INOA-CNR



Dipartimento di Fisica

# Crittografia Quantistica

Alessandro Zavatta

Dipartimento di Fisica - Università di Firenze

Istituto Nazionale di Ottica Applicata (CNR) - Firenze

# Introduzione

- Crittografia
- Il problema della chiave
- La meccanica quantistica
- Distribuzione di chiavi mediante singoli fotoni
- Sistemi commerciali e Reti

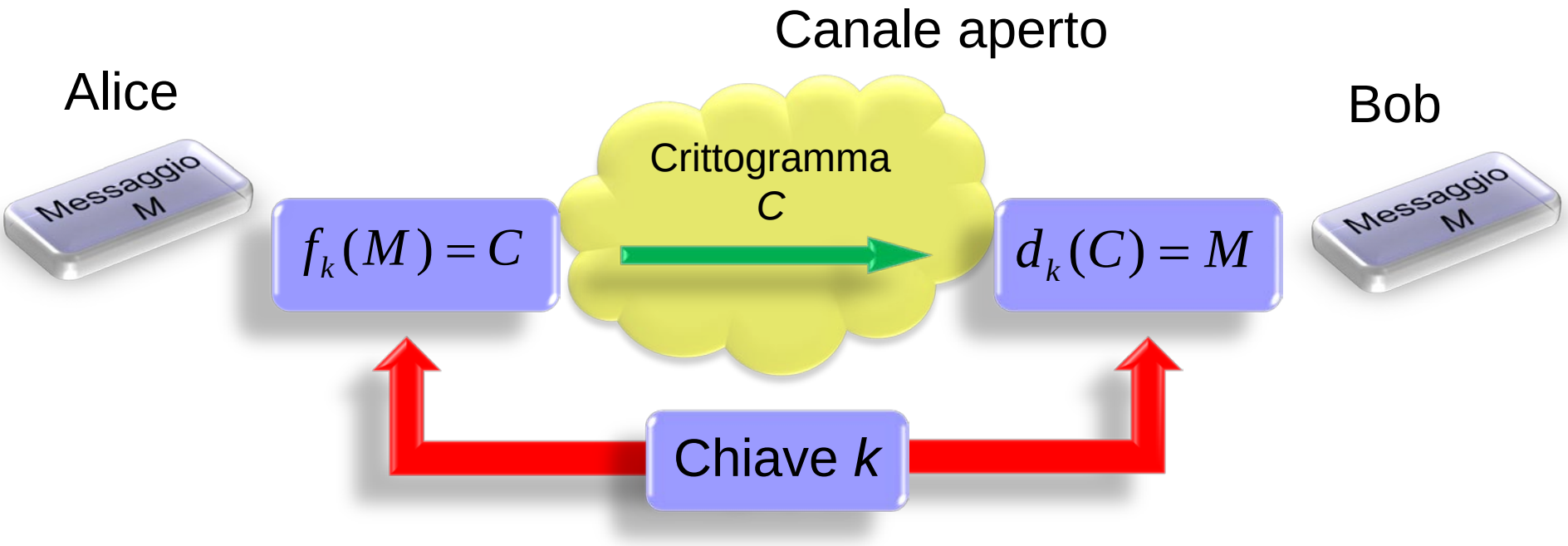
# Crittografia

- Sistema matematico di trasformazione dell'informazione
- Informazione accessibile solo a chi è autorizzato ad accedervi

# Crittografia

- Schemi a chiave segreta
  - Implementazione complessa
  - Sicuri
- Schemi a chiave pubblica (RSA)
  - Gli interlocutori non si accordano su una chiave
  - Semplici
  - Non completamente sicuri

# Crittografia a chiave segreta




Distribuzione di una chiave segreta su un canale sicuro

# Crittografia

- 1946 Claude Shannon: *Un sistema crittografico a chiave segreta è totalmente sicuro se la chiave è* :
  - Composta da numeri casuali
  - Usata una sola volta (One Time Pad)
  - Lunga quanto il messaggio

# Crittografia

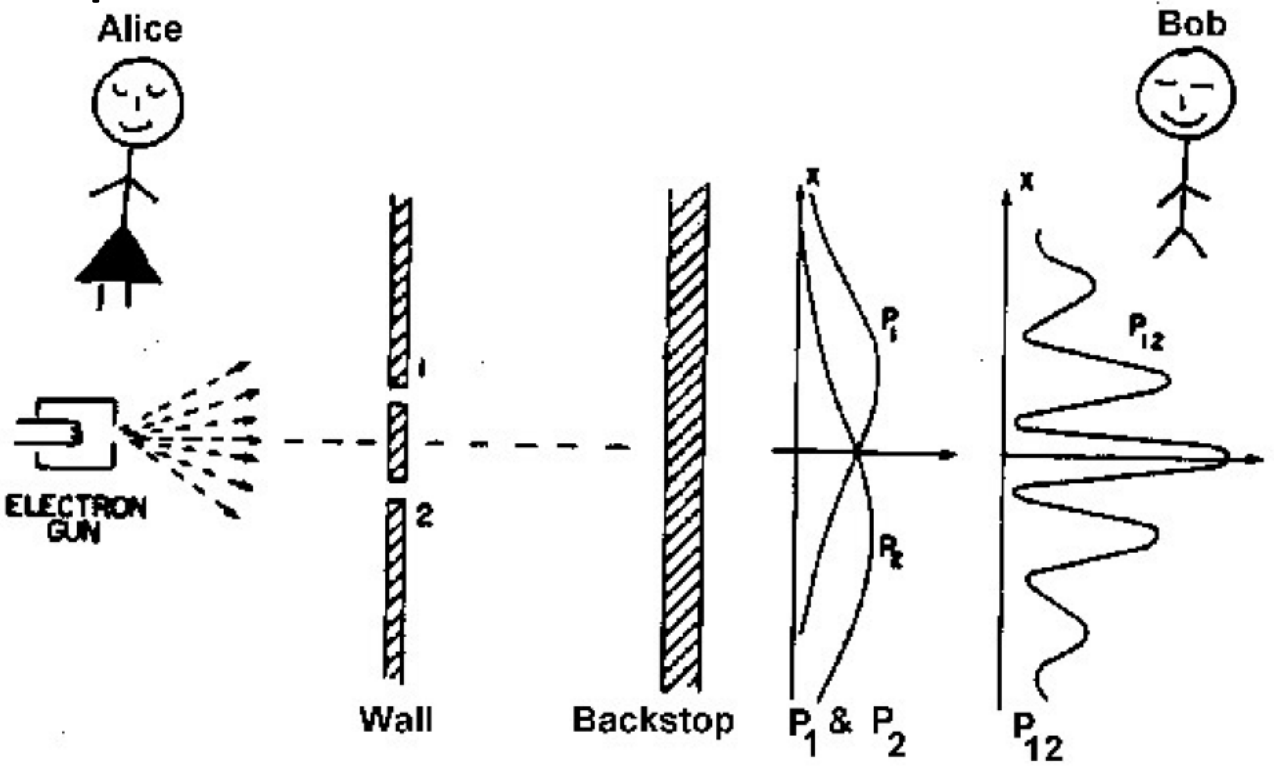
- Come risolvere il problema della chiave?
  - I computer generano numeri pseudo - casuali
  - Qualsiasi canale privato tradizionale per quanto sicuro e protetto può essere intercettato.
  - In fisica classica si possono misurare le proprietà di un sistema senza perturbarlo

# Crittografia quantistica

- Applicazione delle leggi della meccanica quantistica per risolvere i problemi legati alla distribuzione di chiavi .
- Meccanica quantistica: teoria fisica che descrive il comportamento del mondo microscopico (atomi, fotoni) dove l'energia è discretizzata in pacchetti detti quanti.

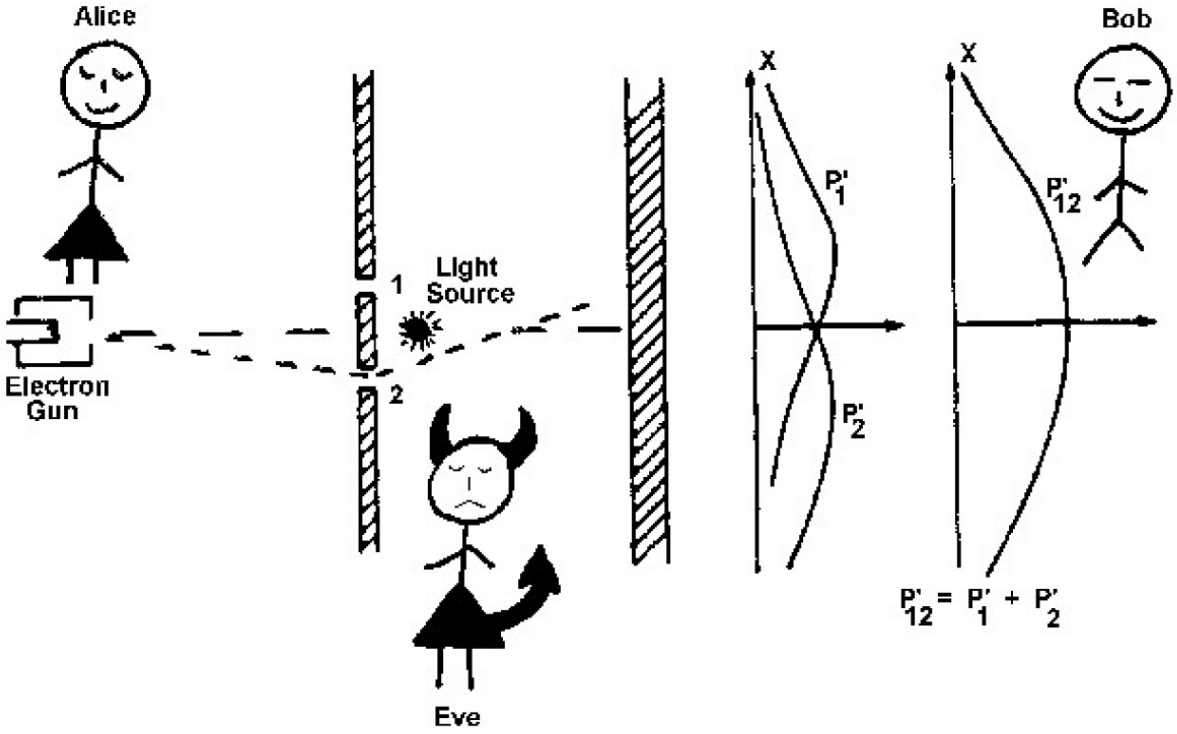
# Crittografia quantistica

- Principio di indeterminazione di Heisenberg



# Crittografia quantistica

- Principio di indeterminazione di Heisenberg

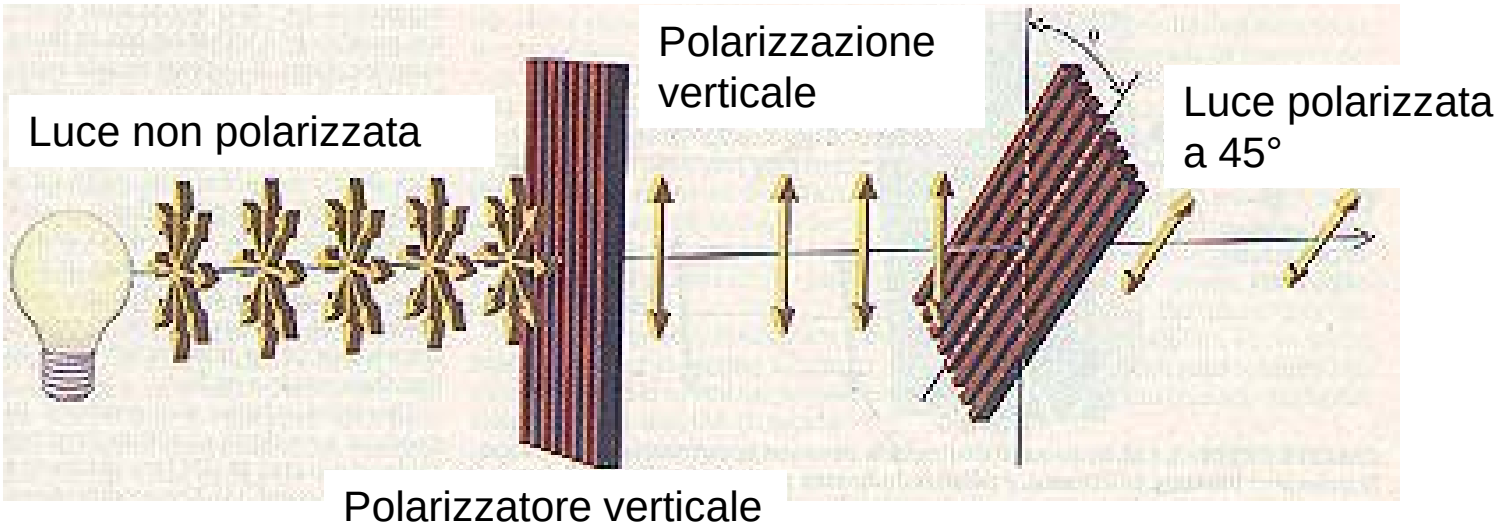


# Crittografia quantistica

- Bennet e Brassard (1984): la chiave è codificata sfruttando la polarizzazione di un singolo fotone.

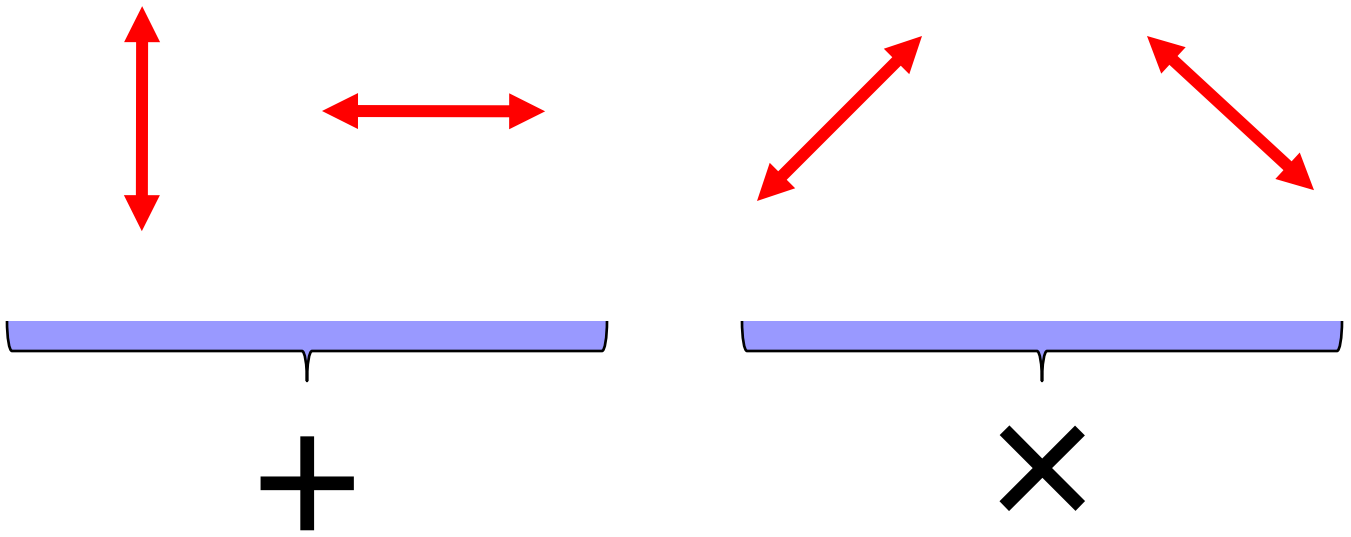
# Crittografia quantistica

- Polarizzazione della luce: proprietà intrinseca



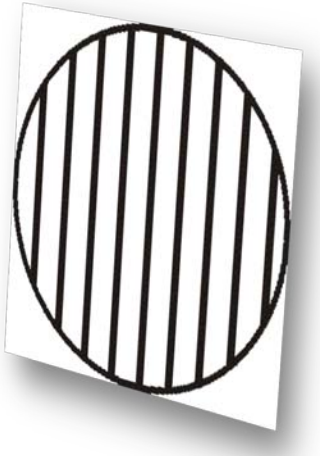
# Crittografia quantistica

- Singolo fotone: particella di luce priva di massa



# Crittografia quantistica

- Fotone verticale (+)



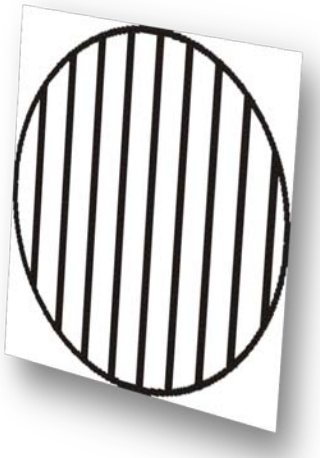
Polarizzatore verticale (+)

1

Rivelatore

# Crittografia quantistica

- Fotone orizzontale (+)



Polarizzatore verticale (+)

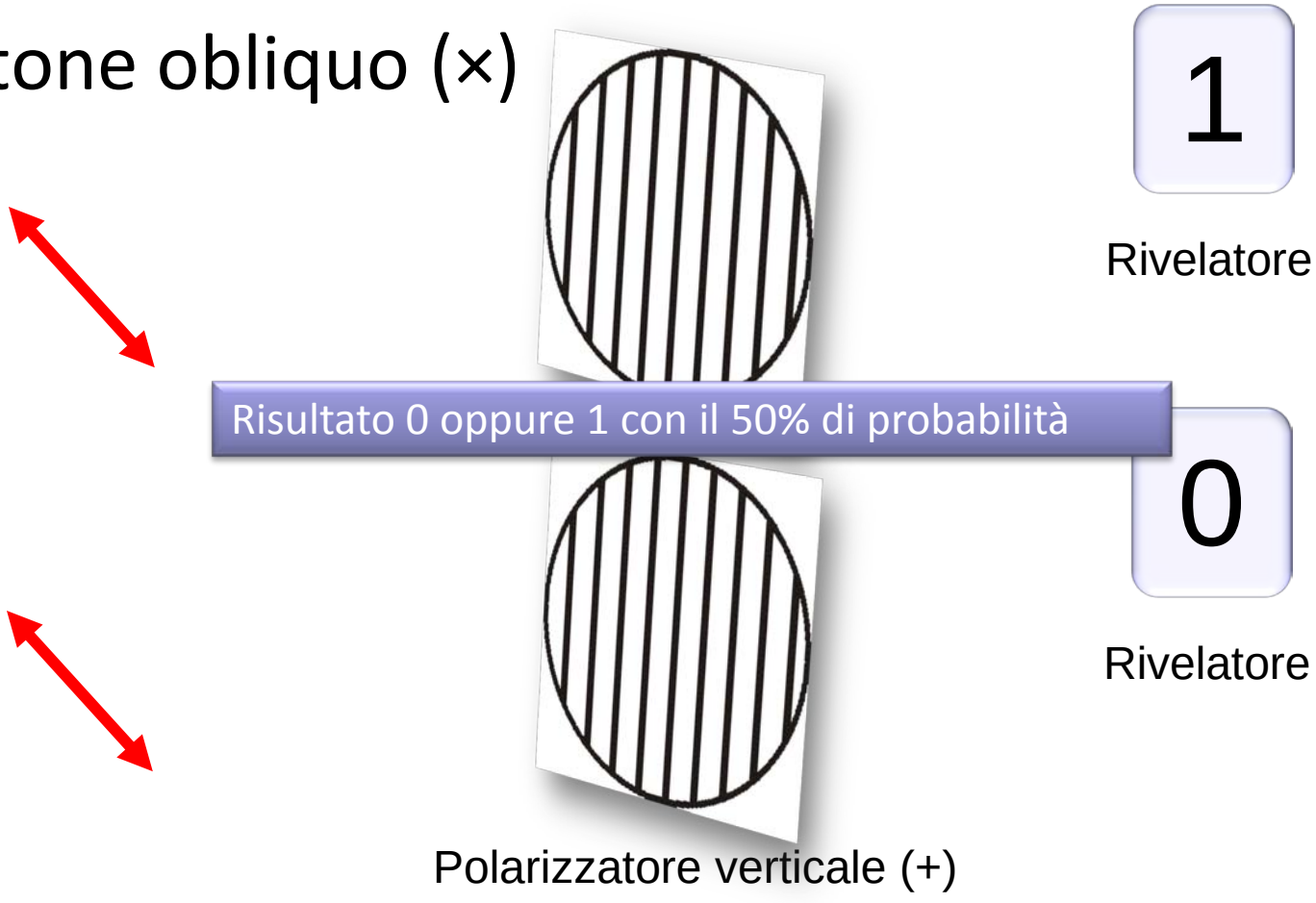
0

Rivelatore

Codifica binaria: 1 se il fotone passa, 0 altrimenti

# Crittografia quantistica

- Fotone obliquo (×)

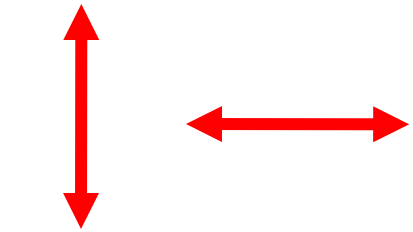


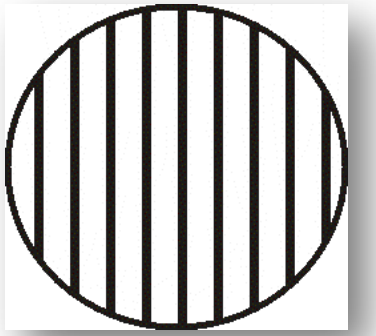
# Crittografia quantistica

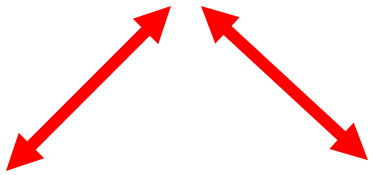
Base (Gruppo)

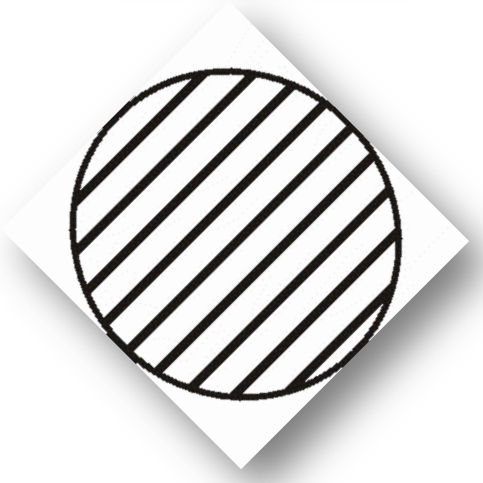
Polarizzazione

Polarizzatore (Filtro)









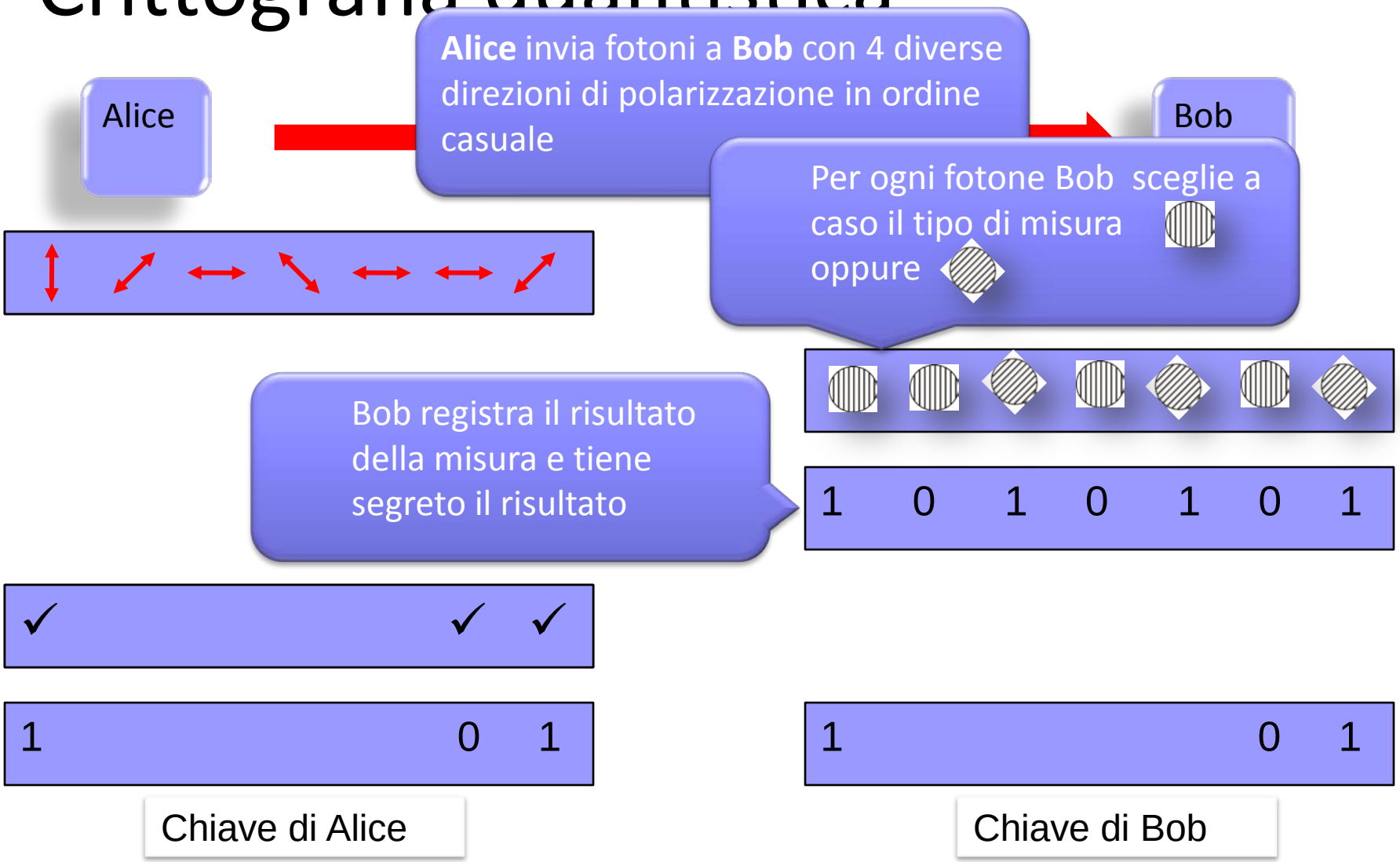
# Crittografia quantistica

| Alice | Bob | |
|---|---|---|
| + |  |  |
| 0 ↔ | 0 | 0 (50%), 1(50%) |
| 1 ↕ | 1 | 0 (50%), 1(50%) |

| Alice | Bob | |
|---|---|---|
| × |  |  |
| 0 ↘ | 0 (50%), 1(50%) | 0 |
| 1 ↗ | 0 (50%), 1(50%) | 1 |

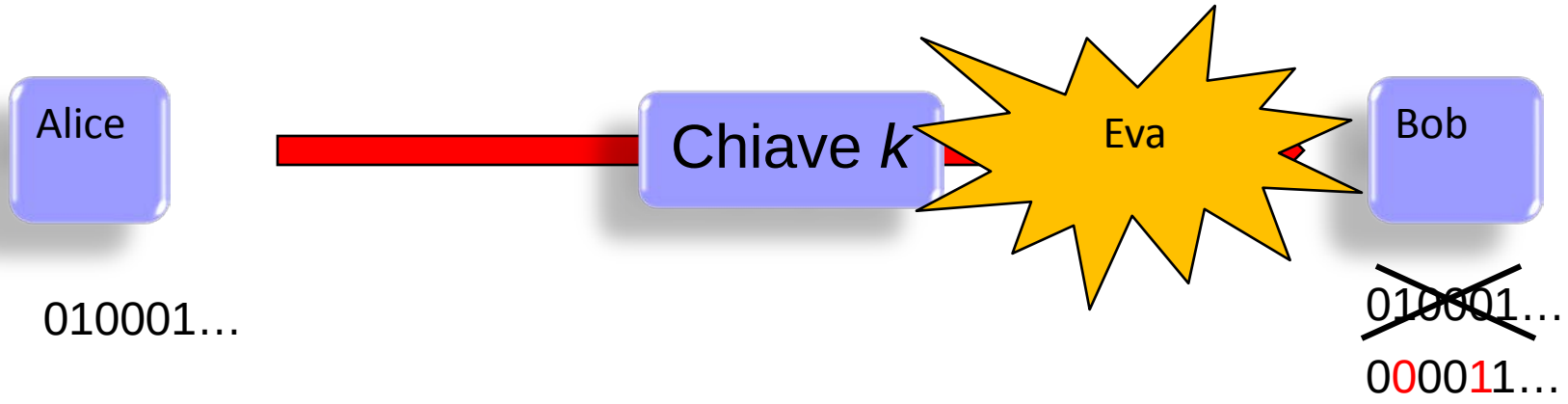
Risultato definito solo se il fotone è osservato con l'orientazione corretta

# Crittografia quantistica



# Crittografia quantistica

- BB84: L'eventuale presenza di una spia perturba il sistema




La chiave ricevuta da Bob non coincide con quella di Alice

# Crittografia quantistica

- La presenza di una spia sul canale quantistico viene rivelata con la presenza di errori nella comunicazione della chiave
- Alice e Bob prima di scambiarsi il messaggio verificano che il canale sia libero da spie confrontando parte della chiave

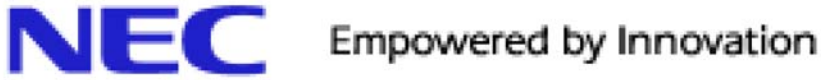
# Conclusioni

- Problema critico in crittografia: distribuzione di chiavi assolutamente casuali e sicure
- Meccanica quantistica fornisce un metodo per la generazione e distribuzione di chiavi casuali
- In un canale quantistico per la distribuzione di chiavi la presenza di una spia viene automaticamente rivelata dal sistema
- La sicurezza è garantita da leggi fisiche e non dalla complessità di alcune procedure matematiche

# Sistemi commerciali

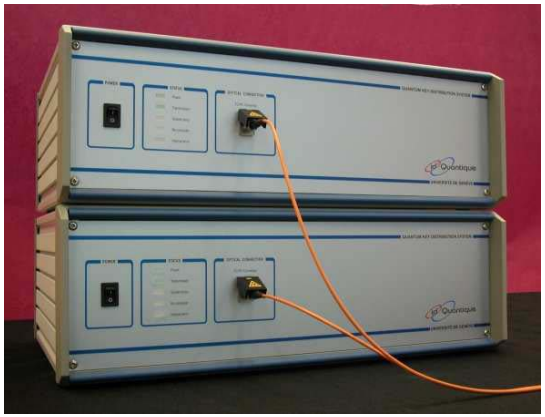
- MagiQ (New York, USA)
- idQuantique (Ginevra, Svizzera)
- NEC (Tsukuba, Giappone)

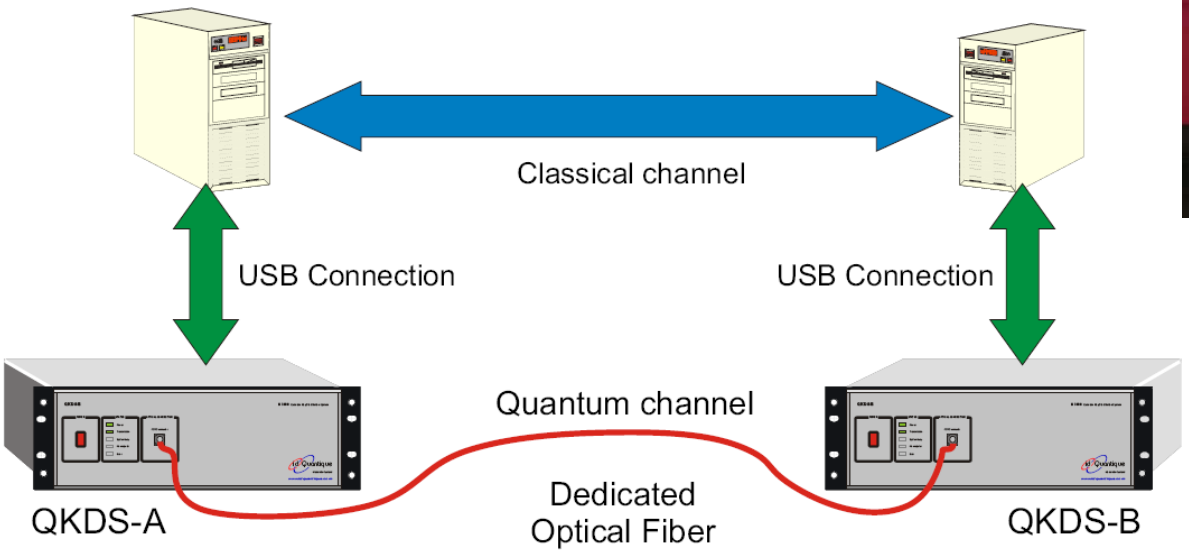

www.magiqtech.com

# Sistemi commerciali

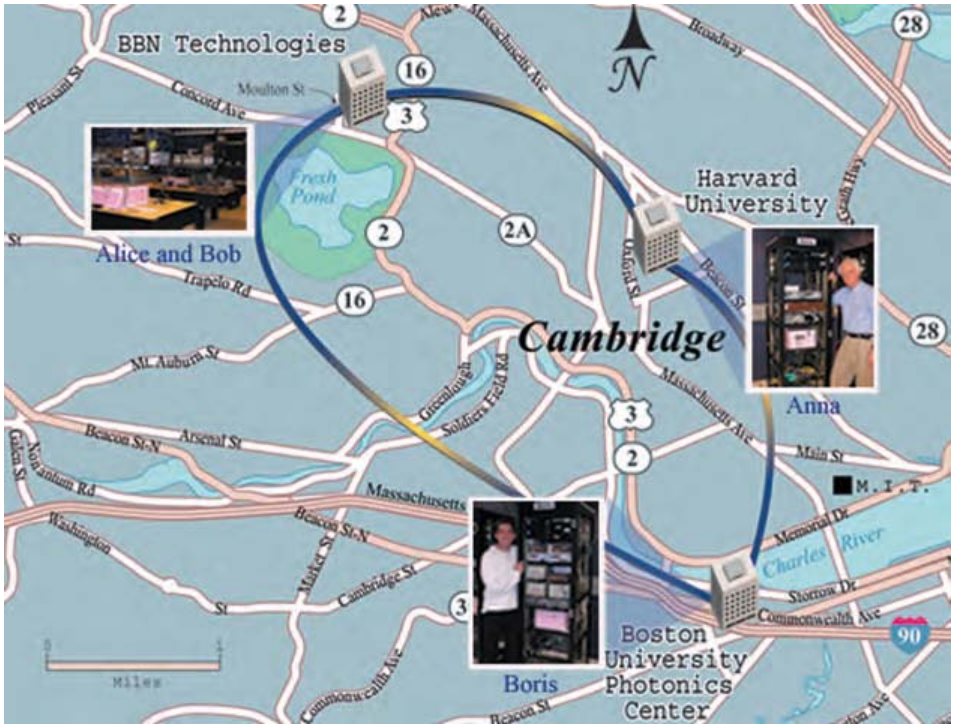
- Distanza: 100 km in fibra ottica (dark fiber)
- Costi: 100.000 €





# Reti (1)

- 2006, Boston (USA): Rete protetta con chiavi quantistiche




**Sponsor:** DARPA - Defense Advanced Research Projects Agency

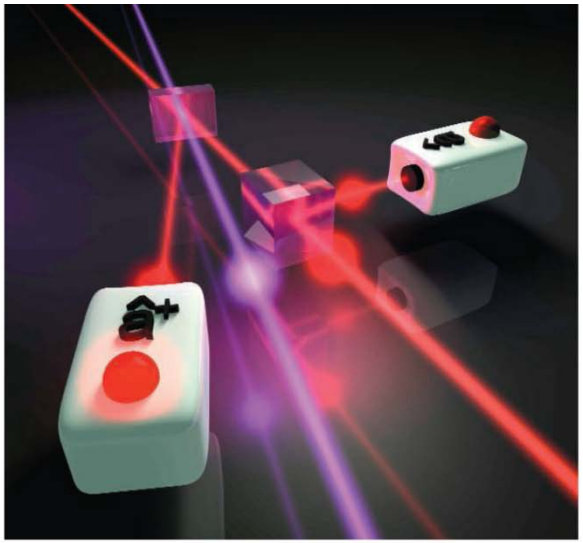
# Reti (2)


www.secoqc.net

- Europa:
  - Progetto integrato UE (FP6) SECOQC: **Sviluppo di una rete globale per comunicazioni sicure basate su crittografia quantistica:**
    - **2004 Vienna: Primo trasferimento bancario protetto da crittografia quantistica (***Bank Austria Creditanstalt***)**
    - **21 ottobre 2007, elezioni in Svizzera: Protezione della trasmissione di dati elettorali con chiavi quantistiche nel cantone di Ginevra**

# Esperimenti di ottica quantistica a Firenze

- “Tomografia” del singolo fotone e generazione di stati quantistici della luce.



THIS WEEK IN Science

EDITED BY STELLA HURTLEY AND PHIL SZUROMI

***Science***, 28 settembre 2007

**When Quantum Arithmetic Doesn't Add Up**

If you add an item to your shopping basket and then remove one that is identical, your total bill does not

**Grazie!**

Email: alessandro.zavatta@inoa.it

Homepage: http://www.inoa.it/home/QOG

# Crittografia quantistica