Квантова криптография

доц. д-р Лъчезар Георгиев

- Неразбиваеми шифри: Vernam and Shannon
- 1-кубит състояния на поляризирани фотони
- Кв. No-cloning theorem: безусловна сигурност
- Квантов генератор на случайни числа
- QKD протокол BB84
- Privacy amplification: тест за сигурност на BB84
- QKD протокол E91

Шифър на Vernam

“most important in the history of cryptography”

Gilbert Vernam (XOR патент USA, 1917)

Съобщение: последователност от 0 и 1

$$M = 01100110011100101000100010010 0010$$

Ключ: случайна последователност от 0 и 1

$$K = 10110110010100101001010100 1011$$

Кодирано съобщение: $C_i = M_i \oplus K_i \bmod 2$

$$C = 11010000001000000001110110 1001$$

Декодирано съобщение: $D_i = C_i \oplus K_i \bmod 2$

$$D = 01100110011100101000100010010 0010$$

Неразбиваемост (случаен ключ)

(C. Shannon, 1949, ∃ !)

Теорема (версия ЛГ)

За всяко (прехванато) кодирано съобщение $C = M \oplus K \in \boldsymbol{Z}_2^{\,N}$ и за всяко отнапред зададено декодирано съобщение $D' \in \boldsymbol{Z}_2^{\,N}$ съществува ключ $K' \in \boldsymbol{Z}_2^{\,N}$ такъв, че $C \oplus K' = D'$.

Доказателство:

$K' = C \oplus D' \in \boldsymbol{Z}_2^{\,N}$

Допълнение: единственост! (Shannon)

One-time pad шифри

Изводи:

- Съобщението е толкова сигурно колкото ключа
- Ако има повторения в ключа от съобщението може да се извлече вярна информация
- Аферата „Julius and Ethel Rosenberg“ (35 000 one-time pad duplicates от СССР)

Quantum Key Distribution (QKD)

- **Шифър на Vernam:** (неразбиваем) основа
- **Квантов генератор на случайни числа:** източник + beam-splitter + детектори
- **Протокол за споделяне на секретен ключ:** фотони по квантов канал (оптично влакно)
- **Квантови степени на свобода:** поляризация на фотоните
- **Забрана за копиране:** no-cloning theorem

Едно-кубитови състояния

- **Фотони** = кванти/носители на електромагнитното поле (ЕМП)
- **Квантово състояние на фотон:**

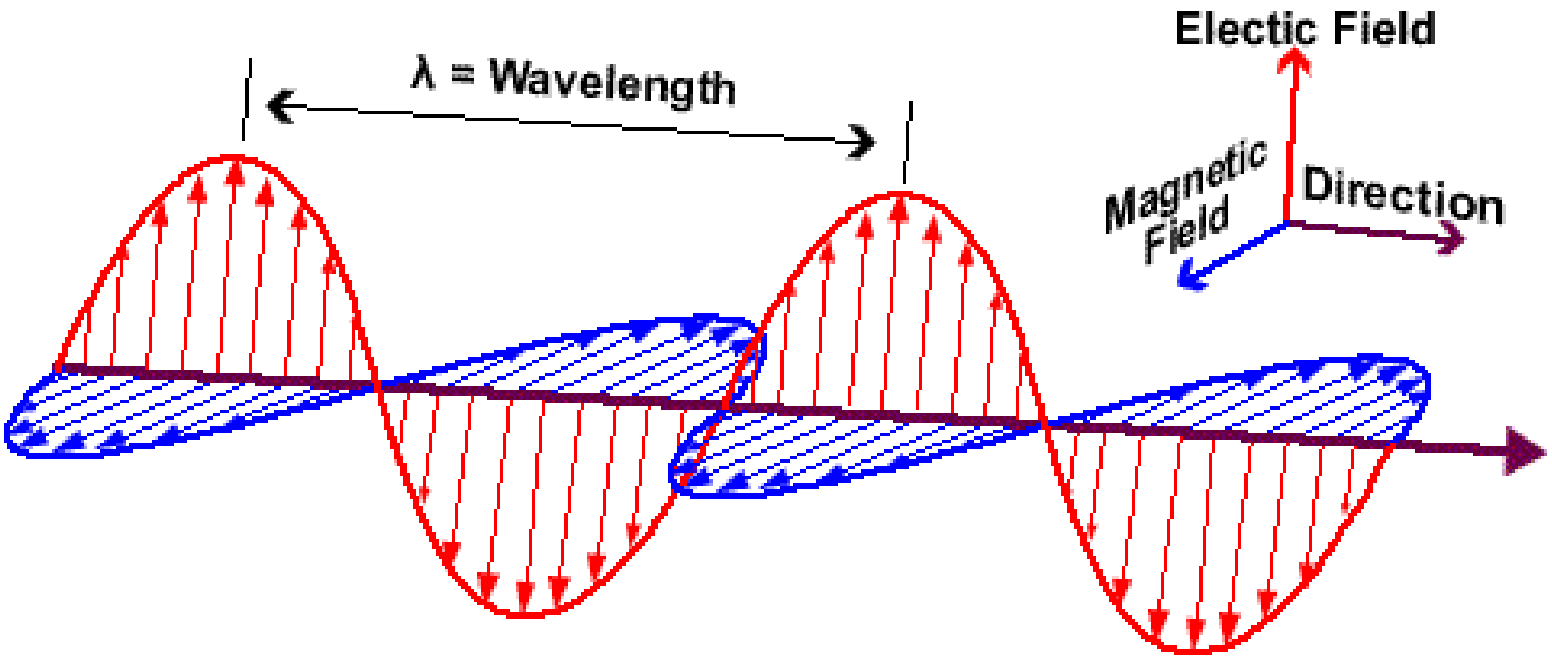
Хилбертово пространство

$$\mathcal{H} = \mathcal{H}_{ext} \otimes \mathcal{H}_{int}$$

- $\mathcal{H}_{ext}$ **описва външни параметри** на фотона (посока, енергия)
- $\mathcal{H}_{int} = \mathbb{C}^2$ **описва вътрешни параметри** на фотона (поляризация)

Линейна поляризация

- Линейно поляризирана светлина (ЕМП)



Линейно поляризирани фотони

- **Поляризирани фотони** (кванти на ЕМП)

  Чисти квантови състояния

  Описват се с вектори на състояния, принадлежащи на Хилбертово пространство

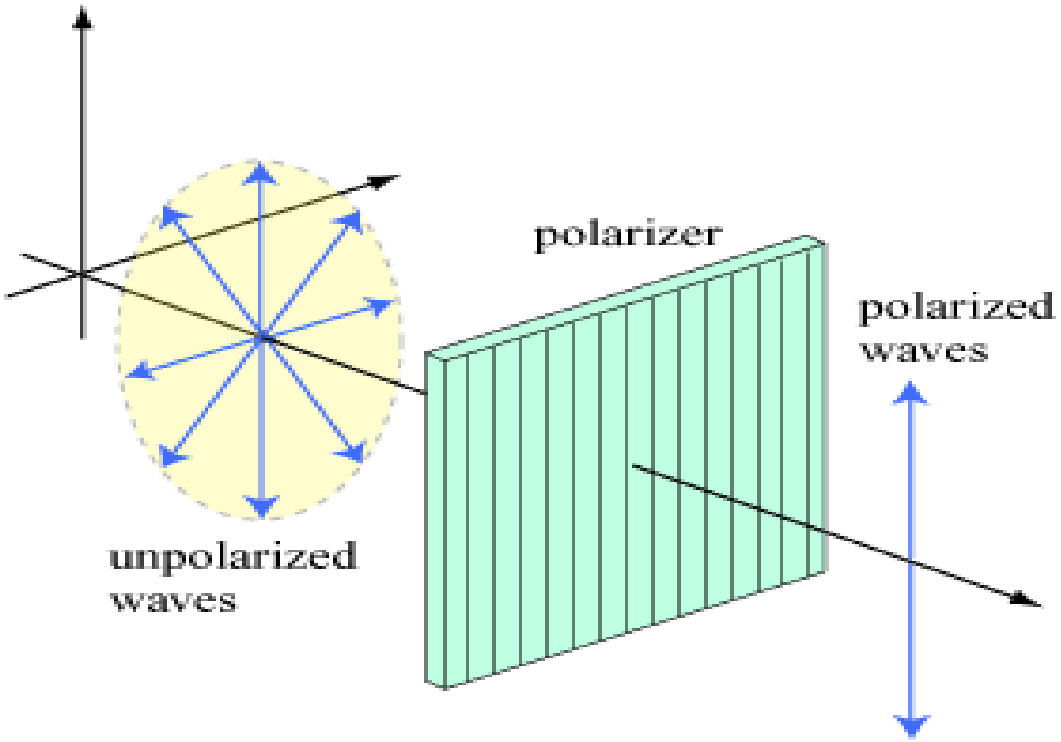
- **Неполяризирана светлина**

  Смесени квантови състояния

  Описват се с матрица на плътността

Поляризатор (кристал $CaCO_3$)

от неполяризирана към поляризирана светлина



Чисти състояния: поляризация

- **Двумерно Хилбертово пространство:** $\mathcal{H}_{int} = \mathbb{C}^2$
- **Квантово състояние**:= фотон с линейна поляризация по произволна ос в равнината определена от векторите $\vec{E}$ и $\vec{H}$

Вектор на състоянието: вектор на поляризацията

- **първи базис:** „+“= $\{|0\rangle, |1\rangle\}$ „правоъгълен“ (rectilinear)

$$\psi = \alpha|0\rangle + \beta|1\rangle,\ \alpha, \beta \in \mathbb{C},\ |\alpha|^2 + |\beta|^2 = 1$$

$|0\rangle =$ фотон с поляризация по оста x
$|1\rangle =$ фотон с поляризация по оста y

„Диагонален“ базис

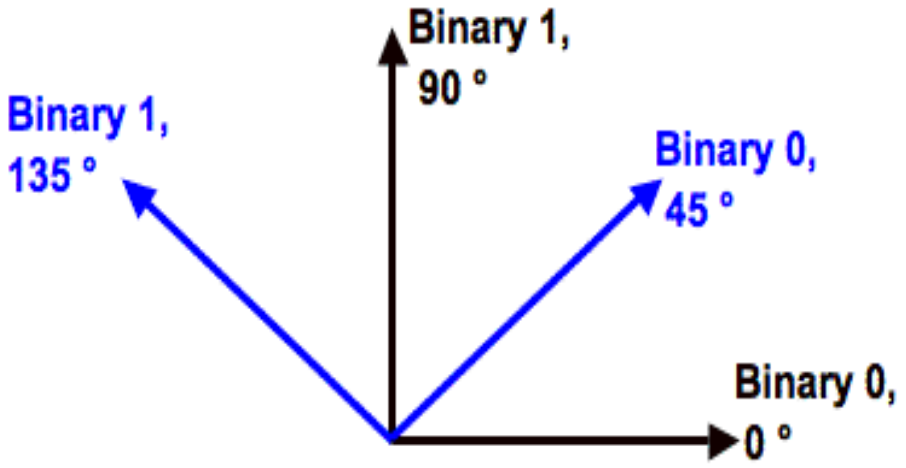
- **Втори базис:**

$$" \times " = \{|+\rangle, |-\rangle\} \text{ (diagonal)}$$

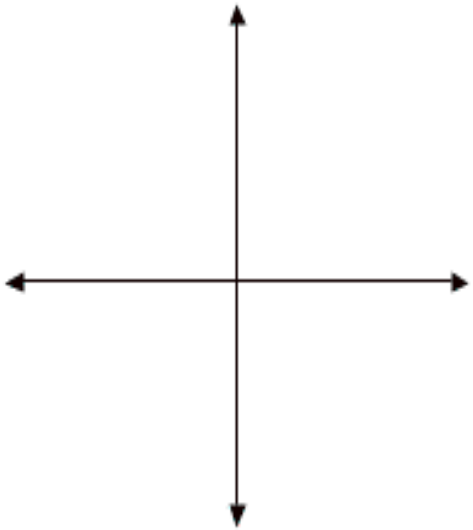
$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$|+\rangle =$ фотон с поляризация под ъгъл 45°

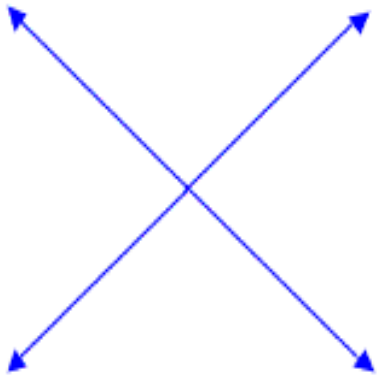
$|-\rangle =$ фотон с поляризация под ъгъл 135°



Photon Polarization



Rectilinear Basis



Diagonal Basis

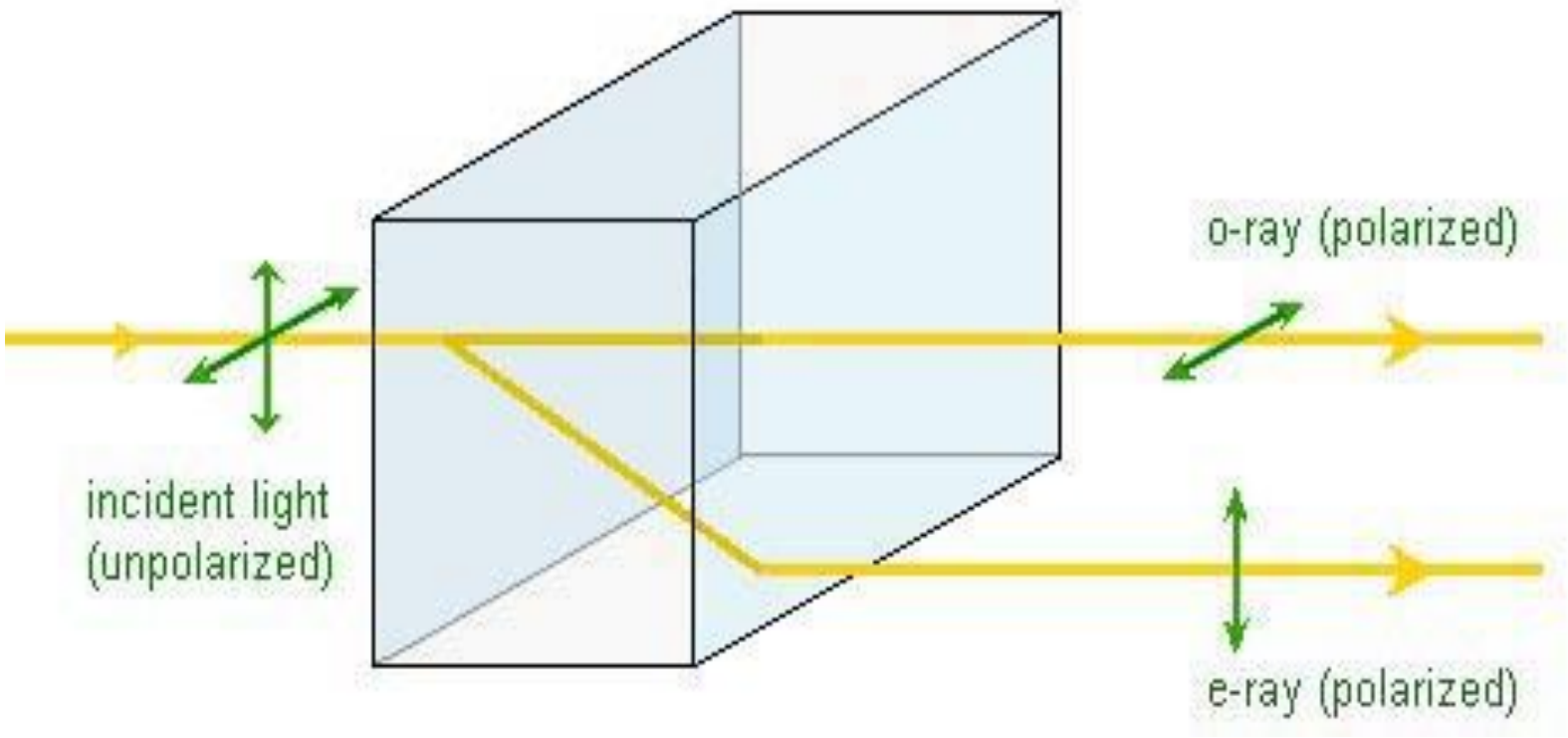
Регистриране на фотони

- Детектори на фотони

- Детектор на поляризирани фотони

  =Поляризатор + детектор

Двойно лъче-пречупване
Polarizing Beam-splitter (birefringent crystal)



Поляризирани фотони: измерване

Нека първоначално фотонът се описва с вектора на състояние $|0\rangle$

Вероятността за регистриране на този фотон в състояние $|0\rangle$ при измерване направено в базиса „+“= $\{|0\rangle, |1\rangle\}$ е

$$Prob(P_0, |0\rangle) = |\langle 0|0\rangle|^2 = 1$$

Докато

Вероятността за регистриране на този фотон в състояние $|1\rangle$ при измерване направено в базиса „+“= $\{|0\rangle, |1\rangle\}$ е

$$Prob(P_1, |0\rangle) = |\langle 1|0\rangle|^2 = 0$$

И обратно: ако първоначално фотонът се описва с вектора на състояние $|1\rangle$ то

$$Prob(P_0, |1\rangle) = 0, \quad Prob(P_1, |1\rangle) = 1$$

Извод:

Ако фотон намиращ се в състояние $|\omega\rangle = |0\rangle$ или $|\omega\rangle = |1\rangle$ е измерен в базиса „+“ = $\{|0\rangle, |1\rangle\}$ то състоянието може еднозначно да бъде определено от вероятностите

$Prob(P_0, |\omega\rangle)$ и $Prob(P_1, |\omega\rangle)$

Поляризирани фотони: неразличимост

Нека сега фотонът се описва с вектора $|+\rangle$

Вероятност за регистриране на този фотон в състояние $|0\rangle$ е

$$Prob(P_0, |+\rangle) = |\langle 0|+\rangle|^2$$
$$= \left|\frac{1}{\sqrt{2}}(\langle 0|0\rangle + \langle 0|1\rangle)\right|^2 = \frac{1}{2}$$

Неразличимост

Също така вероятността за регистриране на този фотон в състояние $|1\rangle$ е

$$Prob(P_1, |+\rangle) = |\langle 1|+\rangle|^2 = \left|\frac{1}{\sqrt{2}}(\langle 1|0\rangle + \langle 1|1\rangle)\right|^2 = \frac{1}{2}$$

- Извод 1: при измерване на фотон описан с $|+\rangle$

в базиса $\{|0\rangle, |1\rangle\}$ в

50% от случаите регистрира детекторът за $|0\rangle$

50% от случаите регистрира детекторът за $|1\rangle$

Неразличимост

Нека сега фотонът се описва с вектора $|-\rangle$

Вероятността за регистриране на този фотон в състояние $|0\rangle$ е

$$Prob(P_0, |-\rangle) = |\langle 0|-\rangle|^2$$
$$= \left|\frac{1}{\sqrt{2}}(\langle 0|0\rangle - \langle 0|1\rangle)\right|^2 = \frac{1}{2}$$

Докато

Вероятността за регистриране на фотон описан с $|-\rangle$ в състояние $|1\rangle$ е

$$Prob(P_1, |-\rangle) = |\langle 1|-\rangle|^2 = \left|\frac{1}{\sqrt{2}}(\langle 1|0\rangle - \langle 1|1\rangle)\right|^2 = \frac{1}{2}$$

- Извод 2: при измерване на фотон описан с $|-\rangle$

в базиса $\{|0\rangle, |1\rangle\}$ в

50% от случаите регистрира детекторът за $|0\rangle$

50% от случаите регистрира детекторът за $|1\rangle$

Общ извод: неразличимост

Ако фотонът е поляризиран хоризонтално или вертикално, а измерването е направено в базиса " $\times$ " $= \{|+\rangle, |-\rangle\}$,

то всички получени вероятности не могат да различат състоянията с хоризонтална поляризация от тези с вертикална,

т.е., не може да се каже дали състоянието е било $|0\rangle$ или $|1\rangle$

Проекционен постулат

В допълнение, след измерването на фотон описван с $|\pm\rangle$ в базиса „+“= $\{|0\rangle, |1\rangle\}$

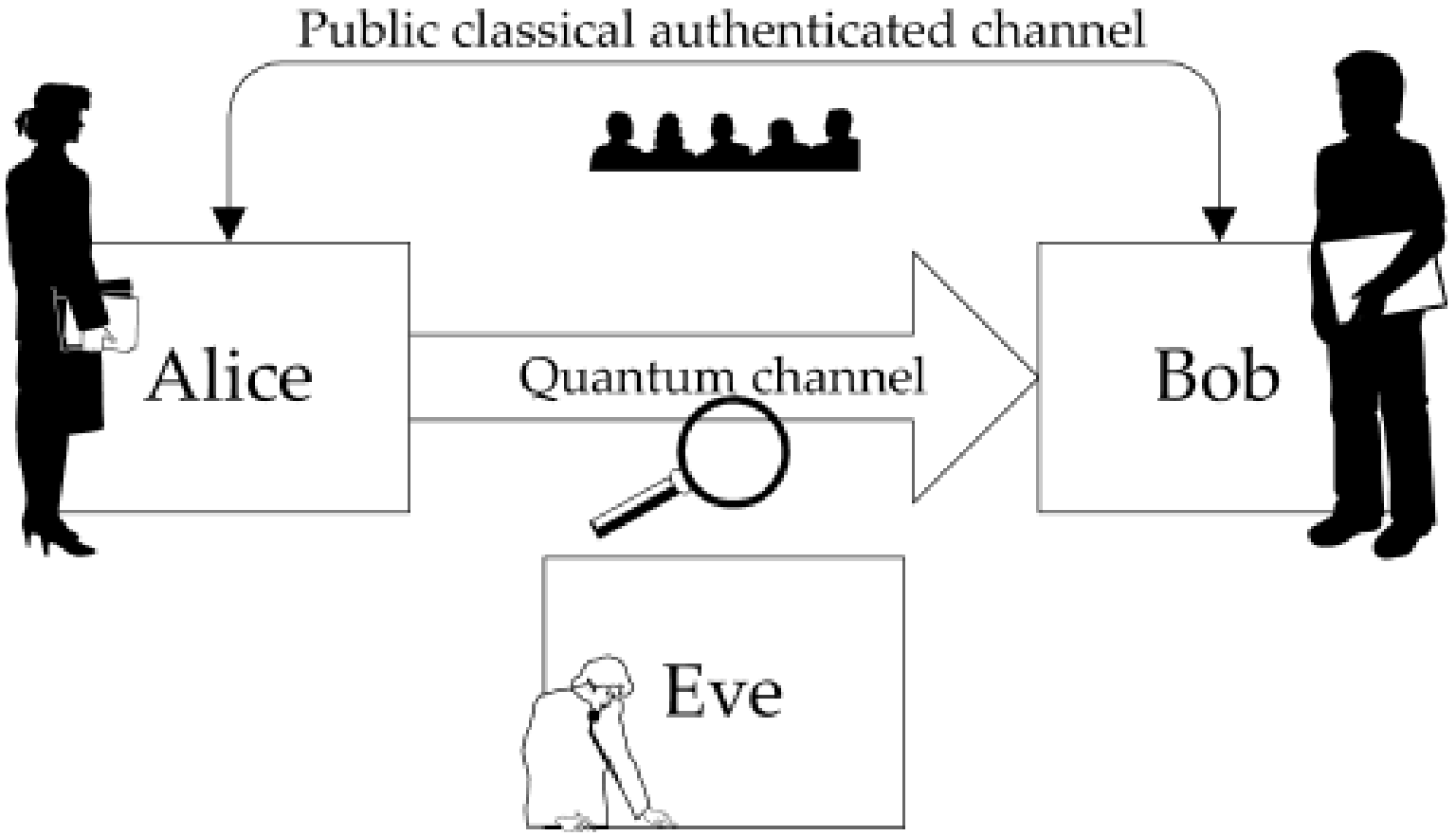
поляризацията му става хоризонтална, ако е настъпило събитието P_0, или вертикална ако е настъпило P_1,

т.е., фотонът напълно „забравя“ своята начална поляризация и преминава респективно в състоянието $|0\rangle$ или $|1\rangle$

QKD: Квантово споделяне на ключ

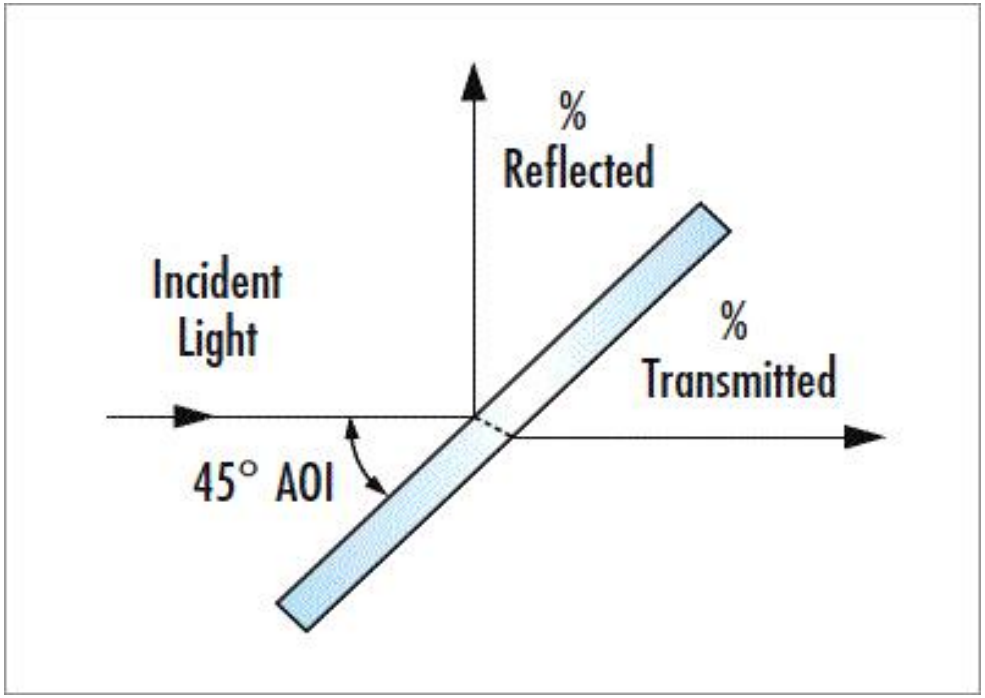
- **Неразбиваем шифър на Vernam**
- **Случаен ключ:** споделен по квантов канал **QKD**
- **Безусловна принципна сигурност:** основана на законите на квантовата физика (**no-cloning theorem**), а не на недоказни предположения за **computational complexity**
- **Заплаха за сигурността:** само в техническото изпълнение (контрамерки)
- **Privacy amplification:** тест за подслушване (всяко подслушване е откриваемо)

QKD протокол Bennett-Brassard 1984 (BB84)

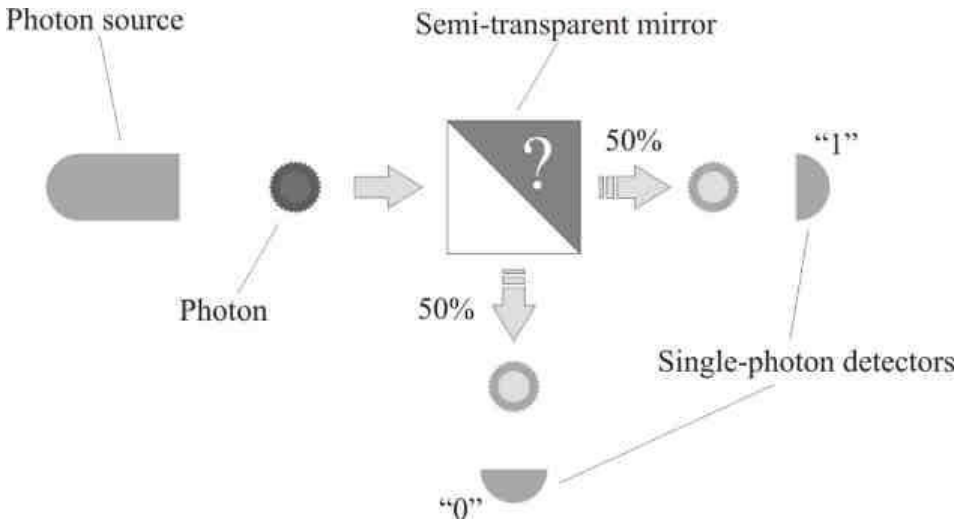


Квантов генератор на сл. числа

- Генератор на случайни числа: източник
- 50-50 Beam-splitter (BS)



Quantum random number generator ID Quantique, Swiss



BB84: стъпки A

1. Alice използва квантов генератор на случайни числа за да генерира случайна последователност
   $$0110011100010101000111000111 00$$

За всеки бит Alice избира случайно в кой от двата базиса $+$ или $\times$ да поляризира фотоните, които изпраща на Bob

2. Ако базисът е + тогава поляризацията е $0 = \leftrightarrow$ или $1 = \updownarrow$
3. Ако базисът е $\times$ тогава поляризацията е $0 = \nwarrow\searrow$ или $1 = \nearrow\swarrow$ (или обратното)

BB84: стъпки B

1. Bob приема фотоните изпратени по квантовия канал от Alice и за всеки от тях решава случайно дали да ги измери в базис + или × чрез завъртане на поляризатора пред детектора

2. Bob записва резултатите от измерванията за всеки фотон заедно с типа + или × на поляризатора; резултатите са:

Резултати от измерванията на Bob

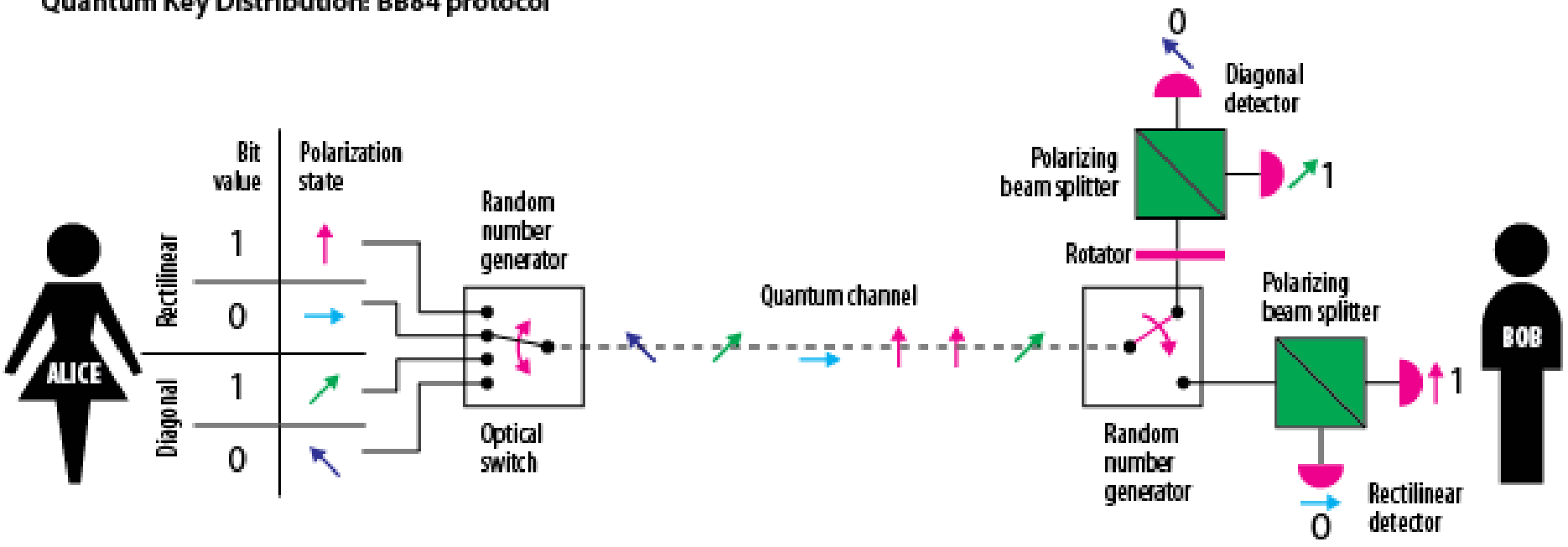
- 0 ако е регистрирал детектора за хоризонтална поляризация при поляризатор в базис +
- 1 ако е регистрирал детектора за вертикална поляризация при поляризатор в базис +
- 0 ако е регистрирал детектора за поляризация 135° при поляризатор в базис $\times$
- 1 ако е регистрирал детектора за за поляризация 45° при поляризатор в базис $\times$

BB84: С-сравняване на базисите

- Bob се обажда на Alice по телефона и за всеки бит съобщава в кой базис е мерил, без да споменава резултатът от измерванията

- Alice потвърждава номерата на битовете, за които базисът на Bob съвпада с нейния и тези битове стават основата на секретния ключ

Quantum Key Distribution: BB84 protocol



Quantum transmission & detection	ALICE sends photons	↖	↗	→	↑	↑	↗	↖	↑
	ALICE's random bits	0	1	0	1	1	1	0	1
	BOB's detection events	↑	↗	↖	↑	↗	↗	↖	↖
	BOB's detected bit values	1	1	0	1	1	1	0	0
Public discussion (i.e., sifting)	BOB tells ALICE the basis choices he made	Rect	Diag	Diag	Rect	Diag	Diag	Diag	Diag
	ALICE tells BOB which bits to keep		✔		✔		✔	✔	
	ALICE and BOB's shared sifted key	–	1	–	1	–	1	0	–

BB84: стъпки Eve - 25 % корупция

- Eve измерва ∀ фотони с номера от 1 до 8
- **Базиси:** +, ×, +, ×, +, ×, +, ×
- **Резултат:** 1, 1, 0, 0, 1, 1, 1, 0
- **Споделен ключ A&B:** -, 1, -, 1, -, 1, 0, -
- **Проектирано състояние (Bob):** ↕, ↗, ↔, ↖, ↕, ↗, ↕, ↖
- **Резултат Bob^E:** 1, 1, 0, 0, 1, 1, 0, 0
- **Намесата на Eve:** **25 % разминаване!!!**

Тест за подслушване

Alice и Bob се договарят и споделят по публичния канал подредица на вече установения секретен ключ, която след публикуването се изважда от ключа.

- **Идеален канал**: ако подредицата избрана от Alice и Bob е идентична, останалата част от споделената редица се приема за окончателен споделен ключ. Ако подредиците не са идентични - налице е подслушване. Процедурата започва отначало.

- **Шумен канал:** ако подредицата избрана от Alice и Bob съдържа повече грешки от допустимата грешка на канала (която се определя от характеристиките на квантовия канал), се предполага, че е имало подслушване. В противен случай остатъка от редицата от битове се приема за окончателен ключ.

Корекции на грешки

- В реалността квантовият канал е „шумен“ и тогава може да се окаже, че Alice и Bob притежават различни ключове след споделянето на ключа.
- Един възможен изход е Alice да използва класически методи за корекция на грешки (напр. Repetition code) преди да изпрати битовете по квантовия канал.
- По време на фазата за корекция на грешки Alice изпраща на Bob информация за начина на кодиране,така че Bob също да може да приложи метода за декодиране.
- Накрая Alice и Bob би трябвало да споделят един и същи секретен ключ.

Забрана за копиране

- **Измерване: проекционен постулат**
  необратима пертурбация на квантовото състояние
- **Предаване на измереното състояние:**
  загуба на първоначалната информация
- **Копиране преди измерването**

- **No-cloning theorem:**
  Не може да бъде копирано неизвестно квантово състояние.

No-cloning theorem

- Копиране на чисти състояния = клониране (дупликиране, запазваме оригинала непроменен и независим)
- Резултат от копирането: разложимо състояние с идентични фактори

$$|\psi\rangle_A \otimes |0\rangle_B \rightarrow |\psi\rangle_A \otimes |\psi\rangle_B$$

- „Класическо“ копиране: унитарен оператор

$$U(|0\rangle_A \otimes |0\rangle_B) = |0\rangle_A \otimes |0\rangle_B$$
$$U(|1\rangle_A \otimes |0\rangle_B) = |1\rangle_A \otimes |1\rangle_B$$

Продължение по линейност

- **Неизвестно** състояние $|\psi\rangle_A = \alpha|0\rangle_A + \beta|1\rangle_A$
- $U([\alpha|0\rangle_A + \beta|1\rangle_A]\otimes|0\rangle_B) =$
  $\alpha|0\rangle_A\otimes|0\rangle_B + \beta|1\rangle_A\otimes|1\rangle_B$
- **Копиране:**
  $|\psi\rangle_A\otimes|\psi\rangle_B$
  $= \alpha^2|0\rangle_A\otimes|0\rangle_B + \alpha\beta|0\rangle_A\otimes|1\rangle_B + \beta\alpha|1\rangle_A\otimes|0\rangle_B$
  $+ \beta^2|1\rangle_A\otimes|1\rangle_B$
- **Сравнение:** $\alpha\beta = 0, \alpha^2 = \alpha, \beta^2 = \beta$

Извод

- Копиране на чисто квантово състояние $|\psi\rangle_A = \alpha|0\rangle_A + \beta|1\rangle_A$
- чрез линеен оператор е възможно само ако

$$\alpha = 0, \beta = 1, \quad \text{или} \quad \alpha = 1, \beta = 0,$$

т.е., могат да се копират само известни и ортогонални квантови състояния като

$|0\rangle_A$ или $|1\rangle_A$, но не и общи състояния!

Неортог. копиране = пертурбация

- Нека $|\psi\rangle$ и $|\phi\rangle$ са две **неортогонални състояния**, т.е., $\langle\psi|\phi\rangle \neq 0$
- Нека $\mathcal{H}_E$ е Хилб. пр-во достъпно за Eve
- **Непертурбирано** копиране

$$U(|\psi\rangle_A \otimes |0\rangle_E) = |\psi\rangle_A \otimes |\psi\rangle_E$$
$$U(|\phi\rangle_A \otimes |0\rangle_E) = |\phi\rangle_A \otimes |\phi\rangle_E$$

- **Унитарност:**

$${}_A\langle\psi|\phi\rangle_A = {}_E\langle 0| \otimes {}_A\langle\psi|\phi\rangle_A \otimes |0\rangle_E$$

$$= {}_E\langle\psi| \otimes {}_A\langle\psi|\phi\rangle_A \otimes |\phi\rangle_E = {}_A\langle\psi|\phi\rangle_A \cdot {}_E\langle\psi|\phi\rangle_E$$

Неортогогонално копиране

$\langle\psi|\phi\rangle \neq 0 \Rightarrow {}_E\langle\psi|\phi\rangle_E = 1 \Rightarrow$

$|\phi\rangle_E = e^{i\beta}|\psi\rangle_E$ (идентичност)

Доказателство: нека $|\phi\rangle_E = e^{i\beta}|\psi\rangle_E + |v\rangle_E$, такова, че ${}_E\langle v|\phi\rangle_E = 0$.

Тогава $\langle\psi|\psi\rangle_E = {}_E\langle\phi|\phi\rangle_E + {}_E\langle v|v\rangle_E = 1$

$\Rightarrow {}_E\langle v|v\rangle_E = 0$

N.B.: $\langle\psi|\psi\rangle_A = {}_E\langle 0|0\rangle_E = 1 \Rightarrow {}_E\langle\psi|\psi\rangle_E = 1$

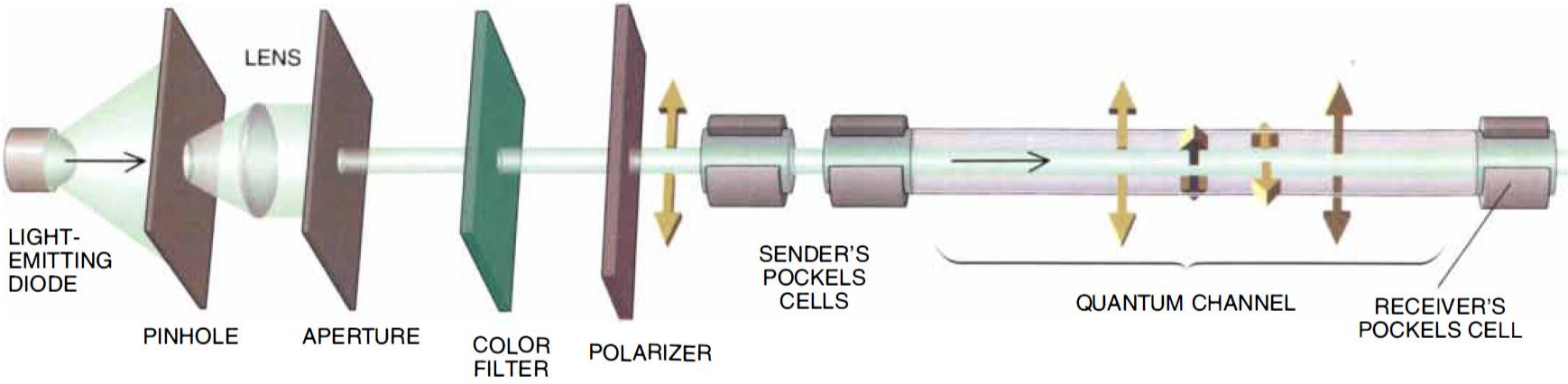
Изводи: no-cloning

- Не е възможно да се придобие информация разграничаваща неортогонални състояния без да бъдат пертурбирани (само разложими състояния)

- Никакво измерване в пространството на Eve $\mathcal{H}_E$ не може да разкрие информация, която да различи $|\phi\rangle_A$ от $|\psi\rangle_A$ ако $_A\langle\psi|\phi\rangle_A \neq 0$.

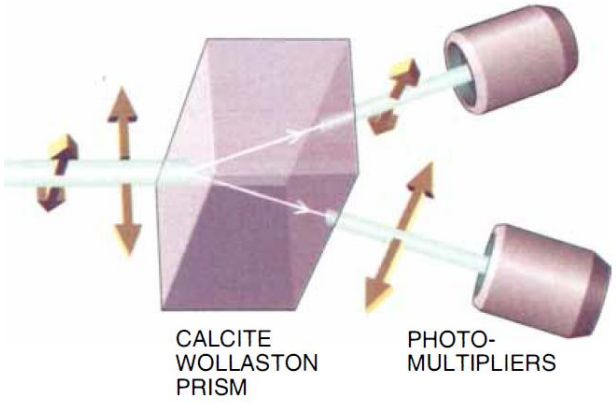
Privacy amplification phase

- One problem remains. Eve can still have quite a bit of information about the key both Alice and Bob share. Privacy amplification is a tool to deal with such a case.
- Privacy amplification is a method how to select a short and very secret binary string *s* from a longer but less secret string *s'*. The main idea is simple. If $|s| = n$, then one picks up n random subsets $S_1,\ldots, S_n$ of bits of s' and let s_i, the i-th bit of S, be the parity of S_i. One way to do it is to take a random binary matrix of size $|s| \times |s'|$ and to perform multiplication Ms'^T, where s'^T is the binary column vector corresponding to s'.
- The point is that even in the case where an eavesdropper knows quite a few bits of *s'*, she will have almost no information about *s*.
- More precisely, if Eve knows parity bits of k subsets of s', then if a random subset of bits of s' is chosen, then the probability that Eve has any information about its parity bit is less than $2^{-(n-k-1)} / \ln 2$.



QUANTUM SYSTEM can distribute information in perfect secrecy. The transmitter produces faint flashes of green light from a light-emitting diode. The pinhole, lens and filter create a collimated beam of dim flashes. The light is then polarized horizontally. Two Pockels cells change the polarization to 0, 45, 90 or 135 degrees. The polarized light flashes are released from the transmitter and eventually reach the receiver. There another Pockels cell shifts the polarization by either 45 degrees or not at all. The action of this Pockels cell allows the receiver to choose between measuring rectilinear or diagonal

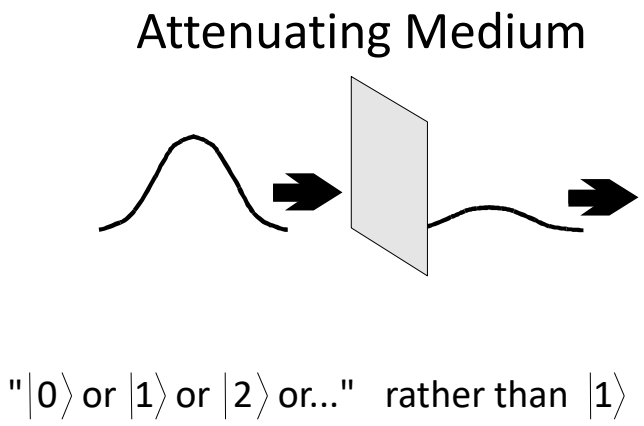
1. LED produces faint flashes of green light.
2. Pinhole, lens, and filter turn dim flashes into a collimated beam.
3. Light beam is polarized horizontally.
4. Pockels cells randomly select an orientation of 45,90, 135 or 180 degrees.
5. Polarized light leaves the transmitter and enters the fiber optic.
6. The polarized photons enter the reciever where another pockels cell randomly chooses to measure rectilinear or diagonal polarization
7. The Prism directs the photons to respective photo-multipliers depending on their polarization

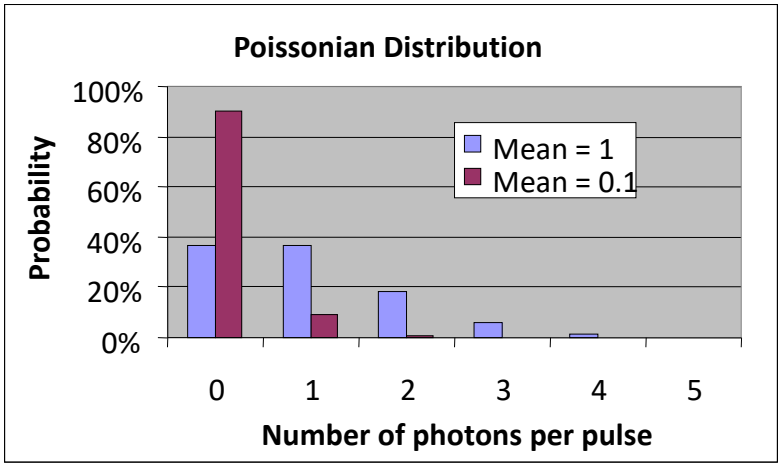


polarization. In the rectilinear case, a horizontally polarized photon will be directed toward the right photomultiplier; a vertically polarized photon will be directed toward the left photomultiplier.

Генериране на единични фотони

Attenuated Laser Pulse

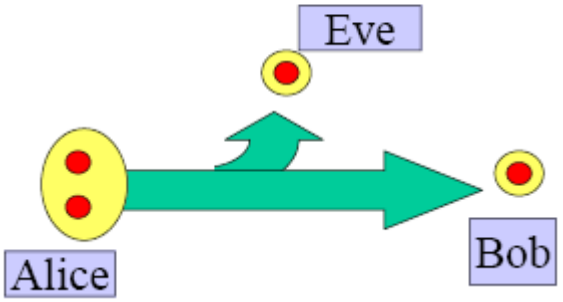




- Поасоново разпределение на броя на фотоните
  Просто, удобно използва утвърдени технологии
  $\Rightarrow$ Най-доброто решение засега

Drawback and PNS Attack

Multi-photon signals



a) still unconditional security for Poissonian photon-number statistics
b) photon number is second-quantization language (only optional, relevant is signal overlap structure)
c) public announcement of basis is crucial for problem!

- Several copies of signal state
- Eve can single out a copy (Jaynes-Cummings dynamics)
- No errors are caused in polarization
- Announcement of basis:

Delayed measurement gives full information to Eve

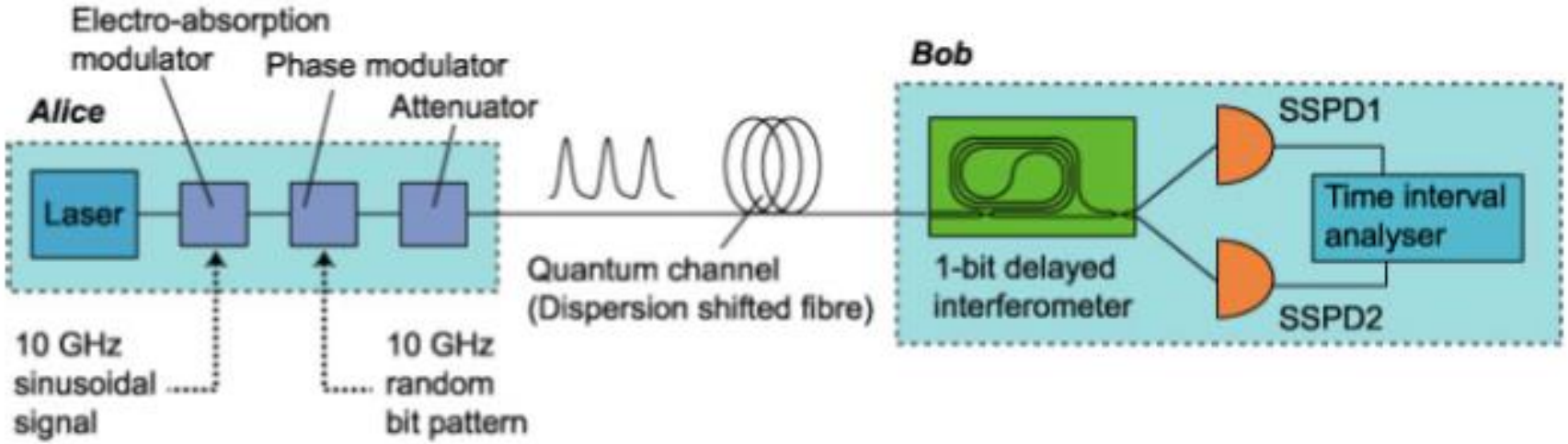
Solution to PNS

- SARG04 Protocol
  [Scarani, Acin, Ribordy, Gisin, PRL **92**, 057901 (2004)]

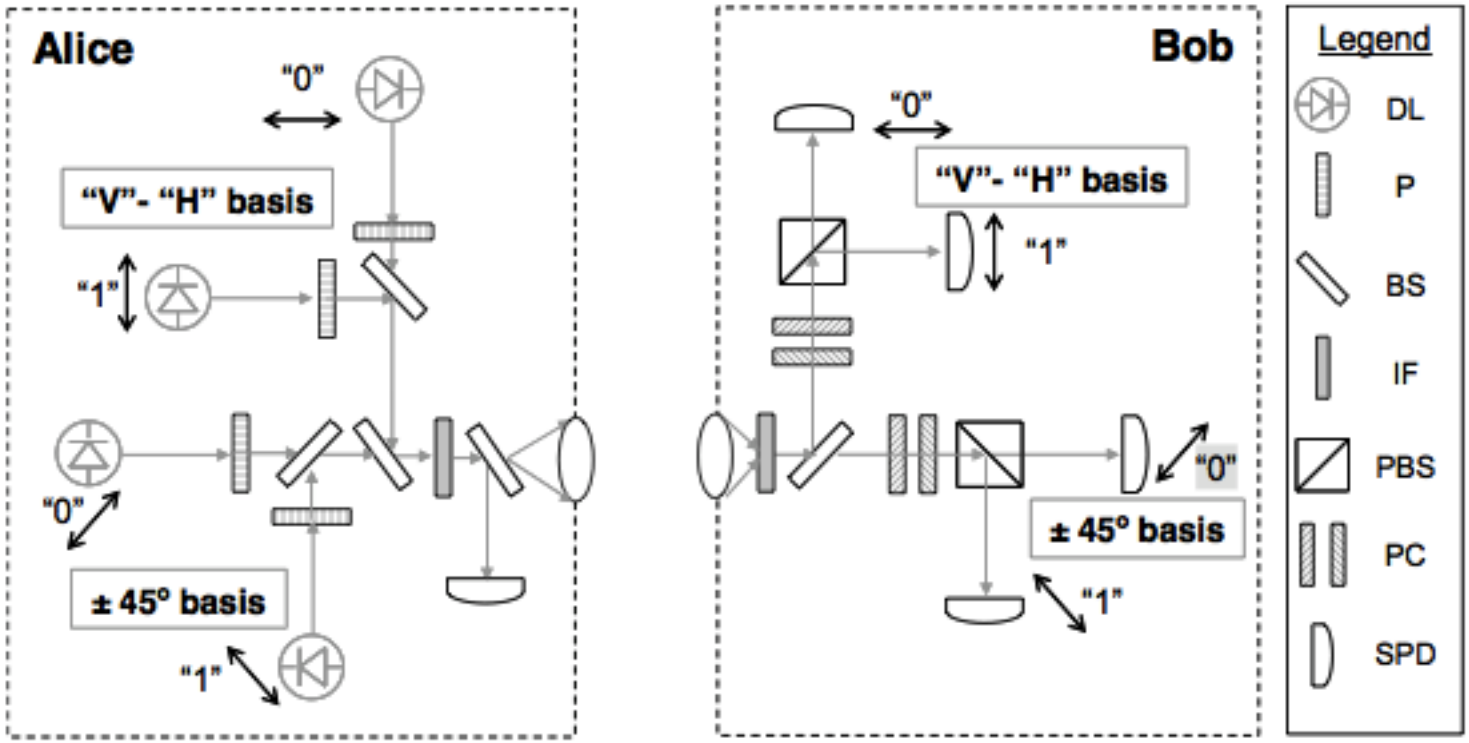
- Decoy State Method
  [Hwang, PRL **91**, 057901 (2003)]
  [Wang, PRL **94**, 230503 (2005)]
  [Lo, Ma and Chen PRL **94**, 230504 (2005)]

- Strong Reference Pulse Scheme
  [Huttner, Imoto, Gisin, Mor, PRA **51**, 1863 (1995)]

Current fiber-based distance record: 200 km (Takesue et al)



Demonstrated free-space link: 10 km



QKD: Ekkert 91 (E91)

- Advantage over BB84 is that Eve can now be detected using rejected qubits
- Eve causes non-violation of Bell inequality – Eve's measurement is a hidden variable

$$|\Psi^-\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 - |V\rangle_1|H\rangle_2)$$

$$= \frac{1}{\sqrt{2}}(|H'\rangle_1|V'\rangle_2 - |V'\rangle_1|H'\rangle_2)$$

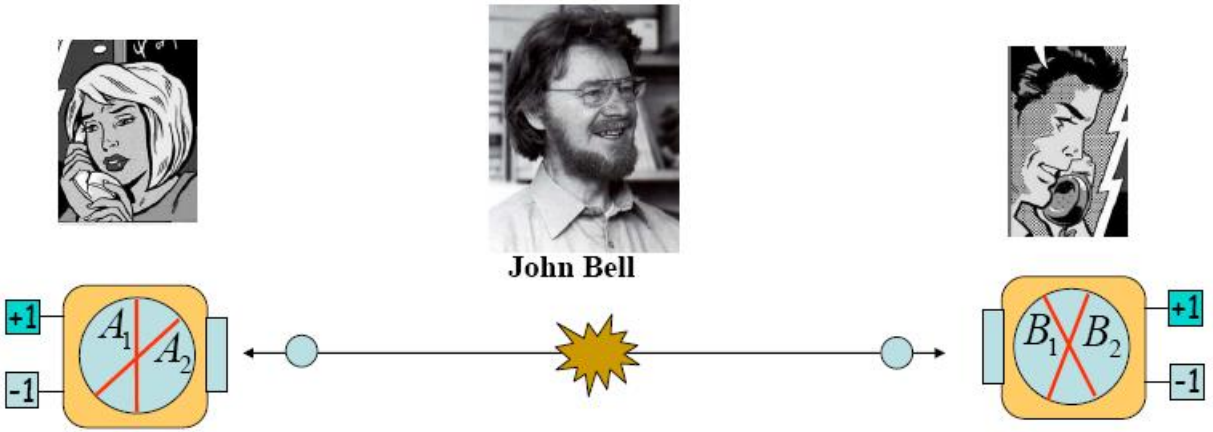
$$|H'\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$$

$$|V'\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$$

Where $|H'\rangle, |V'\rangle$ are the 45 degree Polarization

"If Eve knows precisely which particle is in which state, the entanglement can be concluded from the local reality theory."

----A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991)



$$S = \left| E(\phi_{A1}\phi_{B1}) - E(\phi_{A1}\phi_{B2}) + E(\phi_{A2}\phi_{B1}) + E(\phi_{A2}\phi_{B2}) \right|$$

Local Reality prediction: $S_{MAX} \leq 2$

Quantum Mechanical prediction: $S_{MAX} = 2\sqrt{2}$

QKD: E91

1. Alice и Bob споделят сплетени двойки фотони в състояние $|\Psi^-\rangle_{12}$
2. Alice и Bob измерват и регистрират резултатите в двата различни базиса
3. Alice и Bob избират случайно базисите и независимо за всяка сплетена двойка.
4. Измерванията в едни и същи базиси се използват за конструирането на ключ, а останалите се използват за проверка на неравенствата на Бел.

5. Ако неравенството е нарушено това гарантира, че не е имало подслушване и ключът може да се използва. Ако неравенството не е нарушено, има копиране еквивалентно на класическа теория със скрити параметри, ключа се изхвърля.

The Evolution of Q.C.

- In 1970, Stephen J. Weisner designed a theoretical bank note that would be impossible to duplicate, using the laws of quantum mechanics. He proposed using similar principles for cryptography.

- In the 1980's, Charles Bennett and Gilles Brassard used Weisner's ideas to develop the first quantum mechanics based cryptosystem. They were able to transmit, through open air, a distance of about 30 cm by 1989.

- In June of 2003 British Researchers led by Dr. Andrew Shields transmitted a usable key over 100 km of fiber optic cable.

- Nov. 3, 2003 – MagiQ systems announces general availability of world's first commercially available quantum cryptography system, supporting key exchanges at distances up to 120 km.

Weaknesses and Limitations of Q.C.

- Only works along unbroken and relatively short
- fiber optic cables. Record as of March, 2004 is
- 120 km.

- Doesn’t solve authentication problem.

- Doesn’t address some of the weakest links in
- data security such as human corruptibility and
- key storage.

- Relatively high cost.

Conclusion

- Quantum cryptography developments promise to address some of the problems that plague classical encryption techniques such as the key distribution problem and the predicted breakdown of the public/private key system. quantum cryptography operates on the Heisenberg uncertainty principle and random polarization of light. Another purely theoretical basis involves EPR entangled pairs.
- Due to the high cost of implementation and the adequacy of current cryptological methods, it is unlikely that quantum cryptography will be in widespread use for several years.