Quanti e Segreti

Stefano Mancini

Scuola di Scienze e Tecnologie, Università di Camerino
& INFN Sezione di Perugia

23 Gennaio 2014, Dipartimento di Informatica, Università di Verona

Per iniziare. . .

"Il fatto di avere dei segreti è, probabilmente, l'unica cosa che distingue gli uomini dagli animali" - Osamu Dazai

- $\kappa\rho\upsilon\pi\tau\acute{o}\varsigma$, crittologia, crittografia, crittoanalisi
  - steganografia
- utenti legittimi, mittente (Alice) e ricevente (Bob)
- utente illegittimo o eavesdropper (Eve)
- messaggio in chiaro (plain-text), messaggio cifrato o crittogramma (cipher-text), chiave
- cifrario o codice o crittosistema

Sommario

- La crittologia da *ars* a *scientia*
- Un codice inviolabile
- La crittografia a chiave pubblica
- Meccanica quantistica in pillole
- La distribuzione quantistica delle chiavi (QKD)
- Il futuro della QKD
- Oltre la QKD
- Conclusioni

La crittologia da *ars* a *scientia*

Per un interessante excursus storico sulla crittologia vedere: "The Code Book" by S. Singh

Codice o crittosistema

- alfabeto $\mathcal{A}$
- spazio dei messaggi $\mathcal{M}$ su $\mathcal{A}$ (e.g. $\mathcal{A}^n$)
- spazio delle chiavi $\mathcal{K}$
- funzione di cifratura $E_k : \mathcal{A}^b \to \mathcal{A}^b$
- funzione di de-cifratura $D_{k'} : \mathcal{A}^b \to \mathcal{A}^b$ $(D_{k'} \equiv E_k^{-1})$

Se $k = k'$ (risp. $k \neq k'$) il crittosistema è simmetrico (risp. asimmetrico)

Un semplice esempio (il codice di Cesare)

- $\mathcal{A} = \{0, 1, \ldots, 25\}$
- $\mathcal{M} = \mathcal{A}^n$
- $\mathcal{K} = \{1, \ldots, 25\}$
- $E_k : \mathcal{A} \to \mathcal{A}$ tale che $E_k(m) = m + k \ (mod\ 26) = c$
- $D_k : \mathcal{A} \to \mathcal{A}$ tale che $D_k(c) = c - k \ (mod\ 26) = m$

$$\text{GATTO} \Rightarrow 06\ 00\ 19\ 19\ 14$$

$$E_{15}(06)E_{15}(00)E_{15}(19)E_{15}(19)E_{15}(14) = 21\ 15\ 08\ 08\ 03 \Rightarrow \text{VPIID}$$

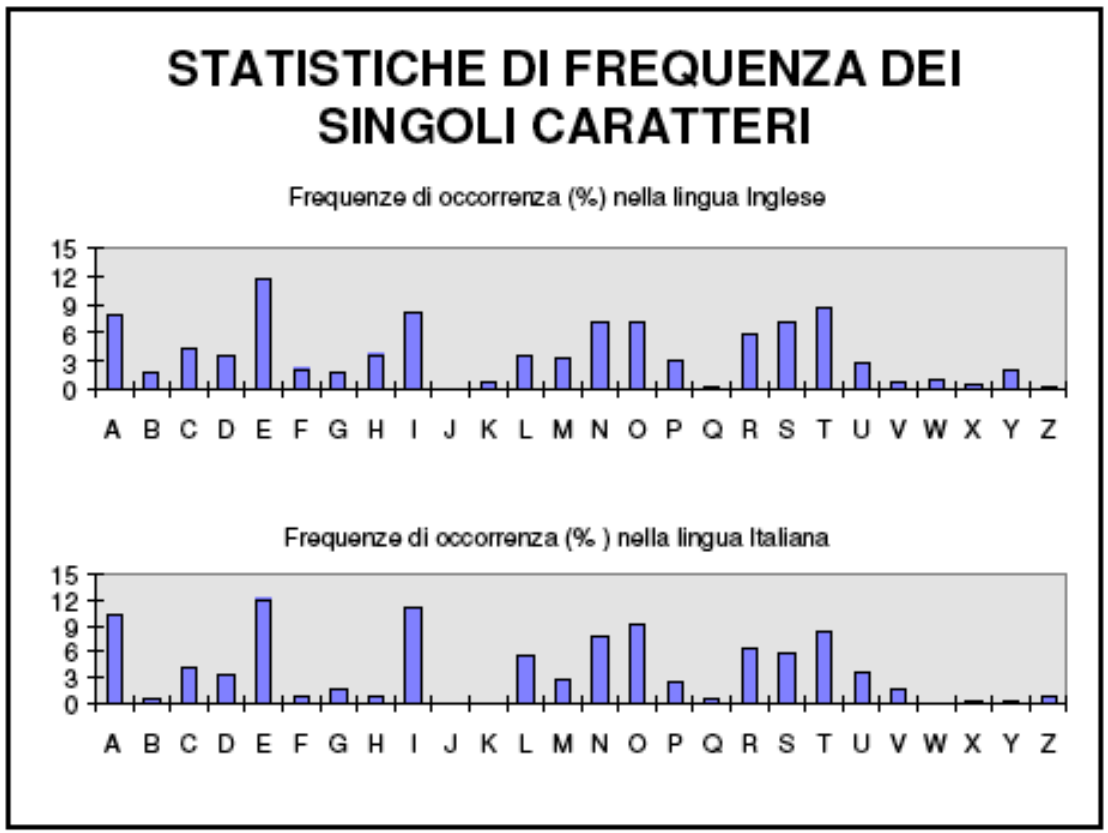
$$D_{15}(21)D_{15}(15)D_{15}(08)D_{15}(08)D_{15}(03) = 06\ 00\ 19\ 19\ 14 \Rightarrow \text{GATTO}$$

Facilmente violabile con metodo di esaustione!

Crittosistemi più convincenti

- $\mathcal{K} = \{1, \ldots, |\mathcal{A}|! - 1\}$
- $E_k : \mathcal{A} \to \mathcal{A}$ tale che $E_k(m) = \sigma_k(m) = c$

Violabile con indagine statistica (esempio in *The Gold Bug*, 1843)



Crittosistemi più convincenti

- $\mathcal{K} = \{1, \ldots, (|\mathcal{A}|^b)! - 1\}$
- $E_k : \mathcal{A}^b \to \mathcal{A}^b$ tale che

  $E_k(m) = \sigma_k(m) = \sigma_{k_1}(m_1)\sigma_{k_2}(m_2)\ldots\sigma_{k_b}(m_b)$

  $m_i \in \mathcal{A},\ k_i \in \{0, 1, \ldots, |\mathcal{A}|!\}$

Violabile con metodo Kasiski:
Si costruiscono b messaggi prendendo una lettera ogni b dal messaggio originale ognuno dei quali è codificato con una singola permutazione σ_{k_i}
Su ognuno dei b messaggi si applica l'indagine statistica

Varianti: Scherbius, Rejewski, Turing, Welchman

Un codice inviolabile

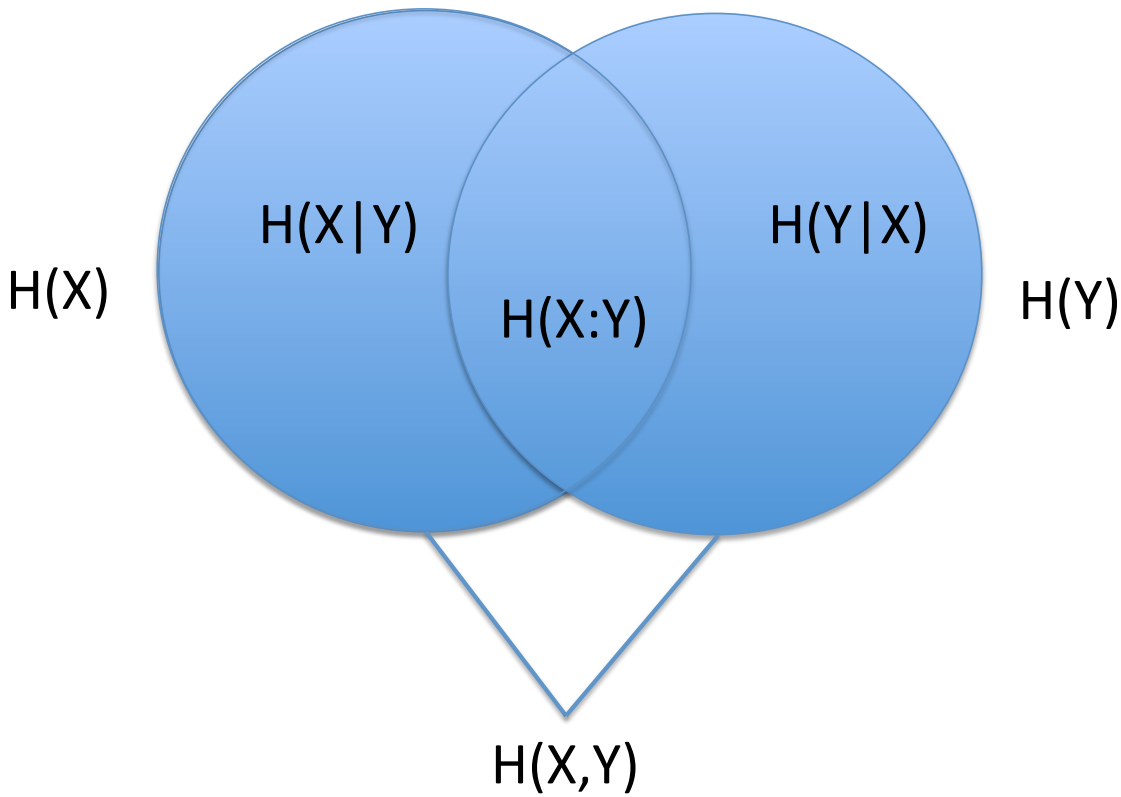
Cifrario di Vernam (1917)

- $\mathcal{K} = \mathcal{M} = \mathcal{A}^n$
- $E_k : \mathcal{A}^n \rightarrow \mathcal{A}^n$ tale che $c = m + k \ (mod \ |\mathcal{A}|)$
- $k \in \mathcal{A}^n$ scelto in maniera random
- $D_k : \mathcal{A}^n \rightarrow \mathcal{A}^n$ tale che $m = c - k \ (mod \ |\mathcal{A}|)$
- la chiave è utilizzata una sola volta (One Time Pad)

Un codice inviolabile

"A Mathematical Theory of Communication" Shannon 1948

Informazione (entropia) di due variabili random X ed Y su di un alfabeto



Un codice inviolabile

"Communication Theory of Secrecy Systems" Shannon 1949

- Se in un crittosistema $H(m|c) = H(m)$ (o $Pr(m|c) = Pr(m)$), allora esso è perfetto
- OTP è un crittosistema perfetto

Inconvenienti

- la chiave deve essere lunga quanto il messaggio ed utilizzata una sola volta
- la chiave deve essere random
- la chiave deve essere condivisa tra Alice e Bob **:-(**

La crittografia a chiave pubblica

In "New Directions in Cryptography", 1976, W. Diffie e M. Hellman introducono l'idea di crittografia (asimmetrica) a chiave pubblica: La funzione cifrante deve essere nota a tutti, essa però è difficile da invertire senza la conoscenza di una chiave privata

Difficile tornare indietro...

Alice e Bob vogliono condividere una chiave k

- Vengono scelti un primo N (grande) ed un intero $g < N$
- N e g vengono resi pubblici
- Alice sceglie intero random x e invia a Bob $u = g^x \ (mod\ N)$
- Bob sceglie intero random y e invia ad Alice $v = g^y \ (mod\ N)$
- Alice calcola $v^x \ (mod\ N) = g^{yx} \ (mod\ N)$
- Bob calcola $u^y \ (mod\ N) = g^{xy} \ (mod\ N)$

Eve dovrebbe calcolare $x = \log_g u \ (mod\ N)$ e $y = \log_g v \ (mod\ N)$

La crittografia a chiave pubblica

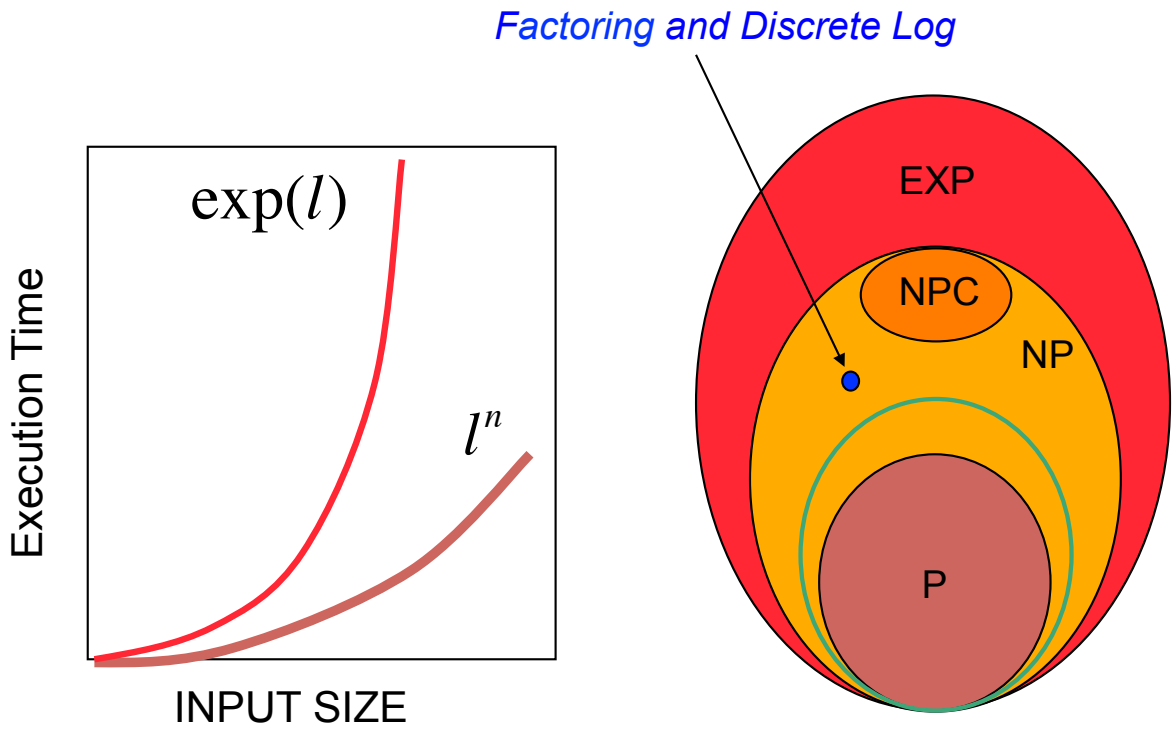
Il metodo RSA (Rivest, Shamir e Adleman, 1977)

- Alice sceglie due primi (grandi) p e q, e calcola $N = p \times q$
- Alice sceglie e random coprimo con $\phi(N) = (p-1)(q-1)$, e calcola d tale che $ed = 1 \ (mod \ \phi(N))$ [i.e. $ed = 1 + j\phi(N)$]
- Alice pubblica N ed e
- Bob rappresenta un messaggio con un intero m coprimo con N
- Bob calcola $c = m^e \ (mod \ N)$ e lo invia ad Alice
- Alice riceve c e calcola $c^d \ (mod \ N)$, recuperando così m:
  $c^d = m^{ed} = m^{1+j\phi(N)} = m \times \left(m^{\phi(N)}\right)^j \equiv m \ (mod \ N)$
  Teorema di Eulero (1736): $gcd(m, N) = 1 \Rightarrow m^{\phi(N)} = 1 \ (mod \ N)$

Eve dovrebbe fattorizzare N in $q \times p$

La crittografia a chiave pubblica

Facile e difficile



La crittografia a chiave pubblica

"Difficile" non sempre per tutti ...

Inoltre, computazione quantistica ...

Meccanica quantistica in pillole

Postulati

- Lo spazio degli stati di un sistema fisico è rappresentato da uno spazio di Hilbert $\mathcal{H}$ e gli stati dai suoi vettori $|\psi\rangle$ (normalizzati ad 1)
- Lo spazio degli stati di un sistema fisico composito è $\otimes$ degli spazi degli stati dei sottosistemi
- I cambiamenti di stato (in un sistema chiuso) sono descritti da trasformazioni unitarie U su $\mathcal{H}$
- Gli osservabili sono operatori autoaggiunti su $\mathcal{H}$
  La misura di un osservabile O ha come possibili risultati i suoi autovalori $\{o\}_{o \in \mathbb{R}}$
  La probabilità di ottenere uno specifico o è $Pr(o) = |\langle \psi | o \rangle|^2$
  L'effetto della misura è una proiezione $|\psi\rangle \mapsto |o\rangle$

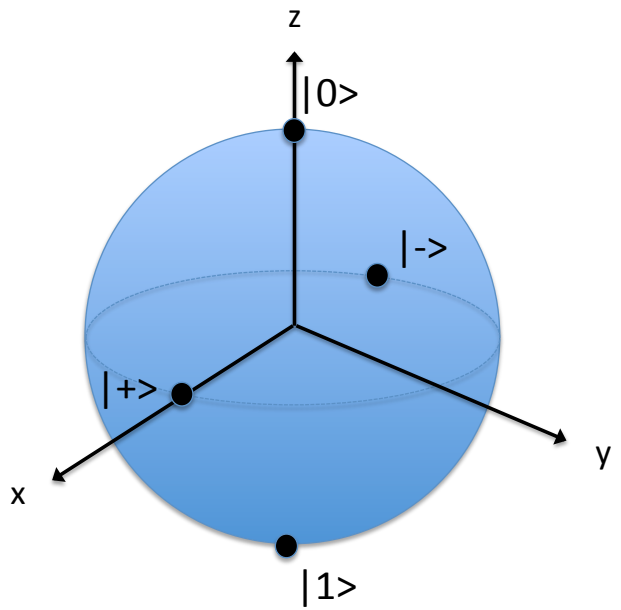
Meccanica quantistica in pillole

Il più semplice sistema quantistico $\mathbb{C}^2$: *quantum bit (S. Wisner 1969-1983, B. Schumacher 1995)*

Base canonica: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Generico stato $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ con $\alpha, \beta \in \mathbb{C}$ tali che $|\alpha|^2 + |\beta|^2 = 1$

Altra base: $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ ($|\pm\rangle$ non ortogonali a $|0\rangle, |1\rangle$)



Meccanica quantistica in pillole

Osservabili rilevanti per un qubit

- Z, tale che $Z|0\rangle = |0\rangle$ e $Z|1\rangle = -|1\rangle$ (quindi $\{|0\rangle, |1\rangle\}$ è detta base Z)
- X, tale che $X|+\rangle = |+\rangle$ e $X|-\rangle = -|-\rangle$ (quindi $\{|+\rangle, |-\rangle\}$ è detta base X)
- Y, tale che $Y = iXZ$

Partendo da $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$,

la misura di Z proietta con $Pr = |\alpha|^2$ su $|0\rangle$ e con $Pr = |\beta|^2$ su $|1\rangle$

la misura di X proietta con $Pr = \frac{|\alpha+\beta|^2}{2}$ su $|+\rangle$ e con $Pr = \frac{|\alpha-\beta|^2}{2}$ su $|-\rangle$

La distribuzione quantistica delle chiavi (QKD)

Tutto nasce dalla "pazza" idea del denaro quantistico (S. Wisner, 1969) rielaborata da C. H. Bennet and G. Brassard nel 1984 (BB84)

Alice basis	Encoding	q-ch	Bob basis	Bob result	Decoding	public-ch
Z	$0 \leftrightarrow \|0\rangle$	$\rightsquigarrow$	Z	$\|0\rangle,\ \Pr = 1$	0	OK
			X	$\|+\rangle,\ \Pr = 1/2$	0	-
			X	$\|-\rangle,\ \Pr = 1/2$	1	-
Z	$1 \leftrightarrow \|1\rangle$	$\rightsquigarrow$	Z	$\|1\rangle,\ \Pr = 1$	1	OK
			X	$\|+\rangle,\ \Pr = 1/2$	0	-
			X	$\|-\rangle,\ \Pr = 1/2$	1	-
X	$0 \leftrightarrow \|+\rangle$	$\rightsquigarrow$	Z	$\|0\rangle,\ \Pr = 1/2$	0	-
			Z	$\|1\rangle,\ \Pr = 1/2$	1	-
			X	$\|+\rangle,\ \Pr = 1$	0	OK
X	$1 \leftrightarrow \|-\rangle$	$\rightsquigarrow$	Z	$\|0\rangle,\ \Pr = 1/2$	0	-
			Z	$\|1\rangle,\ \Pr = 1/2$	1	-
			X	$\|-\rangle,\ \Pr = 1$	1	OK

La distribuzione quantistica delle chiavi (QKD)

Che cosa si guadagna con la QKD?
Consideriamo *Intercept Resending* (e ricordiamo *no-cloning*)

Alice	q-ch	Eve	Eve result	q-ch	Bob	Bob result	Pr
$0 \leftrightarrow \|0\rangle$	$\rightsquigarrow$	$Z,\ \Pr = 1/2$	$\|0\rangle,\ \Pr = 1$	$\rightsquigarrow$	Z	$\|0\rangle \leftrightarrow 0,\ \Pr = 1$	$1/2$
		$X,\ \Pr = 1/2$	$\|+\rangle,\ \Pr = 1/2$	$\rightsquigarrow$	Z	$\|0\rangle \leftrightarrow 0,\ \Pr = 1/2$	$1/8$
			$\|+\rangle,\ \Pr = 1/2$	$\rightsquigarrow$	Z	$\|1\rangle \leftrightarrow 1,\ \Pr = 1/2$	$1/8$
		$X,\ \Pr = 1/2$	$\|-\rangle,\ \Pr = 1/2$	$\rightsquigarrow$	Z	$\|0\rangle \leftrightarrow 0,\ \Pr = 1/2$	$1/8$
			$\|-\rangle,\ \Pr = 1/2$	$\rightsquigarrow$	Z	$\|1\rangle \leftrightarrow 1,\ \Pr = 1/2$	$1/8$

La probabilità che n bits della chiave "grezza" passino un check su di un canale pubblico (siano concordi) è pari a $\left(\frac{3}{4}\right)^n \overset{n\to\infty}{\longrightarrow} 0$
L'eavesdropper può essere sempre scoperto!
Information gain implies disturbance (in distinguishing non-orthogonal states)

La distribuzione quantistica delle chiavi (QKD)

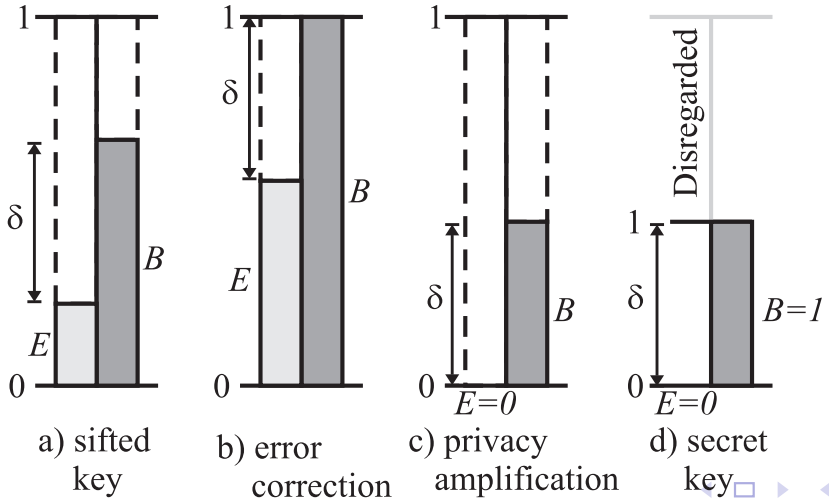
Ma gli errori possono anche non essere dovuti alla presenza di Eve!

- Alice e Bob devono stimare il rate di errore
- Necessità di un upper bound (maggiore di zero) sul rate di errore tollerabile

Teorema di Csiszár & Körner (1978)

Data una distribuzione $p(A, B, E)$, Alice e Bob possono distillare una chiave perfettamente segreta (usando EC e PA) se e solo se

$$H(A:B) \geq H(A:E) \quad \text{o} \quad H(A:B) \geq H(B:E)$$



La distribuzione quantistica delle chiavi (QKD)

Le entropie mutue del teorema CK78 dipendono dal tipo di attacco!

In generale si distunguono:

- Attacchi individuali
- Attacchi collettivi
- Attacchi coerenti

La sicurezza *incondizionale* è quella contro gli attacchi coerenti.

Teorema di Hall (1985)

Siano E e B due osservabili in uno spazio di Hilbert N-dimensionale e siano e, b, $|e\rangle$, $|b\rangle$ corrispondenti autovalori ed autovettori, allora

$$H(A:B) + H(A:E) \leq 2\log_2 \left[N \max_{e,b} |\langle e|b\rangle| \right]$$

La distribuzione quantistica delle chiavi (QKD)

L'attacco più distruttivo di Eve che possiamo immaginare è quello in cui conosce in anticipo le basi utilizzate da Alice! Supponiano

$$\underbrace{XZZXZXZXXZ \ldots XZZXZ}_{n-times}$$

Siccome Eve conosce in anticipo le basi ciò è equivalente ad utilizzare

$$\underbrace{XXXXXXXXXX \ldots XXXX}_{n-times}$$

1) Se $A = B = E = X^{\otimes n}$ si ha $H(A:B) + H(A:E) \leq 2n$
2) Se $A = B = X^{\otimes n}$ e $E = Z^{\otimes n}$ si ha $H(A:B) + H(A:E) \leq n$
Lo scenario in cui Eve conosce la sequenza di basi esatte equivale a quello in cui conosce la sequenza di basi sbagliate, quindi 2)
Inoltre $H(A:B) = n\,(1 - H(p))$, con p rate di errore
In definitiva BB84 assolutamente sicuro se $p \leq 11\%$

La distribuzione quantistica delle chiavi (QKD)

Il protocollo E91 (A. Ekert, 1991)
Alice invia ripetutamente a Bob attraverso un canale quantistico metà di una coppia di qubits *entangled*

$$(|0\rangle|0\rangle + |1\rangle|1\rangle)/\sqrt{2} \equiv (|+\rangle|+\rangle + |-\rangle|-\rangle)/\sqrt{2}$$

Alice basis	Alice result	Alice dec.	Bob basis	Bob result	Bob dec.	public-ch
Z	$\|0\rangle,\ \Pr = 1/2$	0	Z	$\|0\rangle,\ \Pr = 1$	0	OK
Z	$\|0\rangle,\ \Pr = 1/2$	0	X	$\|+\rangle,\ \Pr = 1/2$	0	-
Z	$\|0\rangle,\ \Pr = 1/2$	0	X	$\|-\rangle,\ \Pr = 1/2$	1	-
Z	$\|1\rangle,\ \Pr = 1/2$	1	Z	$\|1\rangle,\ \Pr = 1$	1	OK
Z	$\|1\rangle,\ \Pr = 1/2$	1	X	$\|+\rangle,\ \Pr = 1/2$	0	-
Z	$\|1\rangle,\ \Pr = 1/2$	1	X	$\|-\rangle,\ \Pr = 1/2$	1	-
X	$\|+\rangle,\ \Pr = 1/2$	0	X	$\|+\rangle,\ \Pr = 1$	0	OK
X	$\|+\rangle,\ \Pr = 1/2$	0	Z	$\|0\rangle,\ \Pr = 1/2$	0	-
X	$\|+\rangle,\ \Pr = 1/2$	0	Z	$\|1\rangle,\ \Pr = 1/2$	1	-
X	$\|-\rangle,\ \Pr = 1/2$	1	X	$\|-\rangle,\ \Pr = 1$	1	OK
X	$\|-\rangle,\ \Pr = 1/2$	1	Z	$\|0\rangle,\ \Pr = 1/2$	0	-
X	$\|-\rangle,\ \Pr = 1/2$	1	Z	$\|1\rangle,\ \Pr = 1/2$	1	-

La distribuzione quantistica delle chiavi (QKD)

Il protocollo E91 è equivalente al BB84

Supponiamo che Alice e Bob possano misurare le proprietà $\mathcal{P}_{A_1}$, $\mathcal{P}_{A_2}$ e $\mathcal{P}_{B_1}$, $\mathcal{P}_{B_2}$ delle loro rispettive particelle ottenendo variabili (e.g. binarie) A_1, A_2 e B_1, B_2, allora sotto le ipotesi di *realismo* e *località* deve essere:

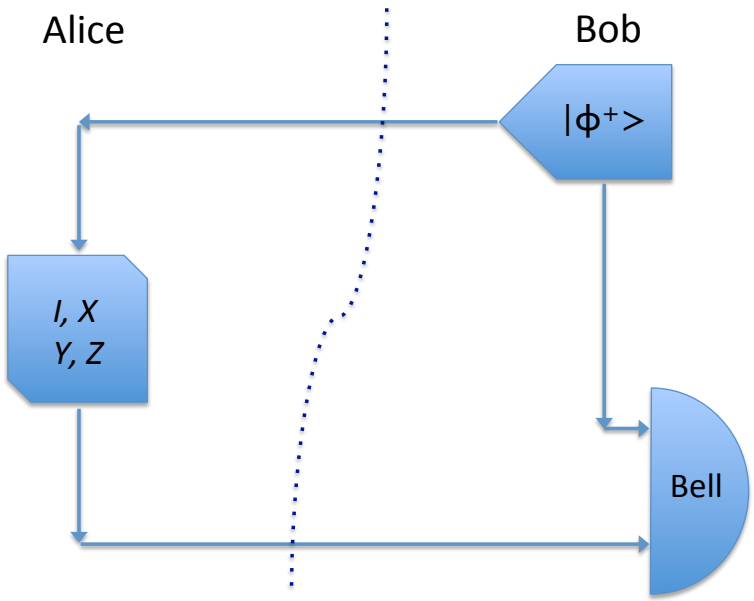
$$\mathbb{E}\left(A_1 B_1 + A_2 B_1 + A_2 B_2 - A_1 B_2\right) \leq 2$$

QM permette $\mathbb{E}\left(A_1 B_1 + A_2 B_1 + A_2 B_2 - A_1 B_2\right) \leq 2\sqrt{2}$

Il futuro della QKD

Superdense coding (1992)

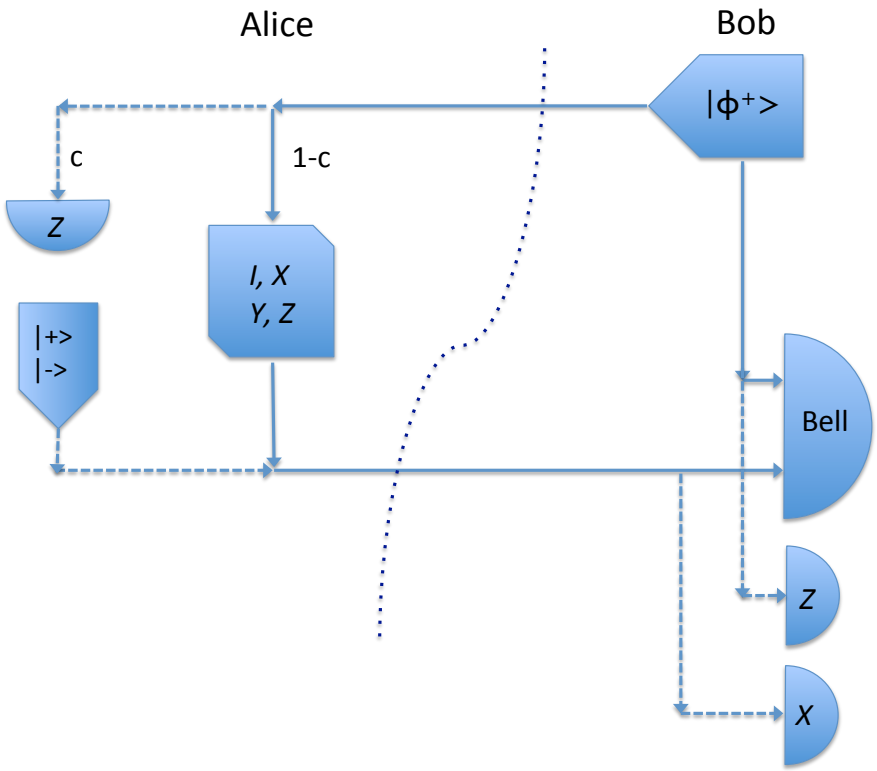
$$
\begin{aligned}
|\Phi^+\rangle &= (|0\rangle|0\rangle + |1\rangle|1\rangle)/\sqrt{2} \\
|\Phi^-\rangle &= (|0\rangle|0\rangle - |1\rangle|1\rangle)/\sqrt{2} = Z|\Phi^+\rangle \\
|\Psi^+\rangle &= (|1\rangle|0\rangle + |0\rangle|1\rangle)/\sqrt{2} = X|\Phi^+\rangle \\
|\Psi^+\rangle &= (|1\rangle|0\rangle - |0\rangle|1\rangle)/\sqrt{2} = XZ|\Phi^+\rangle
\end{aligned}
$$



Cambio di paradigma per la QKD, da one-way quantum channel a two-way quantum channel [K. Boström & T. Felbinger, 2004; M. Lucamarini, S.M., 2005]

Il futuro della QKD

QKD by Superdense coding



Sicurezza assoluta ($p \leq 11.8\%$) superiore ai protocolli one-way [N. Beaudry, M. Lucamarini, S. M., R. Renner, 2013]

Il futuro della QKD

QKD garantisce sicurezza assoluta, ma ci sono comunque delle assunzioni, e.g. Alice e Bob hanno un controllo completo dei loro dispositivi (solo il canale quantistico è attaccabile); la dimensione dello spazio di Hilbert è nota esattamente

- Sicurezza *device-independent*
  Idealmente la sicurezza dovrebbe essere basata solo su caratteristiche testabili, e.g. la statistica degli eventi.
- Post-quantum theories
  $\mathbb{E}\left(A_1 B_1 + A_2 B_1 + A_2 B_2 - A_1 B_2\right) > 2\sqrt{2}$
- Sicurezza non solo "asintotica" ma anche per chiavi finite

Oltre la QKD

Il "bit commitment" è una *primitiva* per implementare calcolo distribuito sicuro. Esempio: Alice ha un input privato x e vuole aiutare Bob (cha ha input privato y) a calcolare una prescritta funzione $f(x, y)$ senza svelare x.

Quantum Bit Commitment

- *Preparazione:* Alice sceglie il valore di un bit b che vuole commissionare a Bob: se $b = 0$ (resp. $b = 1$) prepara $|0\rangle$ (resp. $|1\rangle$) in $\mathcal{H}_A$ e Bob prepara $|BC\rangle$ in $\mathcal{H}_B \otimes \mathcal{H}_C$
- *Commitment:* Rounds di comunicazione quantistica tra Alice e Bob dove ogni round può essere descritto da una trasformazione unitaria su $\mathcal{H}_\bullet \otimes \mathcal{H}_C$ $(\bullet = A, B)$
- *Apertura:* Rounds di comunicazione quantistica tra Alice e Bob dove ogni round può essere descritto da una trasformazione unitaria su $\mathcal{H}_\bullet \otimes \mathcal{H}_C$ $(\bullet = A, B)$

Oltre la QKD

Il "bit commitment" è sicuro se Bob apprende il valore di b qualora Alice abbia commissionato esso alla fine dello passaggio *Commitment*, senza possibilità di cambiarlo al successivo step *Apertura*

Alla fine del passaggio *Commitment* siano $|\Psi_0\rangle$ e $|\Psi_1\rangle$ i due stati corrispondenti ai due possibili valori di b. Bob non ha alcuna informazione su b, pertanto

$$\rho_0^{BC} = \mathrm{Tr}_A(|\Psi_0\rangle\langle\Psi_0|) = \rho_1^{BC} = \mathrm{Tr}_A(|\Psi_1\rangle\langle\Psi_1|)$$

ma allora

$$|\Psi_0\rangle = \sum_k \sqrt{\lambda_k}|e_k\rangle_A|f_k\rangle_{BC}$$

$$|\Psi_1\rangle = \sum_k \sqrt{\lambda_k}|e'_k\rangle_A|f_k\rangle_{BC}$$

ovvero $|\Psi_0\rangle$ e $|\Psi_1\rangle$ legati da una U sul solo spazio $\mathcal{H}_A$ di Alice!

Conclusioni

- Esistono ad oggi una varietà di altri protocolli crittografici oltre la QKD, e.g. Quantum Secret Sharing, Quantum Autenthication, Direct Quantum Communication, etc.
- La crittografia quantistica è annoverata da "Technology Review" come una delle dieci future tecnologie che rivoluzioneranno la nostra vita
- Recenti dimostrazioni sperimentali di QKD su distanze di molti Km utilizzando come quantum bit la polarizzazione dei fotoni
  I dispositivi crittografici quantistici sono già una realtà commerciale
  Prima quantum cryptographic network a Boston 2003, ultima proposta dalla Toshiba nel 2013

Conclusioni

Un approccio informatico alla fisica (quantistica)?

Postulati

- Impossibilità di segnali superluminali
- Impossibilità di perfetto broadcasting
- Impossibilità del bit commitment assolutamente sicuro