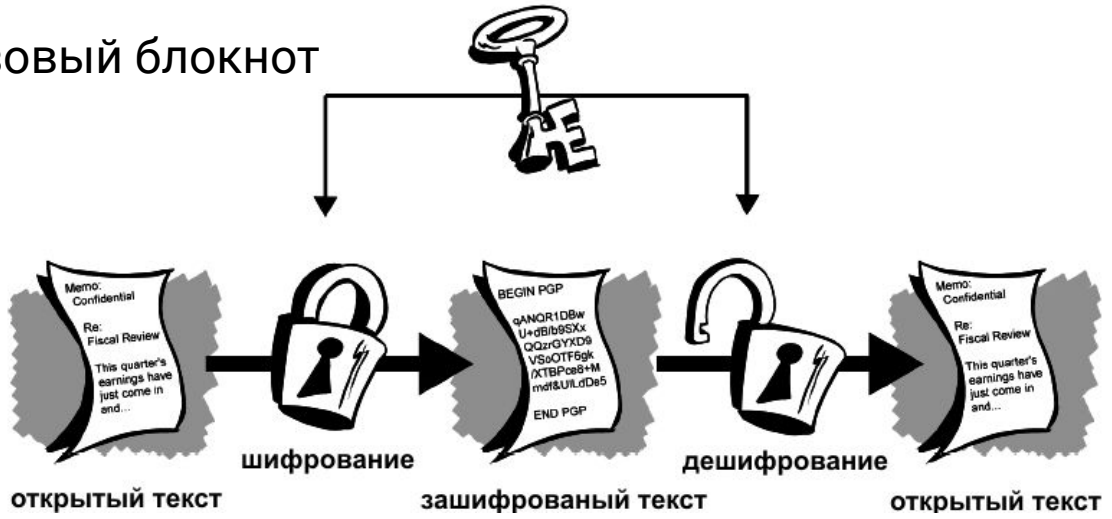
ключ 01000101.. 0100010..

канал передачи

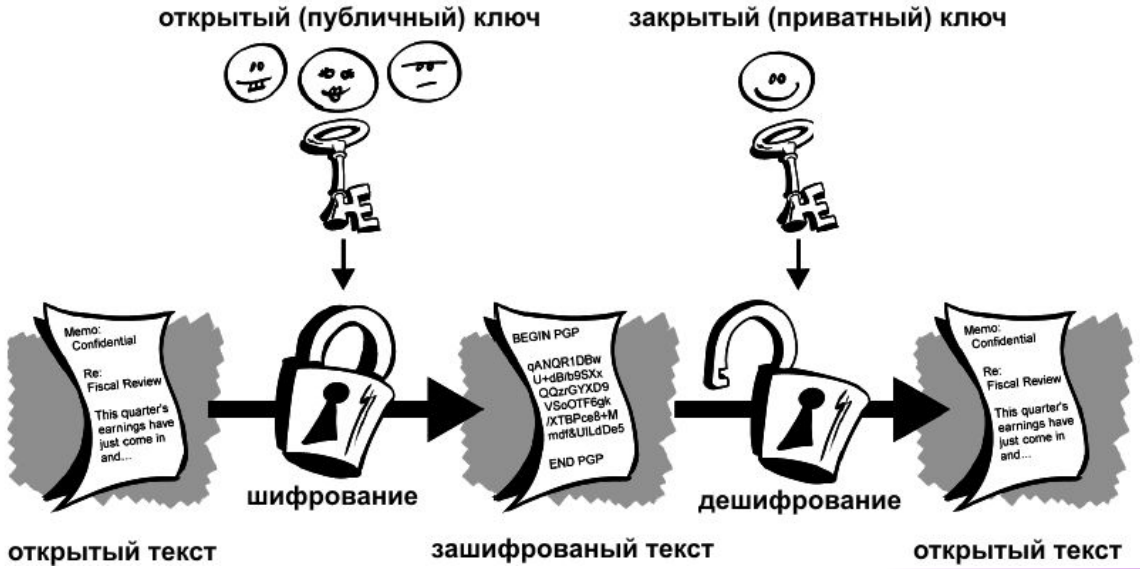
шифрованое сообщение 00101101.. → 0010110..

Расшифрованное сообщение 0110100..

Одноразовый блокнот



Криптография с открытым ключом



Зачем нужна квантовая криптография

Метод открытого ключа

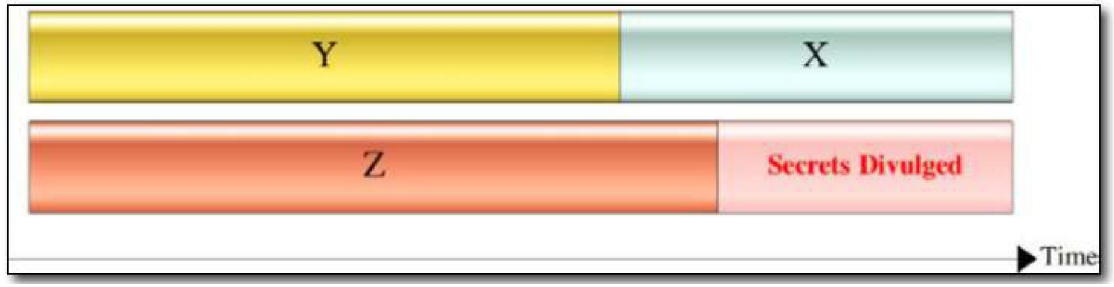
Дёшево. Предварительного общения компьютеров не требуется.

Надёжность не абсолютна. Квантовый компьютер представляет угрозу информационной безопасности.

«Одноразовый блокнот»

Надёжно.

Необходимо решить задачу информационной безопасности – распределение симметричного ключа между абонентами.



X – время, которое наши секреты должны оставаться секретными.
Y – время, которое требуется для внедрения квантовой криптографии.
Z – время, через которое будет изобретён квантовый компьютер.

Квантовая криптография

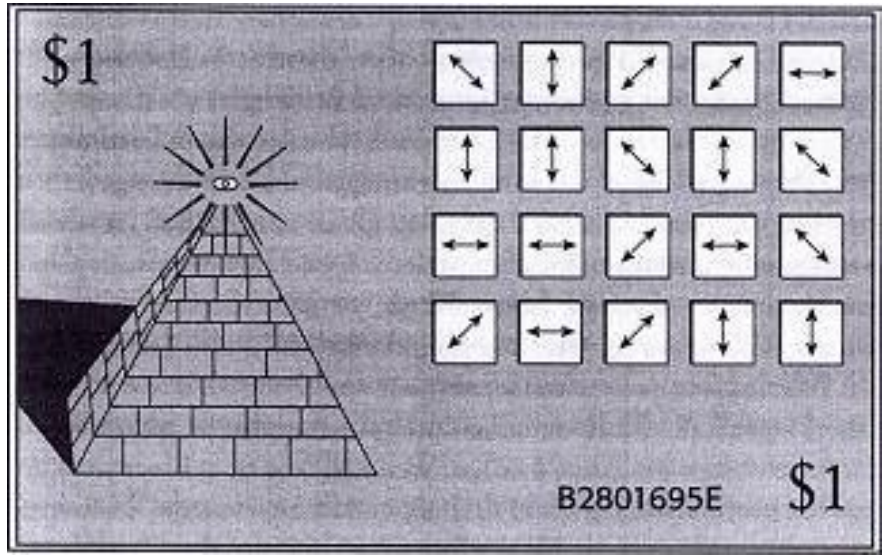
Дёшево. Позволяет безопасную передачу секретного ключа по широкодоступным оптическим каналам ВОЛС.

Секретность гарантируется фундаментальными законами физики.

Квантовая криптография: идея

1983 – публикация работы С.Визнера «Сопряженное кодирование» в SIGACT News.

- **Концепция**
- Информация кодируется в квантовом состоянии отдельных фотонов.
- Постулаты квантовой механики:
  - Фотон неделим
  - Квантовое состояние одной частицы нельзя скопировать
  - Измерение меняет или уничтожает состояние
  - **Если канал подслушивается, это удаётся обнаружить!**



Эскиз квантовой банкноты Стивена Визнера

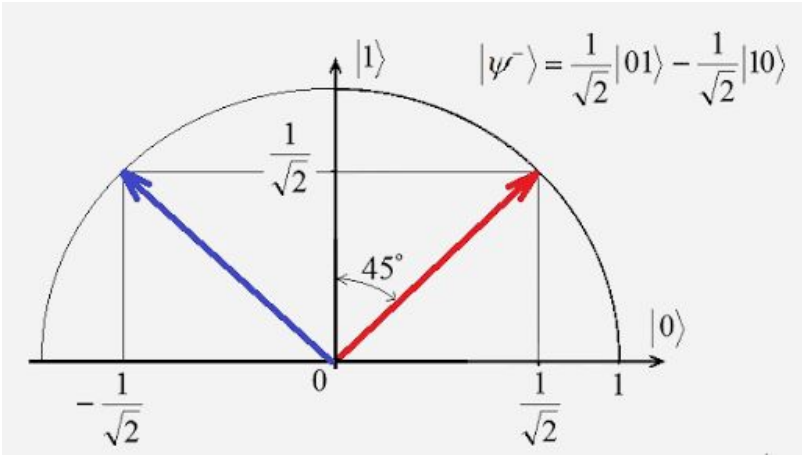
Идея квантовых денег принадлежит аспиранту Колумбийского университета Стивену Визнеру, выдвинута им в конце 60-х годов. Стивен Визнер в 1970 году подал статью по теории кодирования в журнал IEEE Information Theory, но она не была опубликована, так как изложенные в ней предположения редакция посчитала антинаучными.

- Секретность гарантируется фундаментальными законами физики.
- Безусловная устойчивость ко взлому доказана математически.
- Естественный и элегантный способ защиты от квантового компьютера.

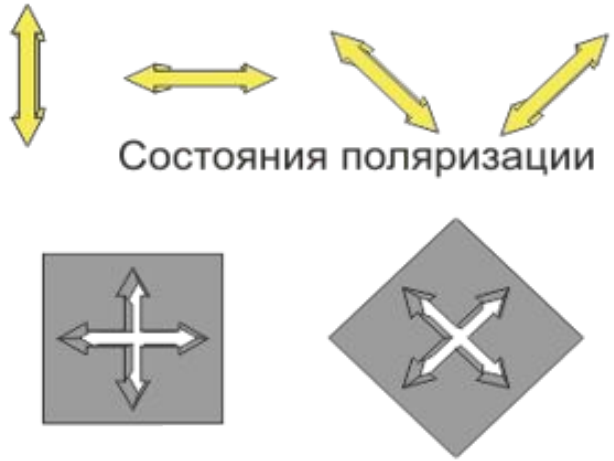
Квантовая информация. Рождение квантовой криптографии

1984 – Ч.Беннет и Ж.Брассард впервые разработали способ кодирования и передачи сообщений. Рождение квантовой криптографии.

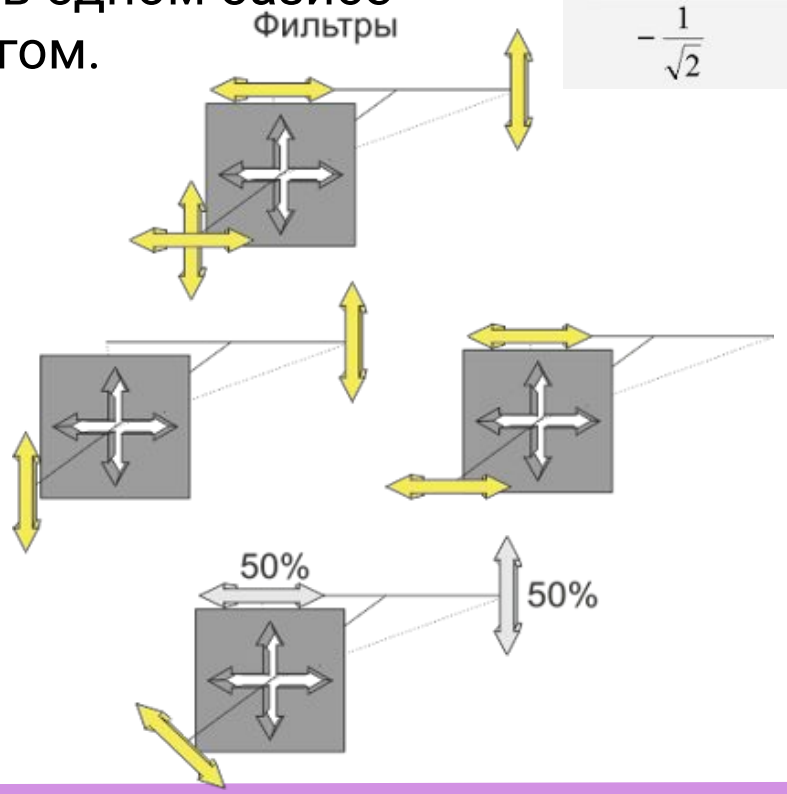
- В состояние поляризации фотона можно зашифровывать информацию.
- При этом определенная поляризация в одном базисе будет суперпозицией состояний в другом.



0 1 1 0

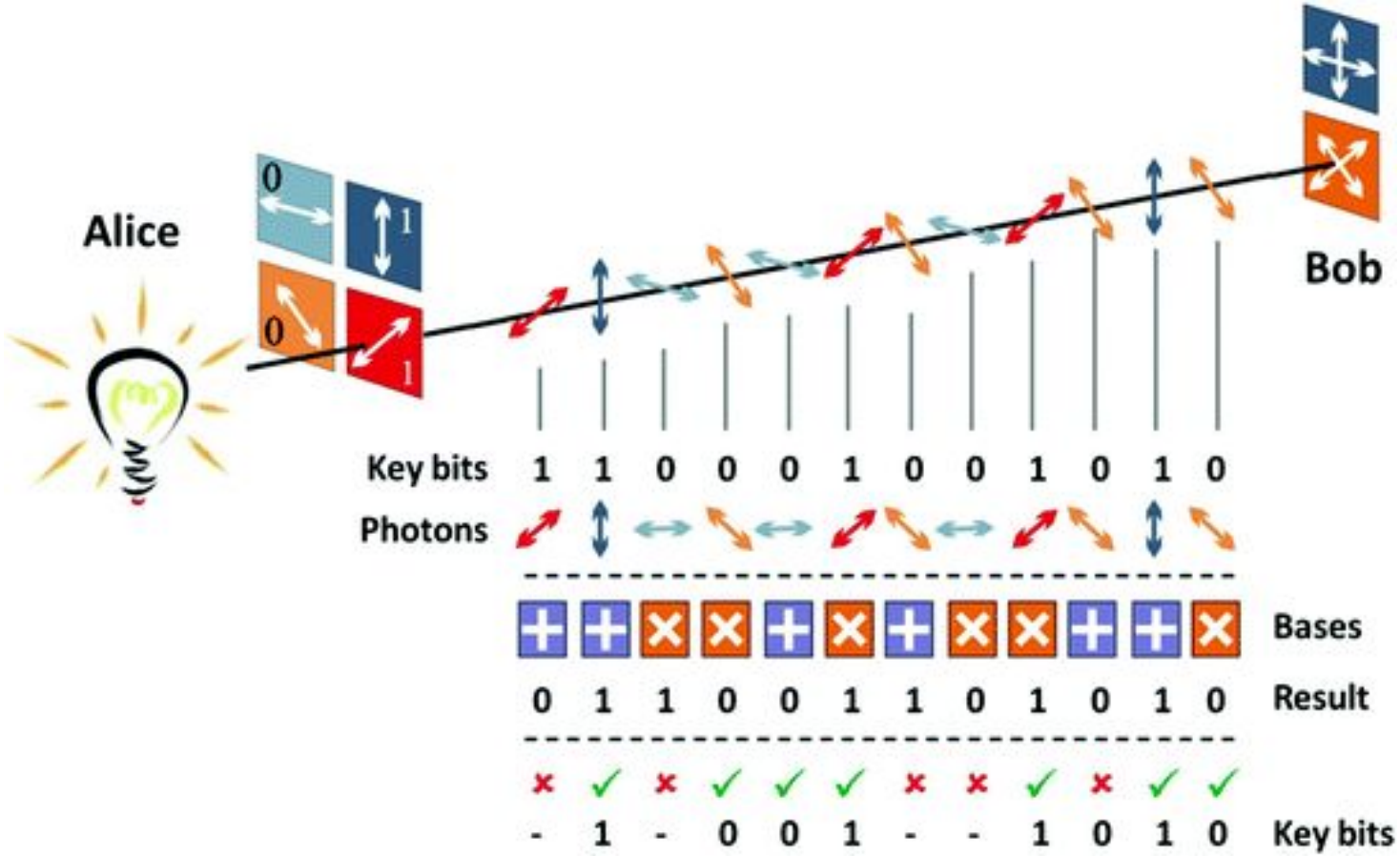


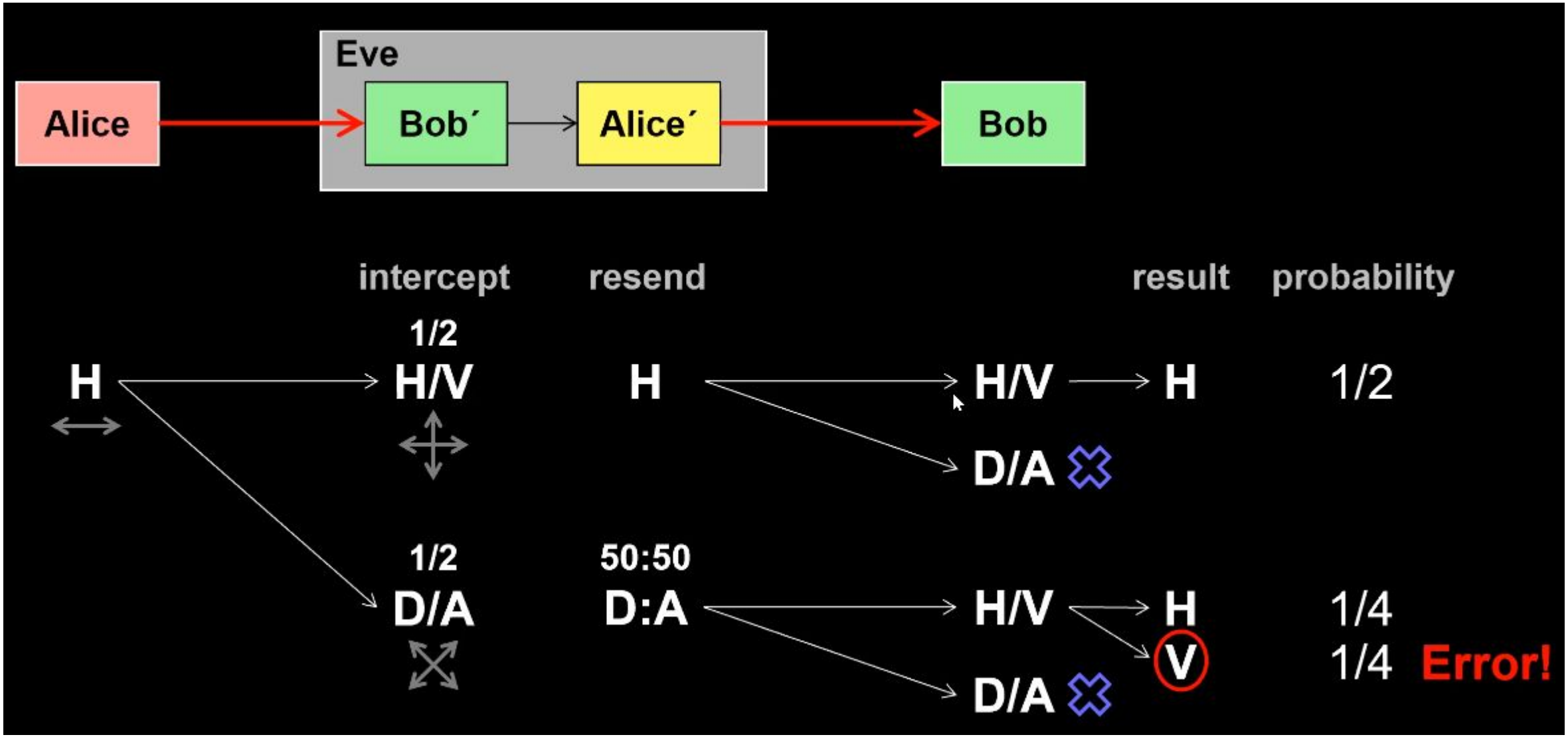
Базис I **Базис II**



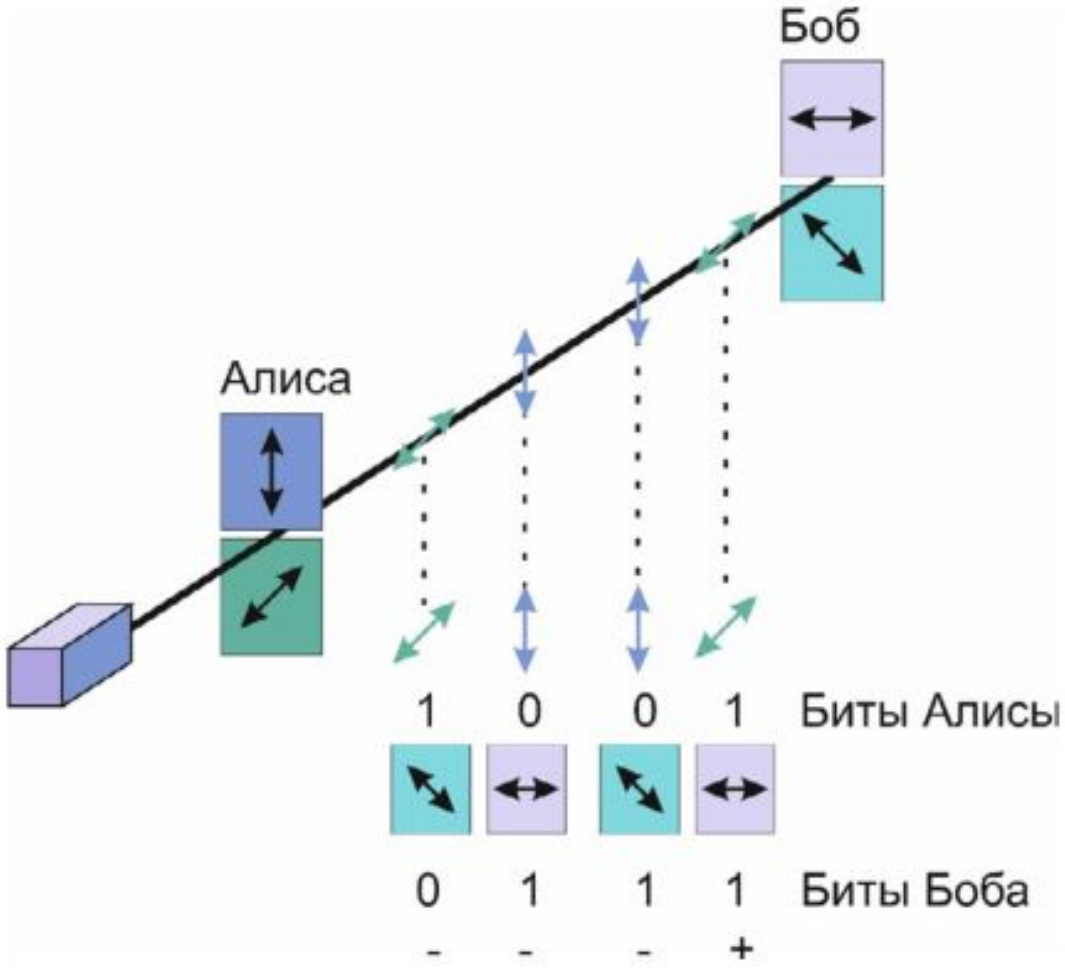
Описание протокола BB84

BB84 – единственный хорошо изученный протокол квантовой криптографии с доказанной криптостойкостью.

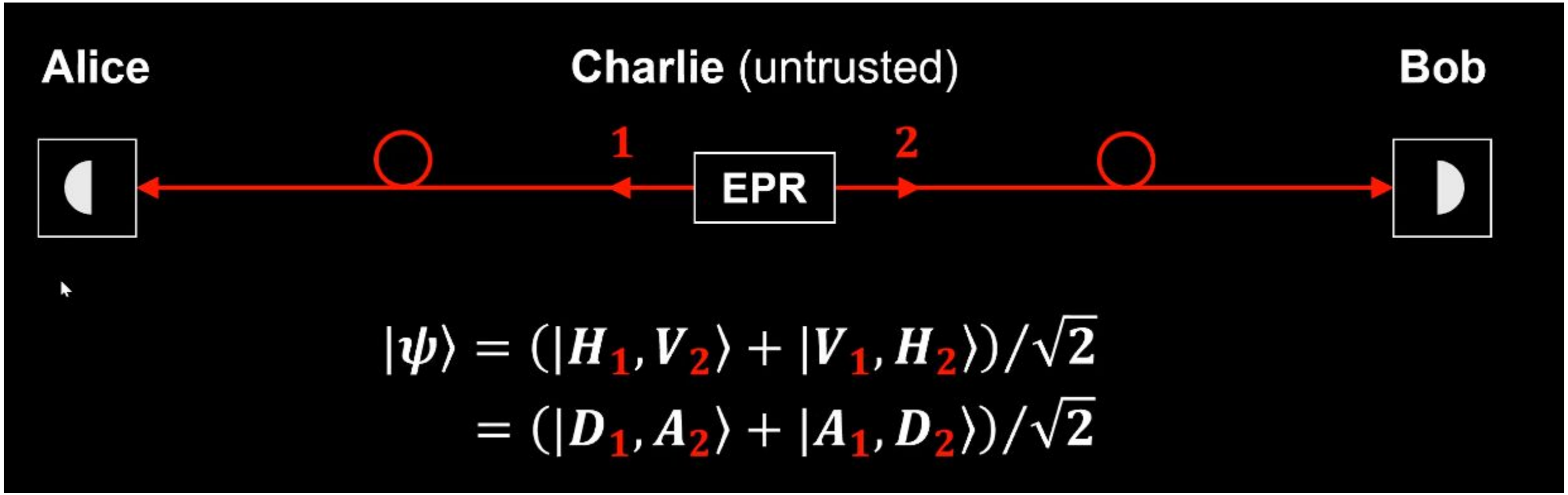



Eve
Alice
Bob´
Alice´
Bob
intercept
resend
result
probability
1/2
H
H/V
H
H/V
H
1/2
D/A
1/2
50:50
D/A
D:A
H/V
H
1/4
V
1/4
Error!
D/A

Описание протокола B92

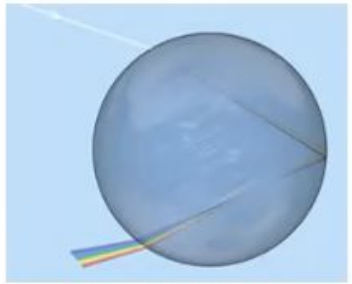


Описание протокола E91




a
Nanshan
1,120 km
Delingha
b
PPKTP
PI
HWP
PBS
DM1
DM2
405
LP
Isolator
HWP
QWP
Collimator
c
SPD5
DM3
532
FSM
BS
BE
SPD3
HWP1
SF
IF
HWP2
PBS2
BF
SPD1
PBS1
SPD4
SPD2

СВЕТ: волна или поток частиц (корпускул)?



Свет – корпускулы?

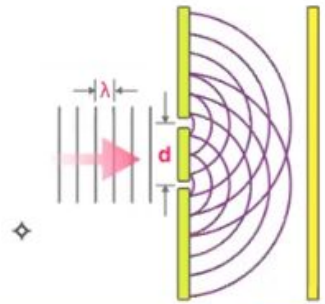
Рене Декарт
1596-1650

Однозначно корпускулы!

Исаак Ньютон
1643-1727

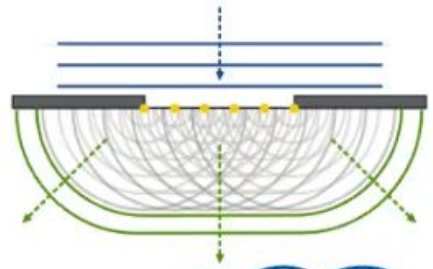
Может, все-таки волны?

Христиан Гюйгенс
1629-1695



Конечно, волны! Интерференция, все дела…

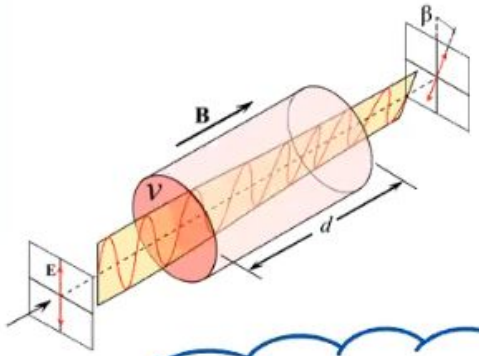
Томас Юнг
1773-1829



По любому, волны! Дифракция же…

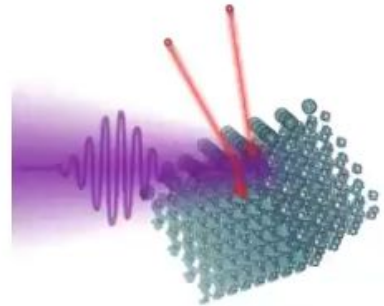
Огюстен-Жан Френель
1788-1827

СВЕТ – электромагнитная волна



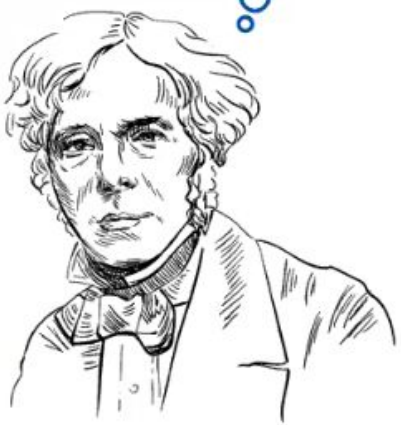
Да это же электромагнитное поле!

$$\nabla \cdot \mathbf{D} = \rho$$
$$\nabla \cdot \mathbf{B} = 0$$
$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}$$
$$\nabla \times \mathbf{H} = \mathbf{j} + \frac{\partial \mathbf{D}}{\partial t}$$



Хм.. как быть с фотоэффектом?

А что насчет черного тела?



Майкл Фарадей
1791-1867

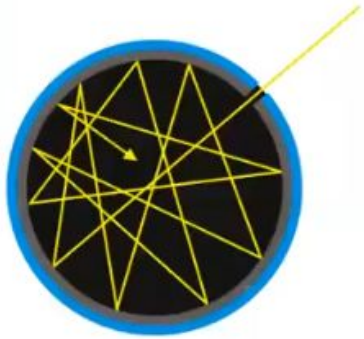
Джеймс Максвелл
1831-1879

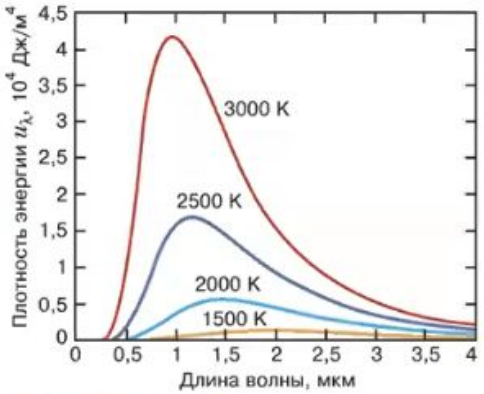
Генрих Герц
1857-1894

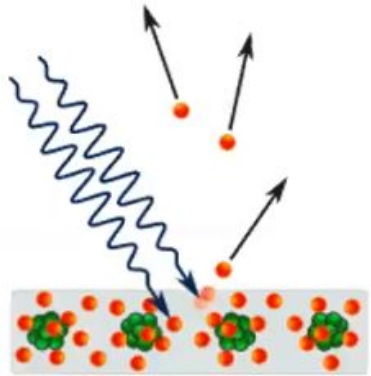
Джеймс Джинс
1877-1946

лорд Рэлей
1842-1919

СВЕТ – поток квантов & электромагнитная волна







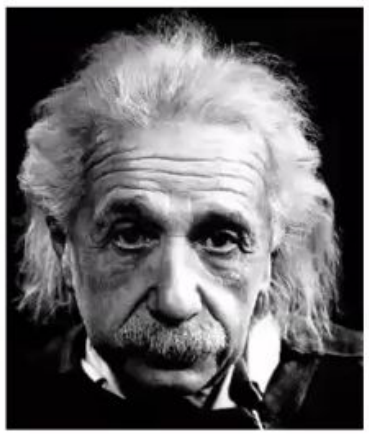
$$\lambda = \frac{h}{p},$$
$$E = h\nu$$

$$B_\nu(\nu, T) = \frac{2h\nu^3}{c^2} \frac{1}{e^{\frac{h\nu}{kT}} - 1}$$

$$h\nu = \phi + \frac{mv_m^2}{2}$$

LIGHT IS A wave!

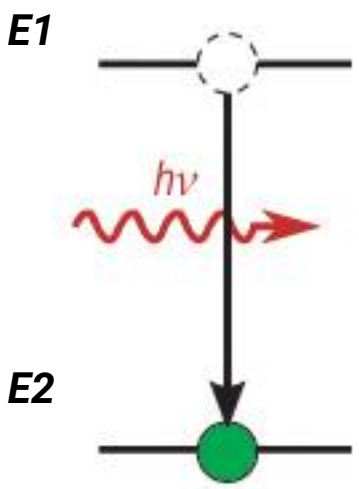
Макс Планк
1858-1947



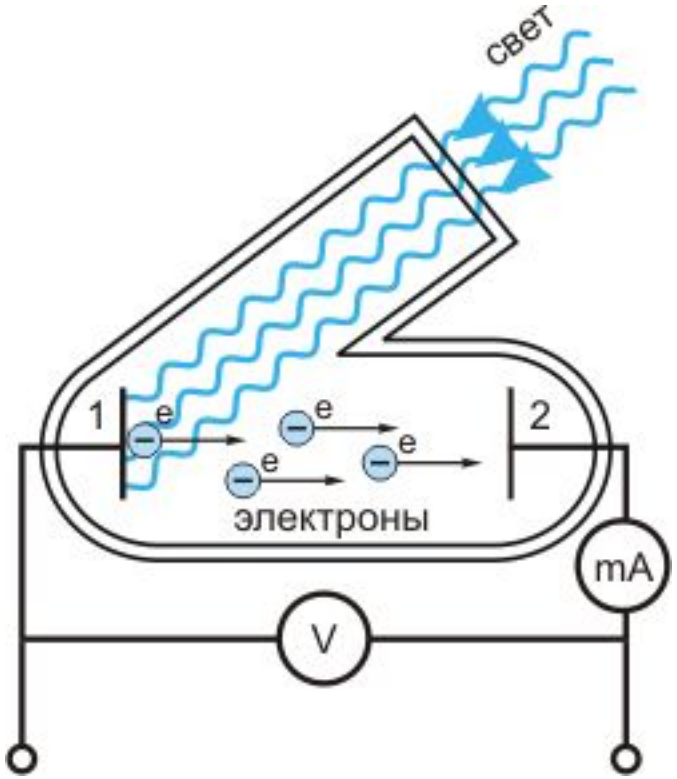
Альберт Эйнштейн
1879-1955

Луи де Бройль
1892-1987

Фотоэффект



- Фотоэффект объяснил Эйнштейн, 1905 г.
- Свет излучается не непрерывно, а порциями (квантами или фотонами)
- Энергия фотона пропорциональна частоте оптической волны
- В нормальных условиях в наши глаза попадает 10^{12} фотонов в секунду

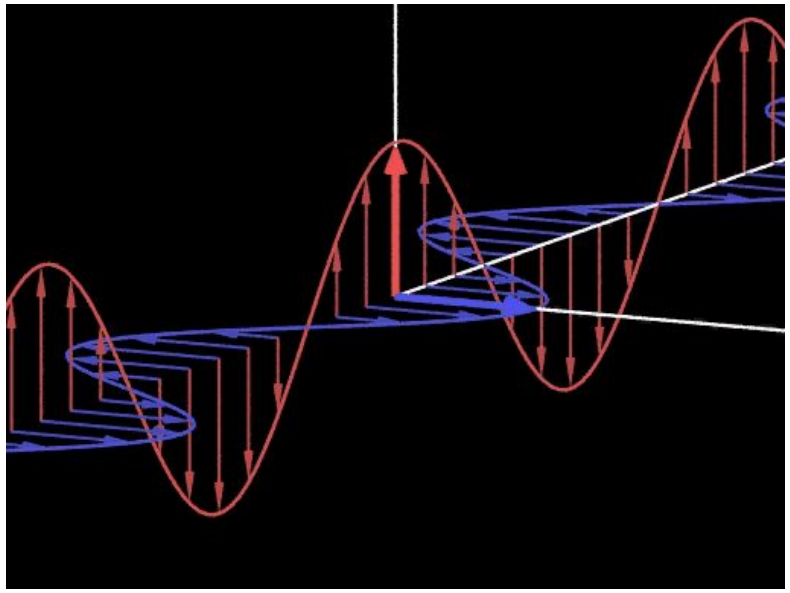


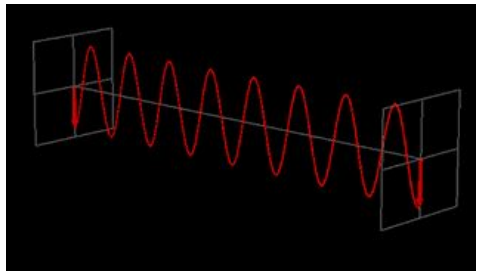
$$E = \hbar\omega$$

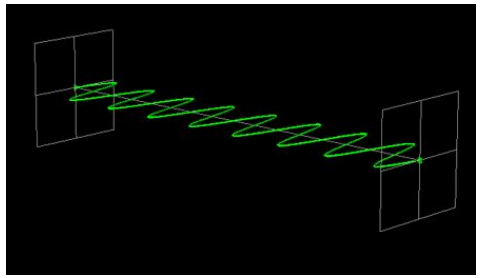
Постоянная Планка, 10^{-34} J×s

Частота оптической волны, ~10^{16} s^{-1}

Поляризация



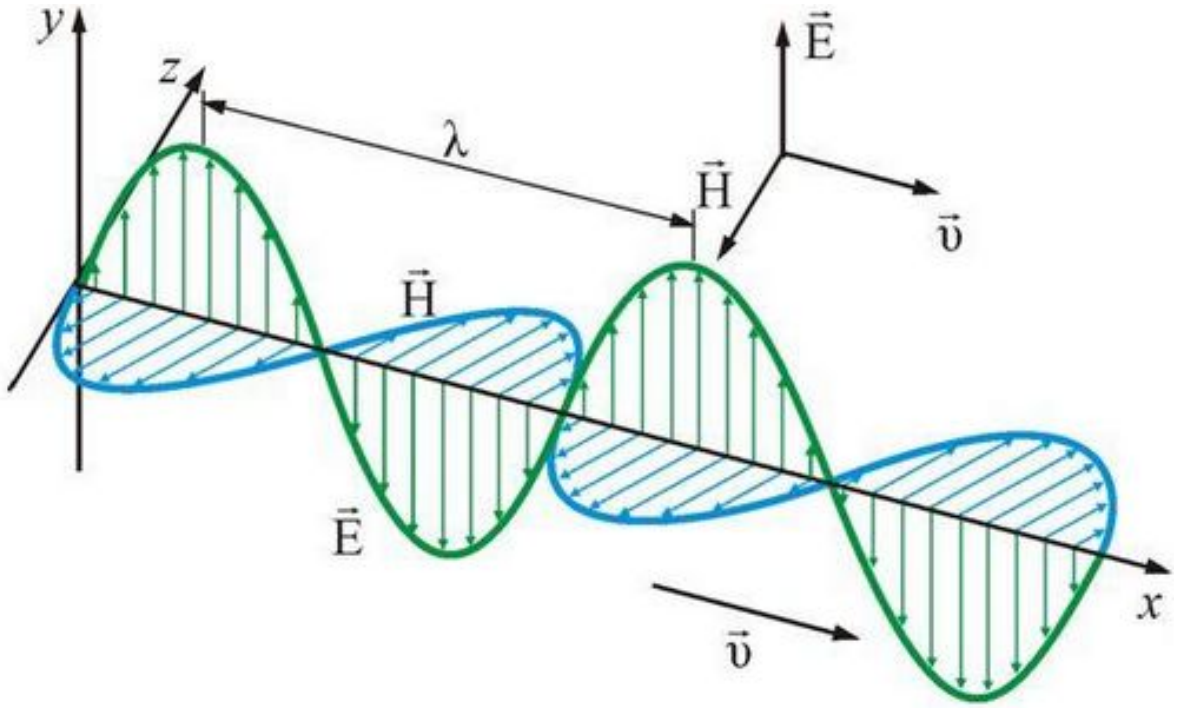


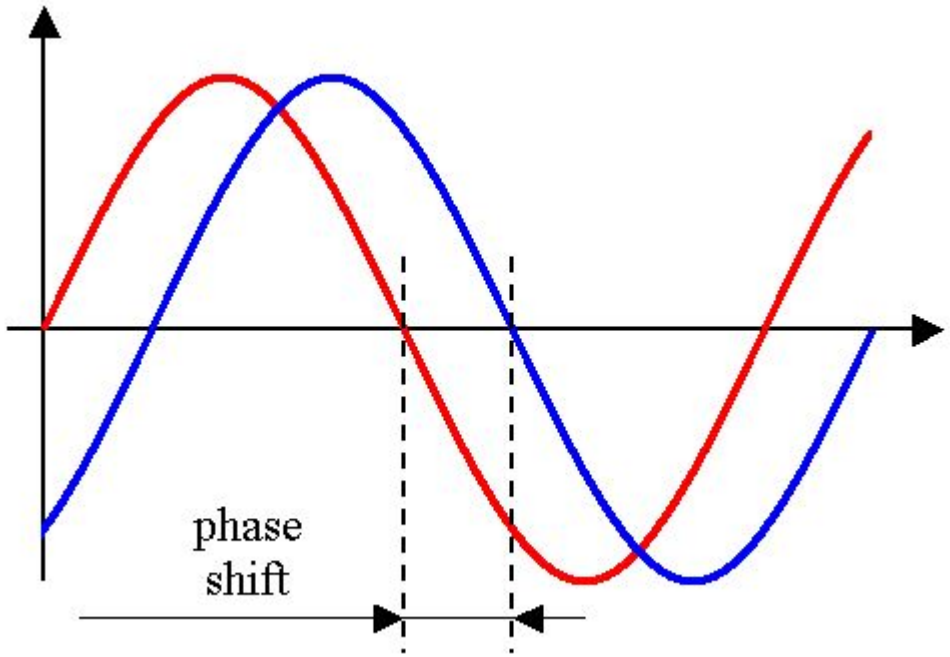


Поляризация = направление колебаний
Присутствует даже в отдельных фотонах. В этом случае говорят о квантовом поляризационном состоянии фотона.
Например:

горизонтальное | вертикальное | диагональное | антидиагональное

Характеристики электромагнитной волны





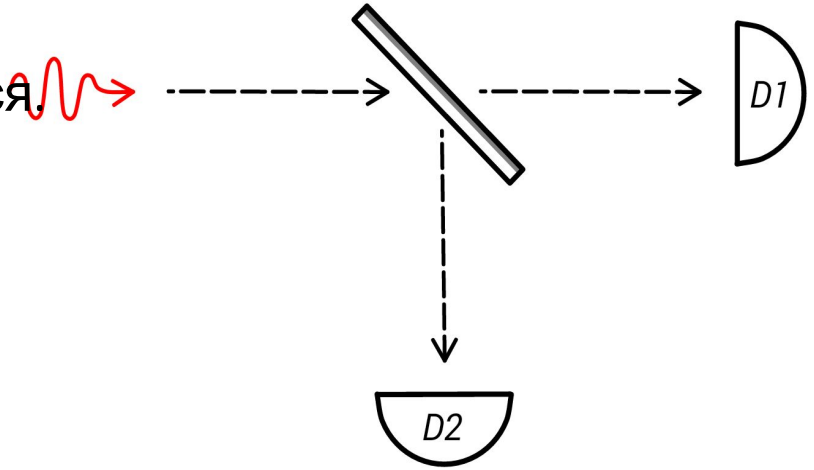
Энергия фотона: E=hν=hc/λ

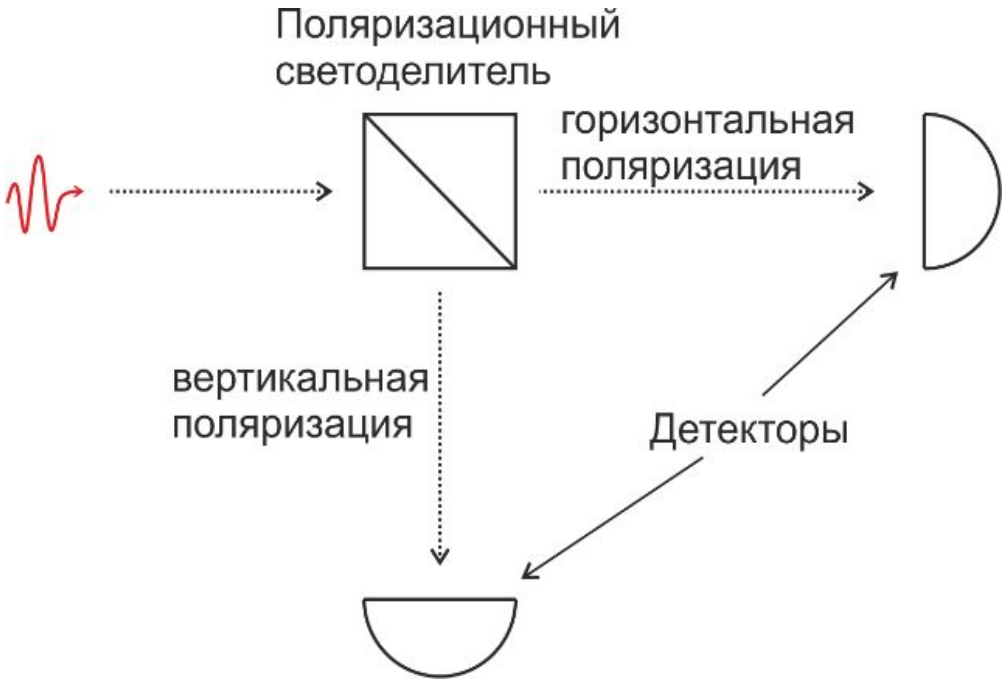
где h - постоянная Планка (6.623·10-34 Дж·с/моль),
ν – частота волны,
λ – длина волны,
c – скорость света (2.998×108 м/с – скорость света в вакууме)

Изменение величины вектора напряженности электрического поля
электромагнитной волны описывается во времени функцией: $E=E_0\sin(\omega t-kx-\varphi)$
где $\Phi = (\omega t - kx - \varphi)$ – фаза колебания (фаза волны)

Однофотонные процессы

- Фотон либо пройдёт через светоделитель, либо отразится
- «Щёлкнет» только один из детекторов
- Предсказать исход в принципе невозможно
- Вероятность каждого исхода = ½

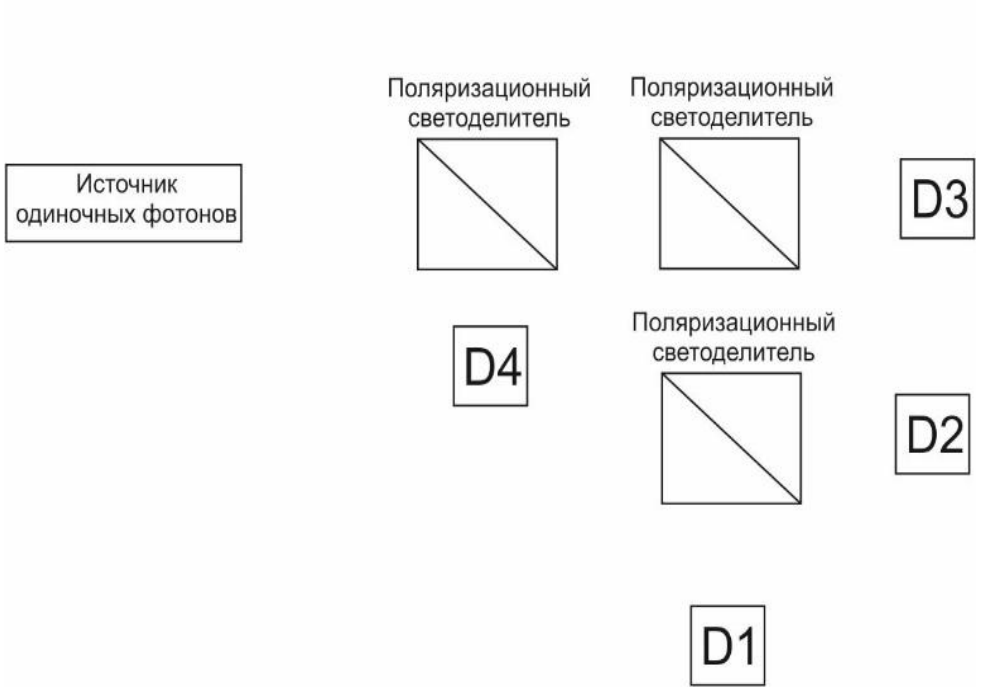




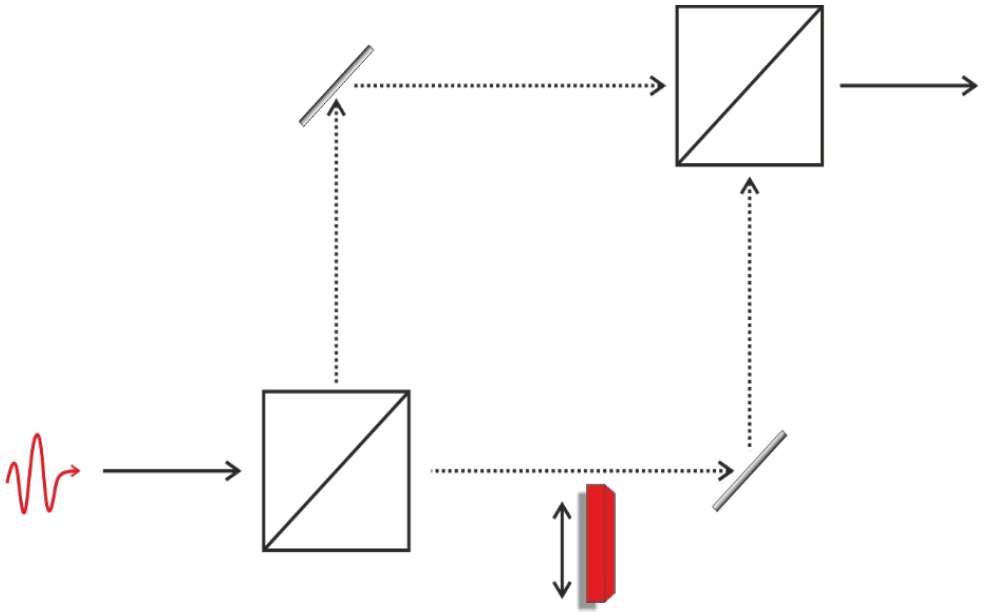
- После измерения поляризации фотона в «неправильном» базисе фотон меняет свое состояние поляризации

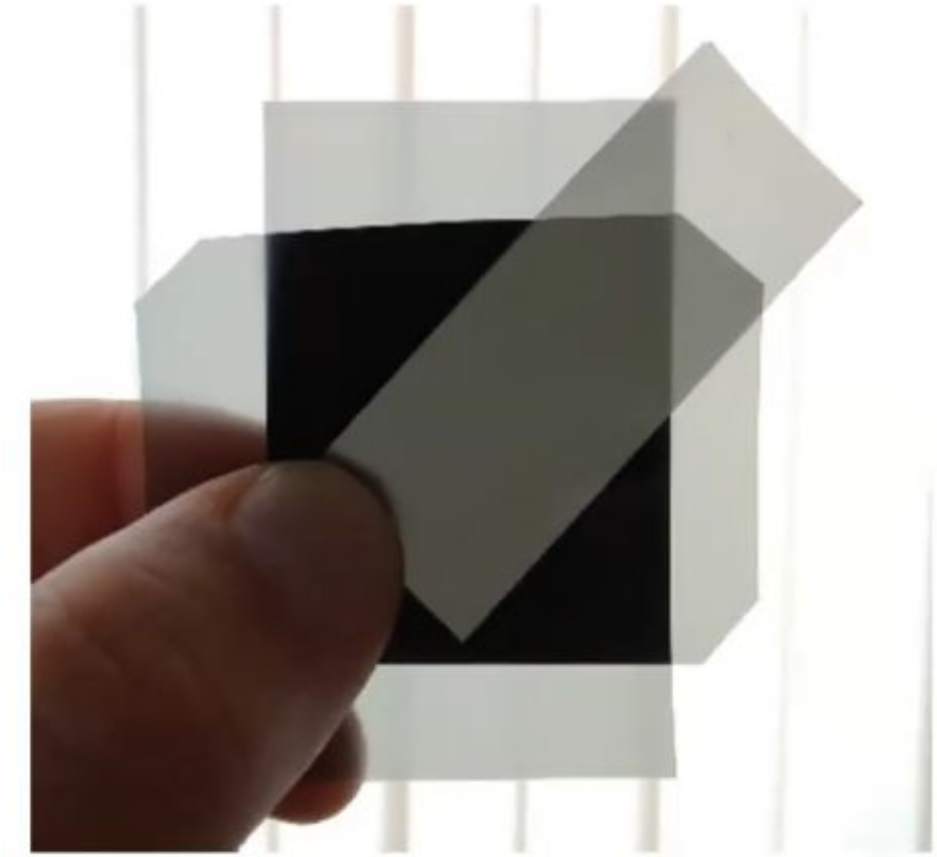
Вопрос 2

Какой детектор и с какой вероятностью будет срабатывать, если на вход схемы подаются фотоны, имеющие диагональную поляризацию.



Квантовая суперпозиция





- Пока над квантовой частицей не проводят измерения, чтобы узнать в каком именно она состоянии, она может находиться словно сразу в нескольких состояниях.
- Но как только мы измеряем ее состояние, фотон выходит из суперпозиции, коллапсирует, до одного состояния.

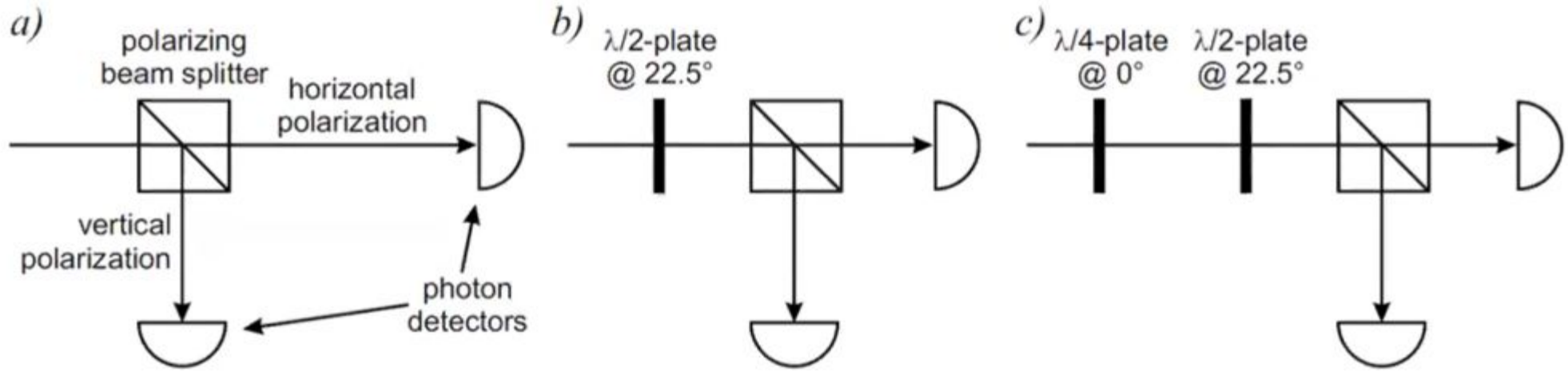
Polarization states

state	matrix	description	notation
$\|H\rangle$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	horizontal	$\|H\rangle$
$\|V\rangle$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	vertical	$\|V\rangle$
$\cos\theta\,\|H\rangle + \sin\theta\,\|V\rangle$	$\begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$	linear polarization at angle θ to horizontal	$\|\theta\rangle$
$\frac{1}{\sqrt{2}}(\|H\rangle + \|V\rangle)$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	diagonal, $+45°$ polarization	$\|+45°\rangle$ or $\|+\rangle$
$\frac{1}{\sqrt{2}}(\|H\rangle - \|V\rangle)$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$	(anti-)diagonal, $-45°$ polarization	$\|-45°\rangle$ or $\|-\rangle$
$\frac{1}{\sqrt{2}}(\|H\rangle + \mathrm{i}\,\|V\rangle)$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}$	right circular polarization	$\|R\rangle$
$\frac{1}{\sqrt{2}}(\|H\rangle - \mathrm{i}\,\|V\rangle)$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}$	left circular polarization	$\|L\rangle$

Jones formalism

Optical element	Orientation	Jones matrix
Linear polarizer	$\parallel x$-axis	$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \rightarrow \begin{matrix} 1 \\ 0 \end{matrix}$
Linear polarizer	φ to x-axis	$\begin{bmatrix} \cos^2\varphi & \sin\varphi\cos\varphi \\ \sin\varphi\cos\varphi & \sin^2\varphi \end{bmatrix}$
Polarization rotator		$\begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix}$
$\lambda/2$-Wave plate	f$\parallel x$-axis	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

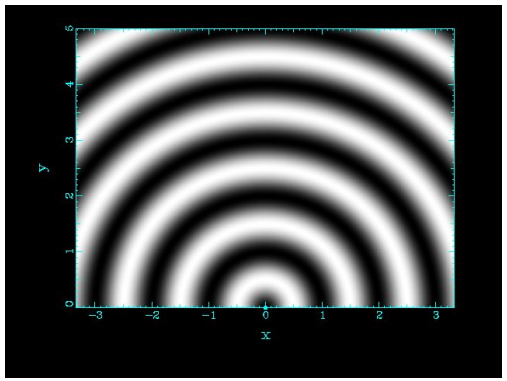
Photon polarization measurements

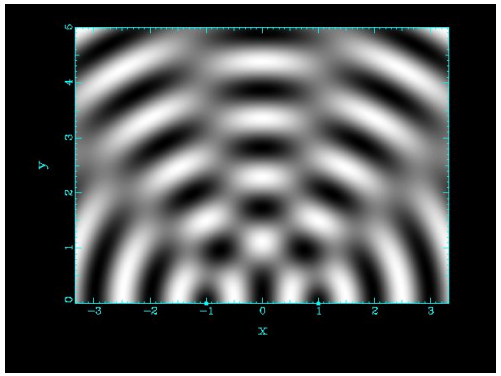


Photon polarization measurements in the canonical (a), diagonal (b), and circular (c) bases

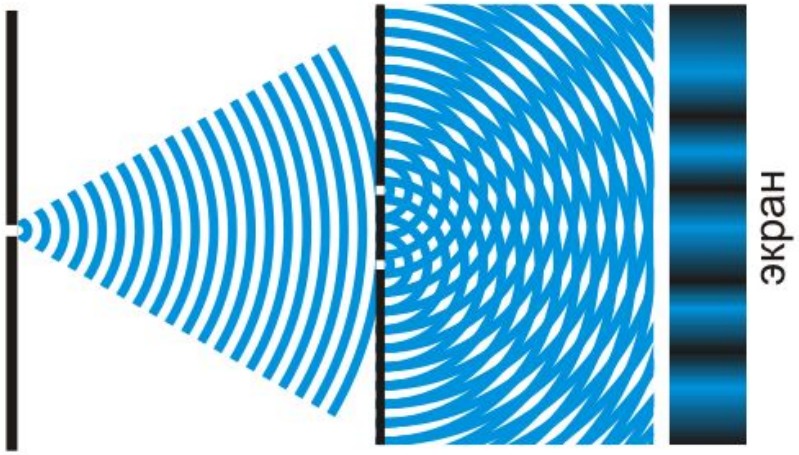
Интерференция

- Волны на поверхности воды

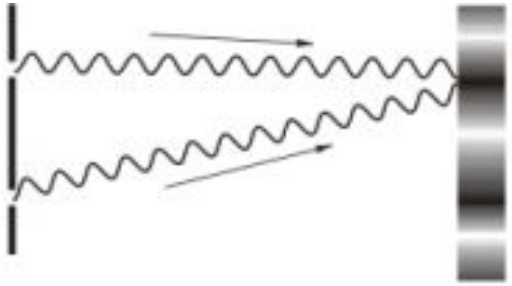




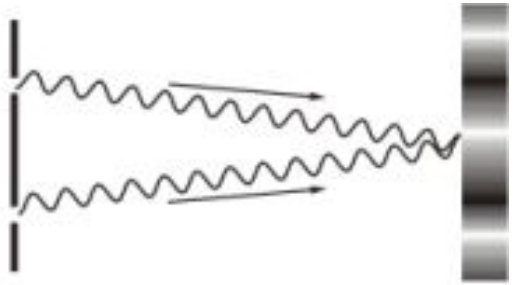
- Интерференция света на двух щелях (Томас Юнг, ~1800)



- Будет ли интерференция конструктивной или ослабляющей, определяется *разницей длин путей* двух волн или разницей фаз этих волн.



а)

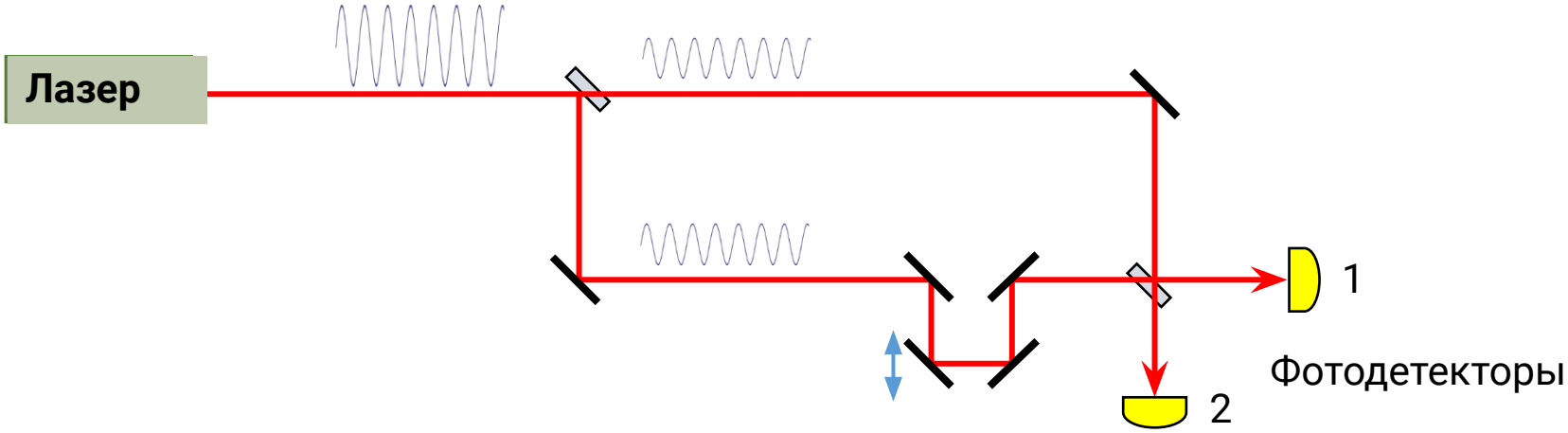


б)

Если волны приходят в данную точку экрана:
а) в одинаковой фазе, они взаимно усиливают друг друга, и на экране в этом месте наблюдается светлая полоса;
б) в противофазе, они взаимно ослабляют друг друга, и на экране в этом месте наблюдается темная полоса.

Интерферометр

Интерферометр = прибор для наблюдения интерференции

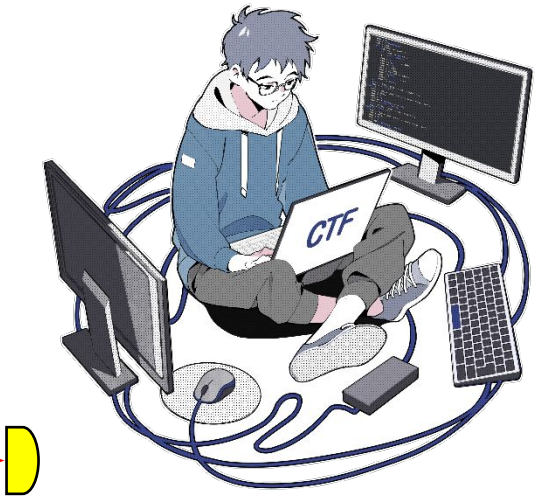


Изменяя длину пути, можно получать конструктивную или ослабляющую интерференцию на каждом из выходов. В сумме выходная мощность постоянна.

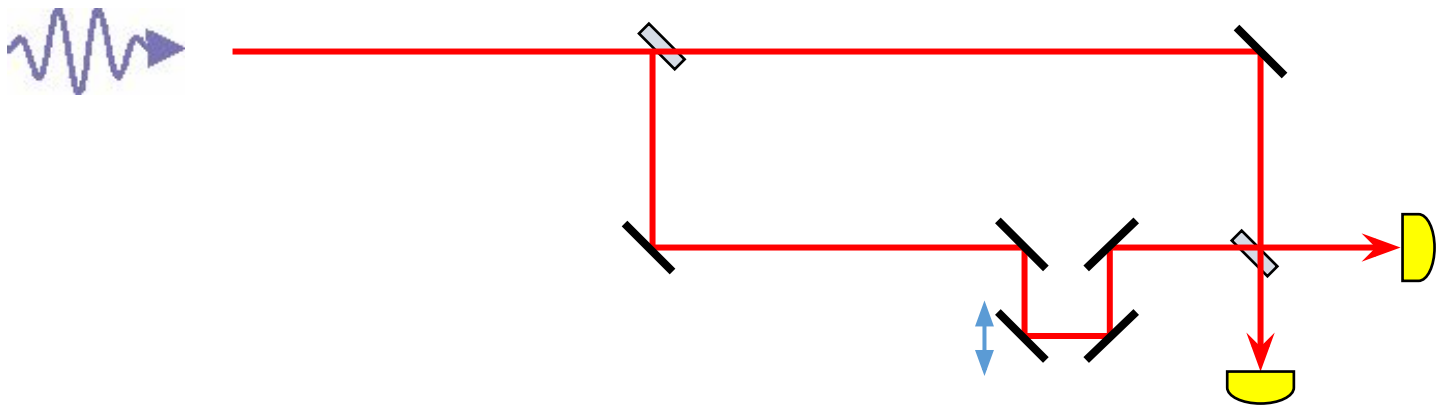
Вопрос 1

Почему в равноплечем интерферометре Маха-Цендера в одном выходе получается конструктивная интерференция, в другом – деструктивная.

Интерферометр с одним фотоном



Эксперимент



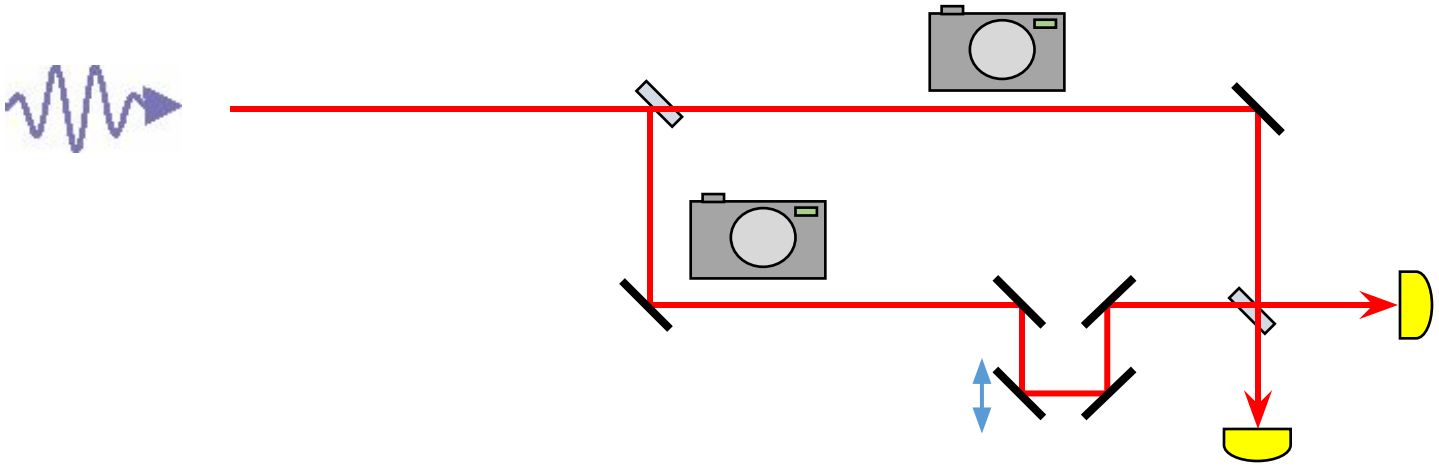
Результат

Вероятность «щелчка» в детекторе

Вероятность «щелчка» в детекторе 2

Интерферометр с одним фотоном

Допустим, один из фотоаппаратов «увидел» фотон



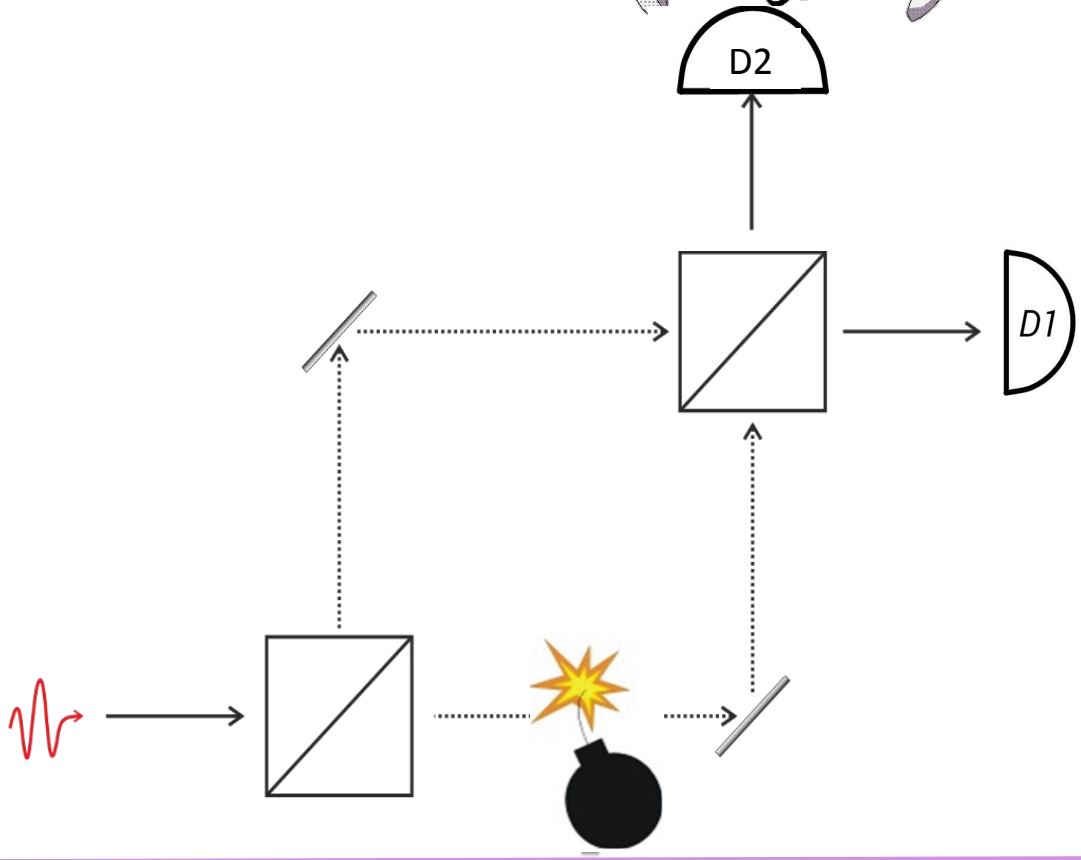
Вероятность «щелчка» в детекторе 1

Вероятность «щелчка» в детекторе 2

Вопрос 3

На складе находятся бомбы с особо чувствительным взрывателем, срабатывающим всего от одного фотона Половина из этих бомб исправна, а половина испорчена. Предположим так же, что исправные бомбы поглощают направленные на них фотоны, а испорченные по какой-то причине –прозрачны для света.

Необходимо определить вид бомбы не взорвав ее.



Вопрос 4

Пусть Ева перехватывает фотоны Алисы и измеряет их в каноническом или диагональном базисе, выбирая случайно. Потом она приготавливает фотон в состоянии, полученном при измерении, и отсылает его Бобу.

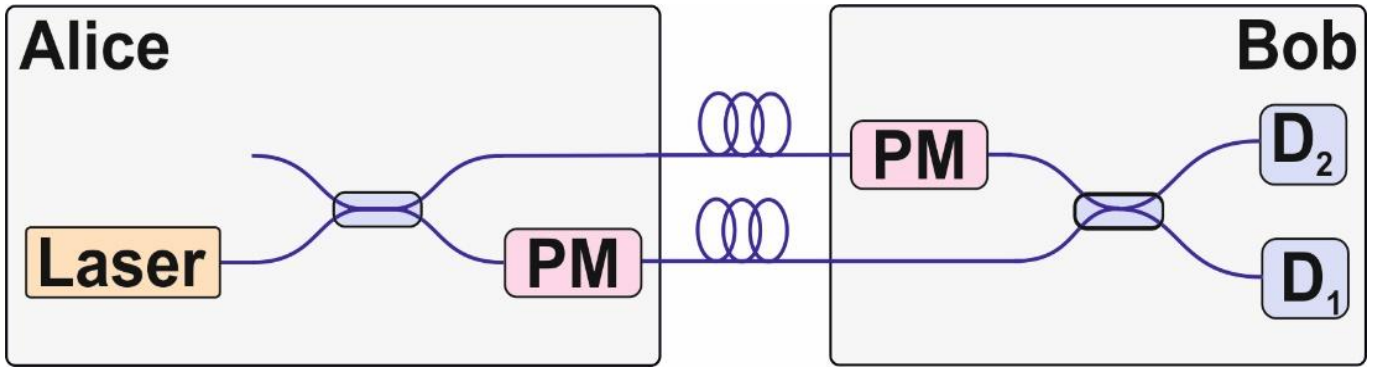
Какую ошибку обнаружат Алиса и Боб, т.е. какая часть бит их секретных ключах в среднем получится разная?

Вопрос 5

Большое количество фотонов, отправленных Алисой, не доходят до Боба. Но Алиса и Боб не знают потерялись ли фотоны из-за рассеяния в линии или были украдены Евой.

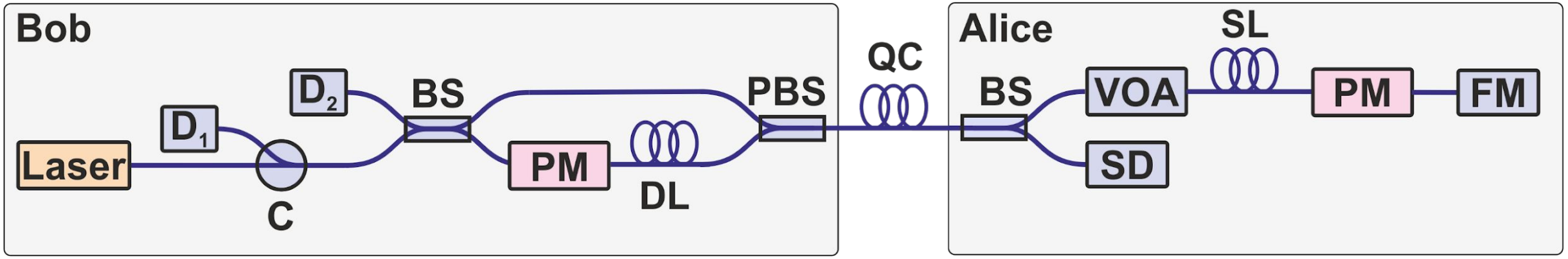
Влияет ли это обстоятельство на секретность квантового распределения ключа?

Фазовое кодирование

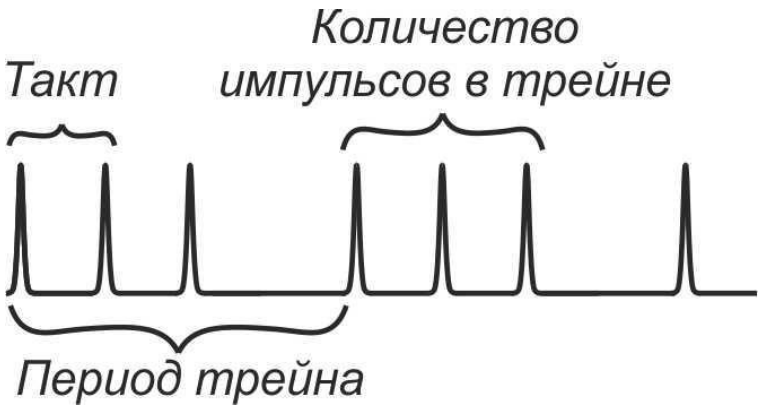


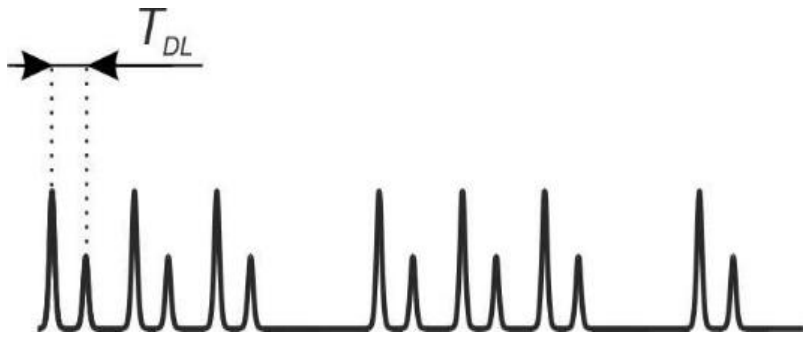
Станция Алиса		Станция Боб		
Значение бита	φ_A	φ_B	$\varphi_A-\varphi_B$	Значение бита
0	0	0	0	0
0	0	$\pi/2$	$3\pi/2$	?
1	π	0	π	1
1	π	$\pi/2$	$\pi/2$	?
0	$\pi/2$	0	$\pi/2$	?
0	$\pi/2$	$\pi/2$	0	0
1	$3\pi/2$	0	$3\pi/2$	?
1	$3\pi/2$	$\pi/2$	π	1

Двухпроходная автокомпенсационная схема Plug&Play



C – циркулятор, D1 и D2 – детекторы одиночных фотонов, PM – фазовые модуляторы, DL – линия задержки, PBS – поляризационный светоделитель, VOA – переменный оптический аттенюатор, SL – накопительная линия, FM – зеркало Фарадея





Вопрос 6

Длина накопительной линии в схеме Plug&Play составляет 25 км. Лазерные импульсы следуют с частотой 5МГц.

Найдите максимальное количество лазерных импульсов в трейне.

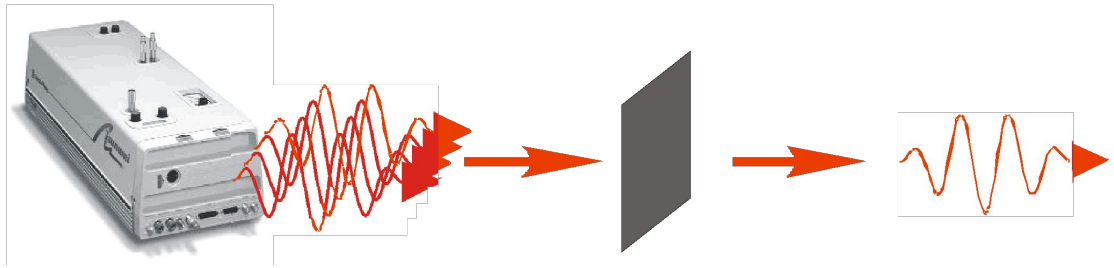
Вопрос 7

Найдите период трейна для квантового канала и накопительной линии по 25 км. Частота следования лазерных импульсов – 5МГц.

Количество импульсов в трейне возьмите из предыдущей задачи.

Как генерировать отдельные фотоны?

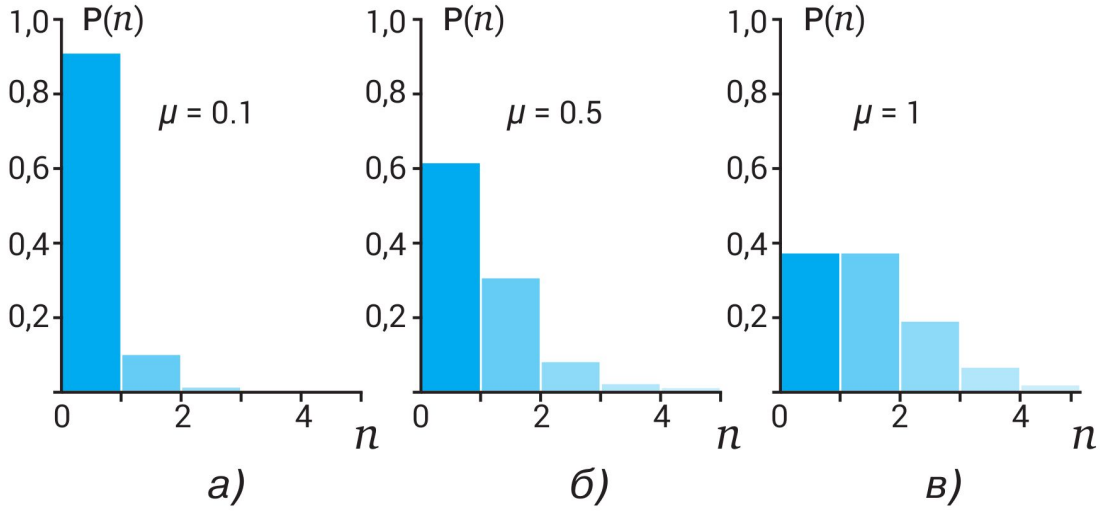
- **Ослабить лазерный луч?**
  - Импульсный лазер



- Результат будет случайным: иногда 0 фотонов, иногда один, иногда больше
- Один фотон только в среднем
- Применимо в квантовой криптографии (с ограничениями)

Статистика Пуассона лазерного излучения: зависимость вероятности числа фотонов n в импульсе интенсивностью μ для (а) μ = 0.1, (б) μ = 0.5 и (в) μ = 1.0.

$$P_0 = \frac{c_0 \nu_0 h \mu}{\lambda}, \qquad \mathrm{P}(n_p, \mu) = \frac{\mu^{n_p}}{n_p!} \exp(-\mu)$$



Вопрос 8

Количество фотонов в лазерном импульсе зависит от (выберите правильный ответ):

а) энергии импульса;

б) энергии и ширины импульса;

в) энергии, ширины и формы импульса;

г) энергии, ширины, формы и поляризации импульса;

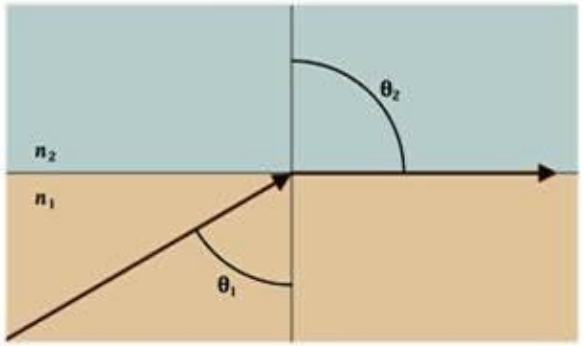
Вопрос 9

Лазер генерирует импульсы с длиной волны 1,55 мкм и с частотой следования 5 МГц. Импульсы содержат по 0,1 фотону в среднем.

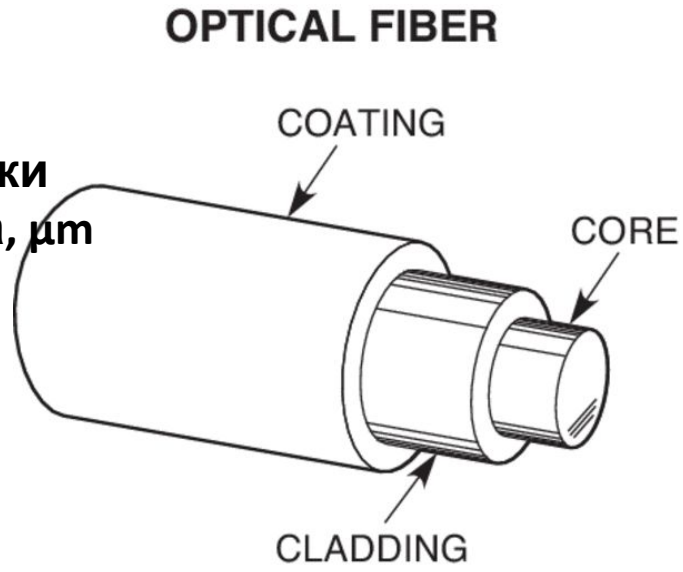
Найдите мощность излучаемого света.

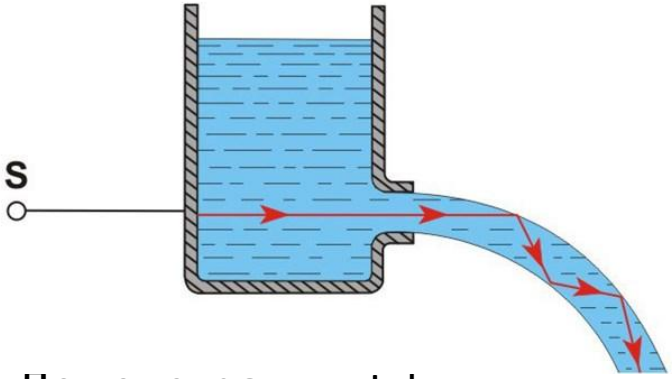
Полное внутреннее отражение

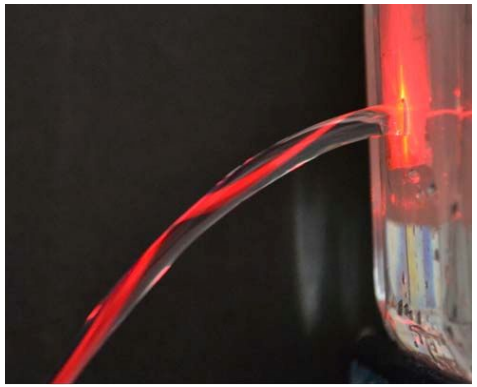
Полное внутреннее отражение



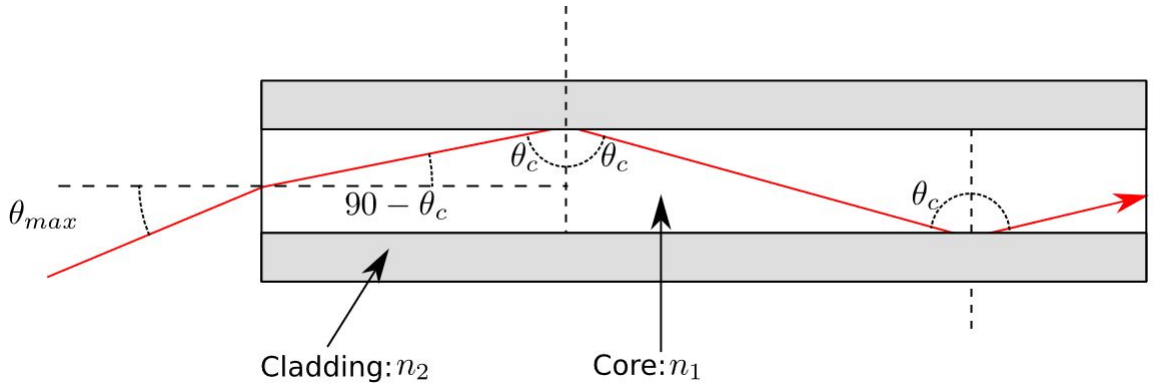
Диаметр сердцевины/оболочки оптического волокна, μm
8/125; 50/125; 62,5/125; 85/125; 100/140







Демонстрация, John Tyndall



Вопрос 10

Какие механизмы потерь могут присутствовать в волоконно-оптической линии связи?

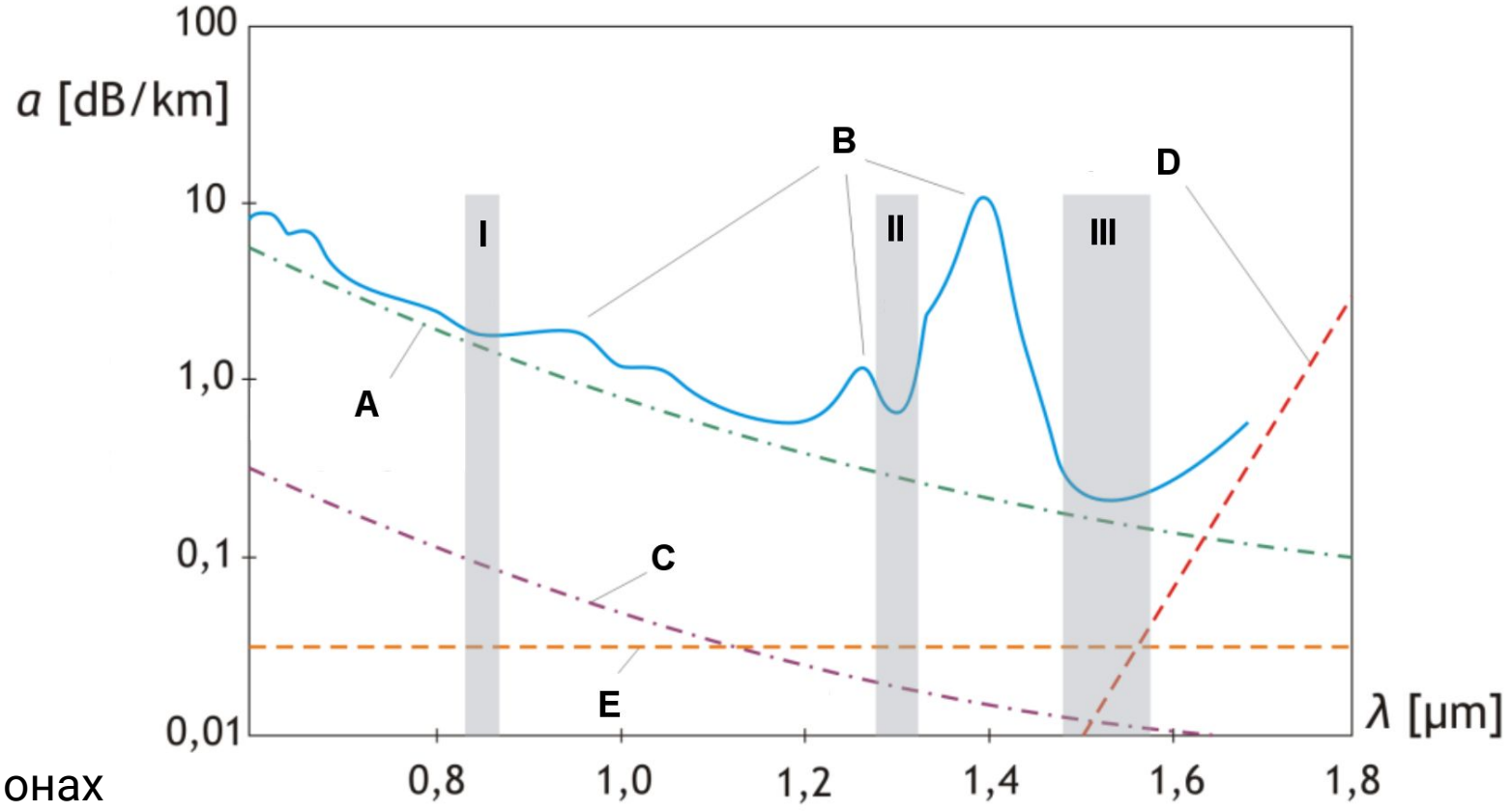
Какие длины волн являются стандартами для телекоммуникации?

Вопрос 11

Алиса посылает фотоны Бобу, по оптоволоконному каналу длиной 100 км. Потери в оптоволокне – 0,3 дБ/км. Какая часть фотонов, посланных Алисой, достигнет Боба?

Потери в оптическом волокне

Уменьшение мощности сигнала при распространении его по волокну

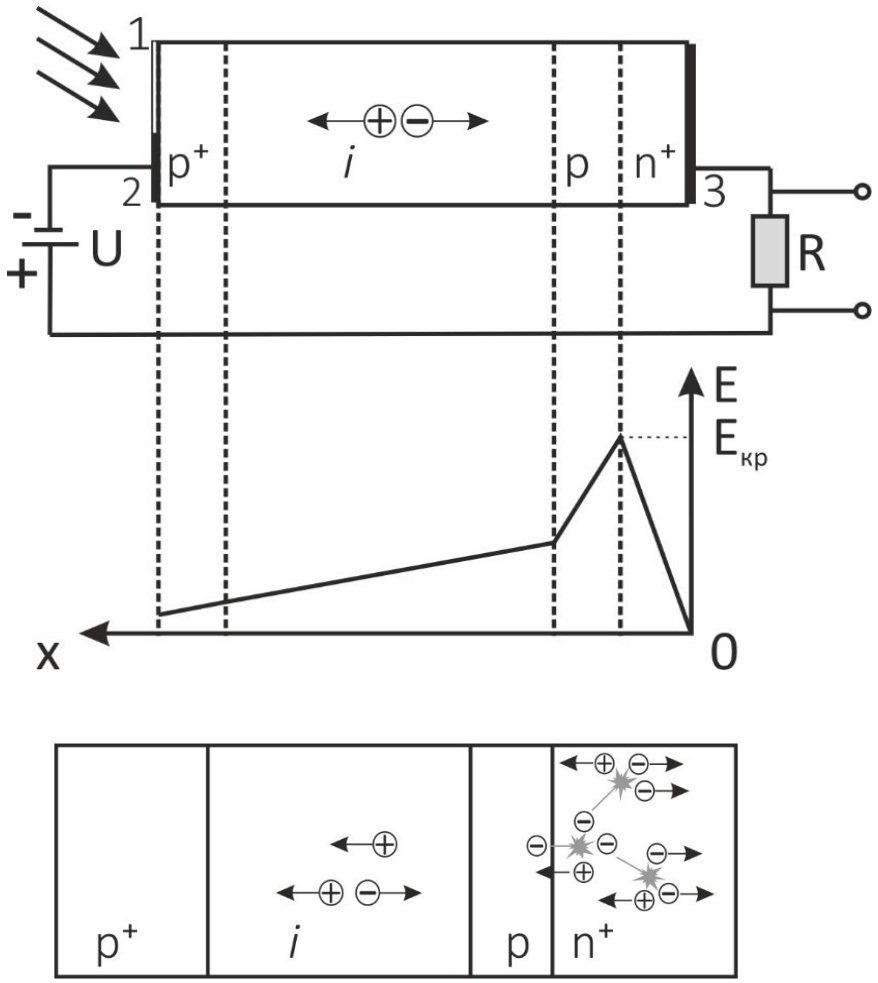


dBm - это децибелы относительно милливатта (mW)

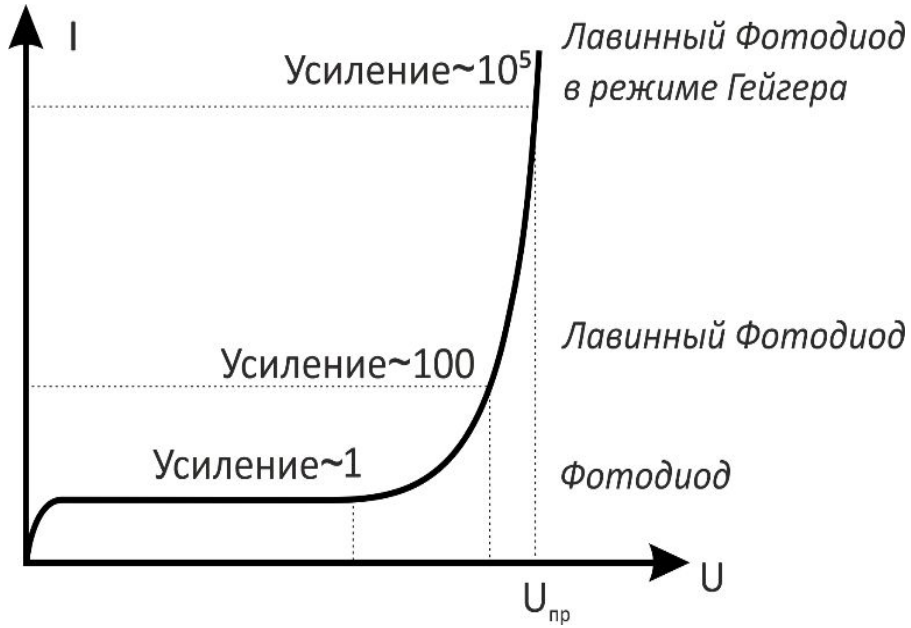
I II III - окна передачи
A - рассеивание Релея $\alpha_R = C/\lambda^4$
B - поглощение в гидроксильных ионах
C - поглощение в ультрафиолете
D - инфракрасное поглощение
E - волноводные потери

Детектор одиночных фотонов

Процесс образования носителей тока в ЛФД



Вольт-амперная характеристика ЛФД



Некоторые характеристики ДОФ

- Спектральный диапазон
- Квантовая эффективность
- Частота темновых отсчетов
- «Мертвое» время

Вопрос 12

От чего зависит частота темновых отсчетов ДОФ?

Чем определяется «мертвое» время ДОФ?

Почему квантовая эффективность ДОФ не равна 1?

Вопрос 13

Чтобы шифровать на лету голос человека методом одноразовых блокнотов нужен ключ, генерируемый со скоростью 5 кбит/с. Пусть лазерные импульсы, следующие с частотой 1 ГГц, содержат 0,1 фотон на импульс; потери в канале 0,3 дБ/км; эффективность детекторов – 10%. Найдите максимальное расстояние квантового распределения ключа по протоколу BB84 для шифрования голоса. Пренебрегите темновым счетом детекторов и возможными атаками Евы с разделением числа фотонов.

Спасибо за внимание!

Головкин Денис
Руководитель специальных проектов

Казиева Татьяна
Кандидат физико-математических наук