9 ELITZUR-VAIDMAN *BOMB TESTER*

I — INTRODUZIONE

La meccanica quantistica è ricca di fenomeni poco intuitivi se interpretati nell'ambito della fisica classica a cui siamo abituati. Alcuni di questi, come l'entanglement e la sovrapposizione di stati, sono alla base delle applicazioni informatiche. Altri stanno ancora trovando piano piano applicazioni nuove e inaspettate.

Quello che discutiamo in questo capitolo è un esperimento proposto da Elitzur e Vaidman nel 1993 [**EV_bomb1993**]. Quello che notarono è che ci sono situazioni in meccanica quantistica si può ottenere informazione su un oggetto senza misurarlo direttamente (o meglio senza interagire con esso). Per questo motivo chiamarono questo fenomeno "misura senza interazione" (*interaction-free measurement*). Per evidenziare l'apparente situazione paradossale (o meglio controintuitiva), immaginarono di costruire un *bomb tester* quantistico per testare lo stato di una bomba senza farla esplodere.

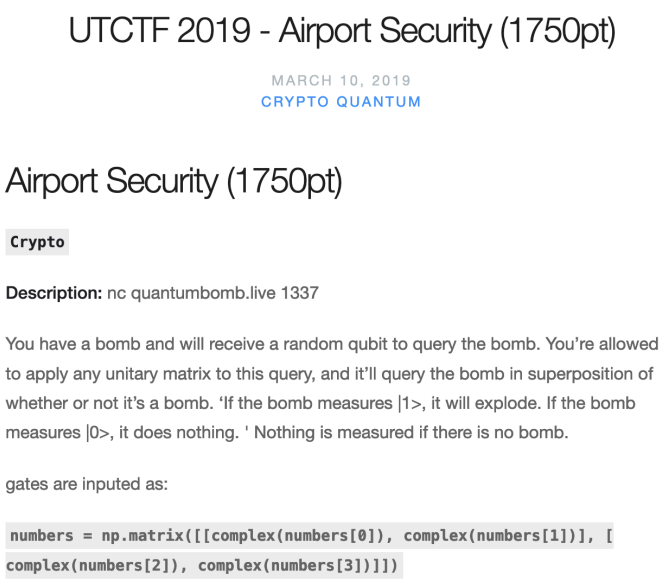
Quello che sembrava una pura idea da laboratorio, ha fatto la sua apparizione nel constato dell'informatica quantistica. In Fig. 25 è mostrata una *challenge* comparsa su un sito di informatici che pone il problema su come usare il *bomb tester* quantistico in un aeroporto.

II — INTERFEROMETRI

In figura 26 (a) è mostrato un tipo esperimento di ottica. Un fascio di luce *beam splitter* che lo divide in due fasci aventi intensità dimezzata. I due fasci vengono riflessi da due specchi (*mirror*) e si ricongiungono su un secondo *beam splitter* che li ricombina. la luce uscente dal secondo *beam splitter* viene infine misurata da due *detector*.

A seconda della lunghezza dei percorsi dei fasci di luce nei due bracci dell'interferometro, si hanno diversi fenomeni di interferenza. In particolare, i percorsi possono essere aggiustati in modo da far sì che solo il detector 1 rilevi il fascio mentre il detector 2 non riceve nessuna illuminazione. Questo eè un tipico fenomeno di interferenza in fisica in cui si ha interferenza costruttiva per il fascio che raggiunge il detector 1 e interferenza distruttiva per quello che raggiunge il detector 2.

Se diminuiamo l'intensità del fascio si raggiunge il regime quantistico dove entra nell'interferometro un solo fotone alla volta. Ls fenomenologia dell'effetto è la stessa ma in questo caso diremo che arrivato sul *beam splitter* il fotone avrà il



UTCTF 2019 - Airport Security (1750pt)

MARCH 10, 2019
CRYPTO QUANTUM

Airport Security (1750pt)

`Crypto`

Description: nc quantumbomb.live 1337

You have a bomb and will receive a random qubit to query the bomb. You're allowed to apply any unitary matrix to this query, and it'll query the bomb in superposition of whether or not it's a bomb. 'If the bomb measures |1>, it will explode. If the bomb measures |0>, it does nothing. ' Nothing is measured if there is no bomb.

gates are inputed as:

```
numbers = np.matrix([[complex(numbers[0]), complex(numbers[1])], [
complex(numbers[2]), complex(numbers[3])]])
```

Figure 25: Una challenge comparsa su un sito informatico. Dedicata alla sicurezza aeroportuale immagina di usare il *bomb tester* quantistico proposto da Elitzur e Vaidman.

50% di possibiltà di passare in un ramo e il 50% di andare nell'altro. Il fotone verrà poi riflesso dagli specchi e "ricombinato" dal secondo *beam splitter*. Anche in questo caso l'interferenza farà in modo che sia misurato solo dal detector 1.

Possiamo formalizzare questo fenomeno usando la notazione della quantum information:

1. i fotoni nei rami orizzontali sono associati allo stato $|0\rangle$.
2. i fotoni nei rami verticali sono associati allo stato $|1\rangle$.

Un fascio/fotone che incide in un *beam splitter* viene "diviso" nei due rami con probabilià del 50%. Lo specchio trasforma i fotoni "orizzontali" in fotoni "verticali". Quindi possiamo fare l'associazione con porte le logiche quantistiche

1. il *beam splitter* è associato ad una porta di Hadamard H.
2. lo specchio è associato ad una porta X (NOT).

Con queste notazioni abbiamo che la dinamica dell'interferometro in Fig. 26 (a) è

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow{X} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow{H} |0\rangle\,. \tag{9.2.1}$$

Come si vede, il fotone finale esce dall'interferometro orizzontalmente ed è quindi assorbito (misurato) sempre dal detector 1. Si noti inoltre che gli specchi (porte

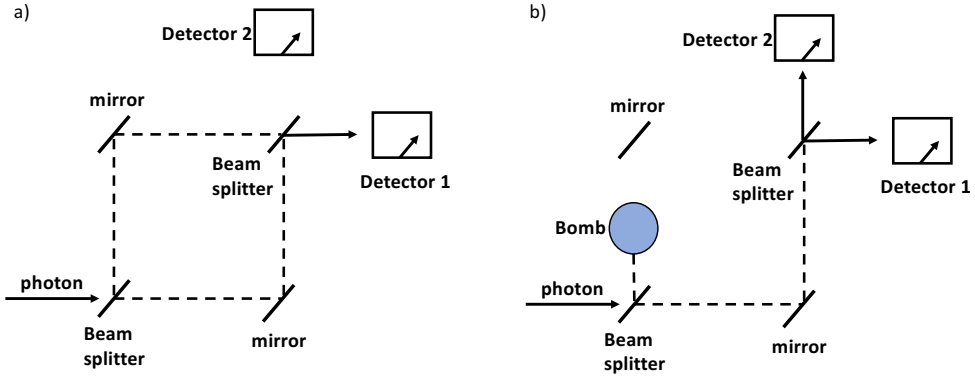


Figure 26: a) Un interferometro costituito da due *beam splitter* e due specchi riflettenti. I bracci dell'interferometro sono costruiti in modo tale che i fotoni arrivino solo al detector 1. b) Lo stesso interferometro in cui è stato posto un oggetto in uno dei bracci. L'oggetto assorbe tutti i fotoni passanti lungo la traiettoria. Questo distrugge il fenomeno di inerferenza fra i due percorsi e di conseguenza i fotoni che arrivano al secondo *beam splitter* sono misurati da entrambi i detector.

logiche X) non hanno effetto sullo stato visto che lo stato $|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$ è autostato (con autovalore 1) dell'operatore X.

Adesso supponiamo che un oggetto assorbente venga posto nel ramo verticale come mostrato in figura 26 (b). Il fotone incidente sul primo *beam splitter* andrà la metà delle volte nel ramo orizzontale e l'altra metà nel ramo verticale. Questi ultimi varranno assorbiti mentre quelli nel ramo orizzontale invece verranno riflessi e poi "divisi" dal secondo *beam splitter*. In questo caso però non ci sarà interferenza con il fotone del ramo verticale dato che questo è stato assorbito. Quindi il fotone incidente sul secondo *beam splitter* potrà essere assorbito sia dal detector 1 che dal detector 2 come mostrato in Fig. 26 (b).

Possiamo anche stimare con che probabilità i fotoni verranno assorbiti dai detector. Il 50% dei fotoni verranno assorbiti dopo il passaggio attraverso il primo *beam splitter*. Della metà passanti nel ramo inferiore, la metà varrà deviata e assorbita dal detector 1 e l'altra metà dal detector 2 (per un totale del 25% in entrambi i casi). Concludiamo che

1. il 25% delle volte si attiverà il detector 1.

2. il 25% delle volte si attiverà il detector 2 .

3. il 50% nessun detector si attiverà .

Notiamo che la differenza fra le due situazioni descritte in Fig. 26, sta nella possibilià di misurare dei fotoni con il detector 2. Questo avviene con probabilità 0.25 se l'oggetto assorbente è presente e non può avvenire quando è assente. Concludiamo che, se un fotone (passando nel ramo inferiore) viene successivamente

misurato dal detector 2, siamo sicuri che ci sia un oggetto assorbente senza che il fotone abbia interagito con esso [1].

Possiamo vedere questo fenomeno a livello più preciso introducendo un terzo stato $|a\rangle$ che rappresenta il fotone assorbito. Il fenomeno in Fig. 26 (b) sarà

$$\begin{aligned} |0\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow{\text{assorbimento}} \frac{1}{\sqrt{2}}(|0\rangle + |a\rangle) \\ &\xrightarrow{X} \frac{1}{\sqrt{2}}(|1\rangle + |a\rangle) \xrightarrow{H} \frac{1}{2}(|0\rangle - |1\rangle) + \frac{1}{\sqrt{2}}|a\rangle \end{aligned} \tag{9.2.2}$$

Si noti che le porte X e H agiscono solo sullo stato $|0\rangle$ e 1 dato che non ha senso applicarle al fotone assorbito. Se vengono misurati i fotoni in direzione orizzontali (dal detector 1) e quelli in direzione verticale (dal detector 2), avremo

1. Probabilità 0.25 di misurare $|0\rangle$ con il detector 1.
2. Probabilità 0.25 di misurare $|1\rangle$ con il detector 2.
3. Probabilità 0.5 di non misurare niente con i detector (lo stato $|a\rangle$ non è misurabile con i detector).

Notiamo che la differenza fra le due situazioni descritte in Fig. 26, sta nella possibilià di misurare dei fotoni con il detector 2. Questo avviene con probabilità 0.25 se l'oggetto assorbente è presente e non può avvenire quando è assente. Esattamente quello che ci aspettavamo dalla discussione più fenomenologica dell'esperimento.

III — BOMB DETECTOR

Per rendere più evidente quanto questo risultato sia controintuitivo, Elitzur e Vaidman proposero di usarlo in una situazione pratica.

Supponiamo di avere un certo numero di bombe che vengono attivate da un detector di fotoni. Se il detector è rotto e la bomba risulta inattiva.

Problema: Vogliamo sapere quali bombe sono attive senza farle esplodere.

Classicamente il problema non è risolvibile. Infatti, l'unico modo per sapere se una bomba è attiva è mandare un fotone ma questo farebbe esplodere la bomba.

Il problema è (parzialmente) risolvibile usando la meccanica quantistica e l'esperimento discusso. Se la bomba è inattiva i fotoni che passano nel ramo verticale dopo il primo *beam splitter* non interagiscono con il detonatore e continuano senza interagire. La bomba inattiva coincide quindi con la situazione in fig. 26 (a) e, a causa dell'interferenza, solo il detector 1 misurerà i fotoni.

Se la bomba è attiva, il 50% dele volte il fotone passerà nel ramo verticale, verrà assorbito e farà esplodere la bomba. In questi casi il nostro protocollo fallisce dato che la bomba *era* attiva ma esplode durante il controllo.

1 Da qui la teminologia usata del lavoro originale: *interaction-free measurement*.

Il restante 50%delle volte il fotone passerà nel ramo orizzontale e da qui (dopo il *beam splitter*) sarà misurato dal detector 1 nel 25% dei casi e nel rimanente 25% dei casi dal detector 2. Se il detector 1 misura il fotone non abbiamo alcuna informazione sulla bomba; infatti, avremmo lo stesso segnale dal detector 1 sia in presenza di una bomba inattiva che in presenza di una bomba attiva.

La discriminazione può avvenire quando è il detector 2 che misura il fotone. Infatti, in questo caso, una bomba attiva non attiverebbe mai questo detector. Concludiamo che, se il detector 2 riceve un fotone, la bomba è attiva. Si noti che però il fotone non ha interagito con la bomba dato che è passato nel ramo orizzontale.

Per quanto sorprendente questo fatto è naturale nella meccanica quantistica ed è simile a quello visto nell'esperimento della doppia fenditura in sec. 3.1.1. Infatti, gli stati quantistici sono descritti da funzioni d'onda; tralasciando per un momento la precisione nel linguaggio, possiamo dire che queste, come le onde nei sistemi fisici, sono "non-locali" e una perturbazione in una parte della funzione d'onda genera o distrugge l'interferenza.

9.3.1 Estensione e miglioramento

Nel caso discusso fino ad ora, il 50% delle volte la bomba esplode, 25% la bomba non esplode ma non abbiamo informazione utile e solo il restante 25% riusciamo ad sapere che la bombda è attiva senza farla esplodere. Sebbene questi risultati siano sorprendenti e migliori di quanto non si possa fare classicamente non sono soddisfacenti in termini assoluti. La domanda naturale è se si può fare meglio. Seguendo la referenza [**Kwiat1995**] mostreremo che la risposta è affermativa.

Supponiamo di fare due modifiche all'interferometro in Fig. 26. La prima è nei *beam splitter* che possono essere costruiti in modo tale che la maggior parte dei fotoni passi nel ramo orizzontale e soli pochi nel ramo verticale.

A livello formale, questo significa che non avremo più un operatore di Hadamard associato al *beam splitter* ma un generico operatore di rotazione scrivibile come

$$U_{BS}(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}. \tag{9.3.1}$$

nella base $\{|0\rangle, |1\rangle\}$. Si noti che per $\theta = \pi/4$, otteniamo la matrice di Hadamard.

La matrice $U_{BS}(\theta)$ è una matrice di rotazione di un angolo θ nello spazio $\{|0\rangle, |1\rangle\}$[2].

La seconda modifica da apportare all'interferometro è di non misurare i fotoni dopo un passaggio ma riprendere i fotoni e farli passare attraverso N *beam splitter* prima di misurarli [3]. Indipendentemente dalla struttura fisica utilizzata, questo equivale ad applicare l'operatore $U_{BS}(\theta)$ e quindi indurre una rotazione di un angolo $N\theta$.

2 Si veda, ad esempio, https://en.wikipedia.org/wiki/Rotation_matrix.

3 Questo può essere fatto utilizzando una sequenza di *beam splitter* oppure prendendo il fotoni nei due rami e, con delle fibre ottiche, reindirizzarli verso il *beam splitter* iniziale.

Supponiamo quindi che la bomba sia inattiva e di applicare $U_{BS}^{N}(\theta)$. Avremo

$$|0\rangle \xrightarrow{U_{BS}(\theta)} \cos\theta\,|0\rangle + \sin\theta\,|1\rangle \xrightarrow{U_{BS}(\theta)} \cdots \xrightarrow{U_{BS}(\theta)} \cos(N\theta)\,|0\rangle + \sin(N\theta)\,|1\rangle \quad (9.3.2)$$

A questo punto si vede che se scegliamo $\theta = \pi/(2N)$, lo stato finale sarà $|1\rangle$ e solo un detector misurerà i fotoni.

Supponiamo adesso che la bomba sia attiva. Dopo il primo passaggio attraverso il *beam splitter*, il fotone nel ramo verticale (stato $|1\rangle$) verrà assorbito. Come sopra, descriviamo questo effetto introducendo la trasformazione $|1\rangle \to |a\rangle$ dovuta all'assorbimento. Il primo passaggio sarà

$$|0\rangle \xrightarrow{U_{BS}(\theta)} \cos\theta\,|0\rangle + \sin\theta\,|1\rangle \xrightarrow{\text{assorbimento}} \cos\theta\ |0\rangle + \sin\theta\,|a\rangle \quad (9.3.3)$$

Come visto sopra la seconda applicazione del *beam splitter* cambierà solo i fotoni negli stati $|0\rangle$ e $|1\rangle$. Avremo quindi

$$\begin{aligned} \cos\theta\ |0\rangle + \sin\theta\,|a\rangle \quad &\xrightarrow{U_{BS}(\theta)} \quad \cos\theta\,(\cos\theta\,|0\rangle + \sin\theta\,|1\rangle) + \sin\theta\,|a\rangle \\ &\xrightarrow{\text{assorbimento}} \quad \cos^2\theta\,|0\rangle + (\cos\theta\sin\theta + \sin\theta)\,|a\rangle \end{aligned} \quad (9.3.4)$$

L'effetto di aver applicato due *beam splitter* (seguiti dall'assorbimento) è di avere lo stato del fotone $|0\rangle$ (quello che è ancora nella fibra ottica o nell'interferometro) con un'ampiezza di probabilità di $\cos^2\theta$. Questo fissa attraverso la normalizzazione anche il coefficiente dello stato assorbito $|a\rangle$.

Estendendo questa osservazione al caso di N applicazioni del *beam splitter*, otterremo lo stato

$$|0\rangle \xrightarrow{U_{BS}^{N}(\theta)} \cos^N\theta\,|0\rangle + (\cdots\cdots)\,|a\rangle \quad (9.3.5)$$

Per $N \gg 1$ e ricordando che abbiamo scelto $\theta = \pi/(2N)$, la probabilità di misurare $|0\rangle$ è

$$\cos^{2N}\theta = \left[\cos\left(\frac{\pi}{2N}\right)\right]^{2N} \approx \left[1 - \left(\frac{\pi}{2N}\right)^2\right]^{2N} \approx 1 - \frac{\pi^2}{8N} \quad (9.3.6)$$

Quindi, in presenza della bomba attiva, la probabilità di misurare $|0\rangle$ si approssima a 1 se prendiamo θ sufficientemente piccolo e N (il numero di *beam splitter*) sufficientemente grande.

Riassumendo per N grande, se la bomba non è attiva misureremo $|1\rangle$ (con certezza) mentre se la bomba è attiva misureremo $|0\rangle$ con una probabilità prossima a 1. Questo schema ci permette quindi di distinguere fra i due casi senza far esplodere la bomba.

Questo schema migliorato è stato proposto e verificato sperimentalmente da ricercatori austriaci e statunitensi **[Kwiat1995]**. Lo schema ottico usato è presentato in figura 27. L'idea è quella di far passare il fotone in una serie di *beam splitter*(rappresentati nella zona centrale delle figure) e di specchi (posti superiormente e inferiormente nelle figure).

In figura 27 a) è mostrato il set-up sperimentale in cui il singolo *beam splitter*fa passere nel ramo superiore dell'interferometro pochi fotoni che nella mag-

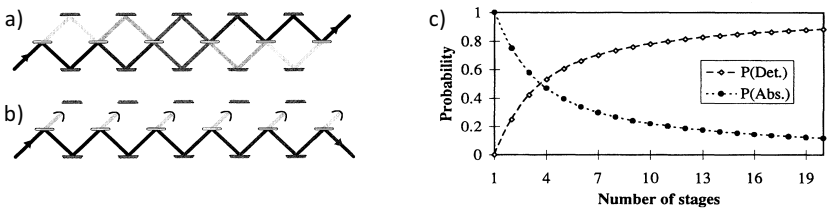


Figure 27: a) Un interferometro costituito da due *beam splitter* e due specchi riflettenti. I bracci dell'interferometro sono costruiti in modo tale che i fotoni arrivino solo al detector 1. b) Lo stesso interferometro in cui è stato posto un oggetto in uno dei bracci. L'oggetto assorbe tutti i fotoni passanti lungo la traiettoria. Questo distrugge il fenomeno di inerferenza fra i due percorsi e di conseguenza i fotoni che arrivano al secondo *beam splitter* sono misurati da entrambi i detector.

gior parte dei casi vengono riflessi verso il basso. Sebbene l'effetto del singolo *beam splitter*sia piccolo, la successione unita agli effetti di interferenza fanno uscire il fotone verso il ramo superiore.

Lo schema in figura 27 b) rappresenta il caso in cui sia presenta la bomba. Questa è descritta da un detector che assorbe i fotoni che, attraversando il *beam splitter*, passano nel ramo superiore dell'interferometro. In questo caso, dopo la successione di interferometri, il fotone esce dal ramo inferiore.

La figura 27 c) rappresenta i risultati sperimentali ottenuti in funzione del numero di interferometri usati. Le funazioni $P(\mathrm{Det.})$ e $P(\mathrm{abs.})$ sono rispettivamente la probabilità di ottenere informazione senza interagire con l'oggetto e la probabilità che il fotone venga assorbito. Come si può vedere, all'aumentare del numero di interferometri si riduce la probabilità di assorbimento del fotone mentre si riesce ad ottenere informazione (con probabilità crescente).