Università degli Studi di Padova

Dipartimento di Fisica e Astronomia "G. Galilei"

Dipartimento di Ingegneria dell'Informazione

Corso di Laurea in Fisica

Generazione di numeri casuali dalle fluttuazioni quantistiche del vuoto elettromagnetico

Autore:
Giulio Foletto

Relatore:
Dott. Giuseppe Vallone

9 luglio 2015

UNIVERSITA' DEGLI STUDI DI PADOVA

Sommario

Dipartimento di Fisica e Astronomia "G. Galilei"
Dipartimento di Ingegneria dell'Informazione

Corso di Laurea in Fisica

Generazione di numeri casuali dalle fluttuazioni quantistiche del vuoto elettromagnetico

di Giulio Foletto

L'obiettivo della presente tesi è esporre le applicazioni della fisica quantistica nell'ambito della generazione di numeri casuali, un problema importante nel mondo informatizzato del XXI secolo. Gli usi dei numeri casuali vanno dai giochi alla crittografia, passando per le simulazioni scientifiche, ma spesso essi vengono generati con tecniche inaffidabili. A seguito di una breve panoramica sulla storia e sullo stato dell'arte in questo campo, si darà una spiegazione dei concetti teorici necessari per comprendere appieno l'argomento dal punto di vista fisico e si mostrerà quindi un setup sperimentale che sfrutta le fluttuazioni del vuoto elettromagnetico per creare stringhe di numeri casuali sicure ed efficaci.

Ringraziamenti

L'autore desidera ringraziare esplicitamente il relatore dott. Giuseppe Vallone per l'assistenza e le spiegazioni fornite, nonché il dott. Davide G. Marangon per il fondamentale aiuto prestato in laboratorio, per l'organizzazione dell'esperimento e la preparazione dell'apparato.

Indice

Capitolo 1

Introduzione

L'uomo ha imparato a sfruttare a suo vantaggio il caso in tempi molto lontani. Si hanno prove di giochi governati dal caso risalenti addirittura alla preistoria, mentre in ere successive si usavano vari stratagemmi per eliminare ogni influenza da un certo evento al fine di renderlo il più "equo" possibile o di interpretare la volontà divina. Tuttavia, è stato in epoca moderna che lo studio della casualità ha preso una dimensione nuova e di fondamentale importanza per la ricerca scientifica.

Gustav Fechner, negli anni 50 del XIX secolo, confrontò dati meteorologici, nascite, morti e suicidi con una sequenza di numeri casuali ottenuta da dieci diverse lotterie attive negli anni precedenti, il tutto allo scopo di verificare se tali fenomeni potessero essere influenzati da circostanze "locali" o fossero "puramente casuali" [1]. Vent'anni dopo, Erastus DeForest eseguì la prima vera simulazione con dati randomici, con l'obiettivo di comparare funzioni matematiche e dati reali, tenendo però conto degli errori di osservazione. Nel 1927 Leonard Tippet fu il primo a pubblicare una tabella di ben 41600 cifre casuali, poi superata dalla "A Million Random Digits with 100000 Normal Deviates" della RAND Corporation (1955) [2]. Tali dati erano utilizzati per previsioni economiche, studi biologici, sociologici, meteorologici, matematici e fisici. Rapidamente crebbe la domanda di dati (e poi semplicemente numeri) casuali, che servivano per simulazioni e statistiche. Nondimeno, con l'avvento del calcolatore fu chiaro che usare tabelle non sarebbe stato sufficientemente rapido e si cercarono strategie per generare fenomeni casuali nuovi ogni volta che fosse stato necessario. Nacquero così i primi Random Number Generators (RNG).

Parallelamente all'avanzamento delle tecniche e delle necessità, progredì in modo notevole anche lo studio teorico, che pian piano avrebbe rivoluzionato il concetto stesso di caso. L'idea, quasi innata, di casualità è associata all'imprevedibilità o alla mancanza di cause, ma profondamente radicato è anche il legame con l'ignoranza: un fenomeno è

casuale solo perché non sono note le condizioni iniziali che lo caratterizzano [3]. Questa linea di pensiero fu favorita dalla fisica newtoniana, le cui regole obbediscono a un determinismo perfetto: con un'infinita precisione sui dati iniziali si può prevedere l'evoluzione futura (e passata) di un sistema, ma ogni minimo errore aumenta esponenzialmente la sua importanza col tempo. È anche per questo che si tende ad associare risultati casuali a fenomeni complessi, in cui gli errori possono avere le conseguenze più varie e imprevedibili.

Oggi, tuttavia, si vorrebbe slegare la nozione di casualità dall'ignoranza dell'osservatore riguardo al sistema e andare oltre il banale (ma non facile) atto di nascondere il determinismo dietro la complessità. Per quanto non si sia arrivati ad una definizione universale [4], in questo lavoro si parlerà di "numeri veramente casuali'" per indicare sequenze uniformi e scorrelate da qualsiasi informazione esterna [5]. La fisica quantistica fornisce tecniche semplici e puramente indeterministiche, i cui risultati sono imprevedibili anche con un livello di conoscenza perfetto dei dati iniziali. Con il giusto apparato si possono generare sequenze di elevata qualità (relativamente ai test) che possano quindi essere usate in simulazioni scientifiche o in contesti in cui si richiede grande sicurezza, come in crittografia.

1.1 I Random Number Generators

Le tecniche utilizzate per produrre risultati casuali hanno fatto passi da gigante nell'ultimo secolo. Mentre i primi lavori di Tippet (1920) si basavano ancora sull'estrazione di cartoncini numerati da una scatola [2], oggi i calcolatori possono generare lunghissime sequenze binarie a grandi velocità [6]. Per farlo vengono impiegati vari metodi: quelli più rapidi ed economici, a partire da una piccola variabile randomica (seme), ad esempio l'istante temporale esatto in cui viene iniziata la procedura, usano algoritmi matematici per ottenere lunghe stringhe di 0 e 1. Con le giuste funzioni è possibile ricavare sequenze di buona qualità che possono essere usate anche in applicazioni scientifiche come le simulazioni Monte Carlo. Tali tecniche sono evidentemente di facile implementazione e utilizzabili da qualsiasi computer; inoltre, come tutte le soluzioni software, sono molto versatili e velocemente migliorabili. Tuttavia, la loro lacuna principale è insita nella natura algoritmica del processo: la stringa finale è completamente prevedibile a partire dal seme (e da parti di essa stessa, a causa di correlazioni) e per questo è detta pseudocasuale, da cui Pseudo Random Number Generators (PRNG).

Un primo passo avanti è quello degli Hardware Random Number Generators, che sfruttano fenomeni fisici come il rumore termico dell'apparecchiatura elettronica. Ad esempio si usa frequentemente l'effetto Johnson, per cui una differenza di potenziale casuale si

genera ai capi di una resistenza a causa del moto dei portatori di carica. Oppure si può utilizzare il rumore Zener, dovuto ad elettroni che attraversano barriere di potenziale per effetto tunnel. Comunque, a livello pratico ciò che si fa è misurare tensioni e confrontarle con un valore di soglia predefinito: i due possibili risultati di questa operazione (minore o maggiore) vengono poi tradotti in una nuova cifra casuale (0 o 1). Il problema è che la conoscenza dei parametri che governano questi fenomeni è limitata ed è quindi complicato scegliere la soglia, risulta dunque più conveniente selezionarla empiricamente al fine di minimizzare il bias fra 0 e 1 nella sequenza output, ma questa resta comunque un'operazione dispendiosa e imperfetta.

Un'altra tecnica spesso usata è quella dei Free Running Oscillators. Si costruisce un oscillatore logico dando come input ad un inverter il suo stesso output. Un secondo oscillatore, più lento, viene usato per testare il valore logico del primo e generare quindi la cifra casuale. È chiaro che le frequenze dei due apparati non possono essere costanti, altrimenti il risultato esibirebbe periodicità, tuttavia questo non è un grosso problema vista la suscettibilità di tali circuiti al rumore del segnale in ingresso. I FROs sono una soluzione relativamente economica e producono ottimi risultati, ma, come tutti gli HWRNG basati su fenomeni classici, non lavorano mai in maniera totalmente indeterministica e il loro comportamento è, in linea di principio, prevedibile [7].

1.2 Qubit e QRNG

Tutti i dispositivi di cui si è parlato finora lavorano, almeno a livello macchina, per produrre dei bit, cioè variabili a due soli valori, 0 o 1. L'utilizzo del sistema binario è estremamente pratico per l'elettronica basata sul transistor, ma è anche comodo a livello teorico, in quanto più semplice metodo per codificare ogni tipo di messaggio, per questo il bit è l'unità elementare di informazione. I computer possono immagazzinare i bit tramite apparati fisici a due stati, come campi magnetici orientati o le fossette scavate sulle superfici dei dischi ottici. Ma non esistono solo sistemi classici: vi sono moltissimi sistemi quantistici a due stati perfettamente in grado di rappresentare un bit. Ad esempio una particella di spin $\frac{1}{2}$ può trovarsi nello stato $|+\rangle$ (up, su) o nello stato $|-\rangle$ (down, giù) e da essi si può definire una corrispondenza del tipo $|+\rangle \to 0$, $|-\rangle \to 1$. C'è però una fondamentale novità: tale particella può anche trovarsi in una sovrapposizione dei due stati

$$|\varphi\rangle = \lambda|+\rangle + \mu|-\rangle \text{ con } |\lambda|^2 + |\mu|^2 = 1$$

Si introduce quindi il concetto di qubit, cioè una combinazione lineare dei due valori 0 e 1

$$|\varphi\rangle = \lambda|0\rangle + \mu|1\rangle$$

Quando si esegue una certa misura sul sistema che lo rappresenta, nell'esempio quella della componente dello spin lungo un asse fissato, lo si proietta su 0 o 1. La probabilità che il risultato sia 0 (1) è $|\lambda|^2$ ($|\mu|^2$). È in questa natura probabilistica della misura che si mostrano le potenzialità dei sistemi quantistici per la generazione di numeri casuali.

Viene presentato ora un primo esempio di Quantum Random Number Generator (QRNG). Esso consiste di una sorgente (S) che invia fotoni verso un Polarizing Beam Splitter (PBS), e di un rivelatore (Alice, o A) che non fa altro che notare la presenza del fotone in una delle due uscite del PBS e registrare 0 o 1 a seconda di quale delle due sia stata colpita.

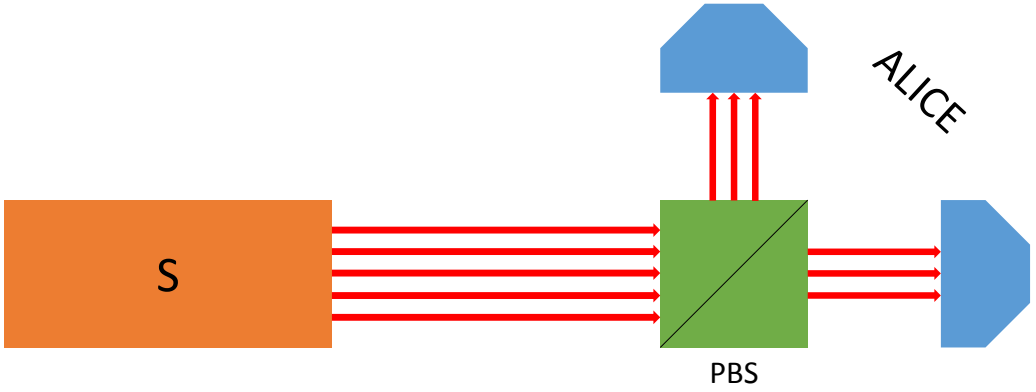

FIGURA 1.1: Schema di QRNG basato sulla polarizzazione di un fotone

Il PBS in generale ha il compito di separare la componente lineare verticale (V) della luce da quella lineare orizzontale (H) e di mandarle a due diverse uscite: un singolo fotone, essendo inscindibile, dovrà passare per l'una o per l'altra porta con una certa probabilità. Questa dipende dalla polarizzazione della luce in ingresso, sulla quale si può operare con una lamina mezz'onda e/o un phase shifter. Ad esempio se il fotone è polarizzato linearmente nello stato $|+45°\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$, la probabilità sarà $\frac{1}{2}$ per entrambe le uscite. In pratica Alice, tramite il PBS, sta eseguendo una misura di polarizzazione sul qubit (astrazione del fotone) facendone collassare lo stato su uno solo dei due possibili risultati.

Questo esempio è assai basilare e come tale non è privo di problemi. Innanzitutto non si sta tenendo conto delle imperfezioni che caratterizzano le realizzazioni pratiche di

apparati del genere, come una polarizzazione imprecisa, impurità nello stato del fotone, oppure un disallineamento del PBS. Inoltre, una misura nella base $\{H, V\}$, come quella eseguita dal rivelatore, non può distinguere fra stati misti del tipo $|\lambda|^2|H\rangle\langle H|+|\mu|^2|V\rangle\langle V|$ e puri come $\lambda|H\rangle + \mu e^{ia}|V\rangle$, $a \in R$, né può trovare la fase relativa a. A causa di ciò, applicazioni di questo tipo risultano vulnerabili. Si pensi per esempio ad una spia (da ora in poi "Eve", da "eavesdropper") interessata a predire la sequenza di cifre; ella potrebbe intercettare il fotone, eseguire una misura analoga a quella del QRNG e spedire al PBS uno stato $|V\rangle$ per ogni risultato uscito dalla porta verticale, e $|H\rangle$ per ognuno passato da quella orizzontale. Alice troverebbe una sequenza all'apparenza casuale, ma perfettamente correlata con quella ottenuta da Eve. Come risolvere questi ed altri problemi sarà oggetto di interesse dei prossimi capitoli.

Capitolo 2

Preliminari

In questo secondo capitolo ci si occuperà di fornire i preliminari teorici necessari per comprendere l'apparato sperimentale di cui si parlerà nel seguito, nonché per valutarne i risultati. Per prima cosa si toccheranno i fondamenti di teoria dell'informazione, fra cui l'entropia di Shannon e i suoi corrispondenti quantistici, ponendo l'accento sulle grandezze rilevanti per l'esperimento. Dopodiché si analizzeranno gli aspetti più propriamente fisici, in particolare il concetto di campo elettromagnetico quantistico e la tecnica della rivelazione omodina.

2.1 Entropia, informazione e randomicità

Fra gli obiettivi della teoria dell'informazione, uno dei più importanti è la valutazione della quantità di dati contenuta in un messaggio. Per questo scopo si usa prevalentemente il concetto di entropia di Shannon, così nominata in onore del matematico che la introdusse nel 1948. Se ad ogni carattere di un codice X si associa una probabilità $p(x_i)$ allora l'entropia di Shannon è:

$$S(X) = -\sum_i p(x_i) \log_2 \Big(p(x_i)\Big)$$

(d'ora in poi si userà il simbolo log in luogo di $\log_2$). Il primo significato pratico di questa misura è quello di massima compressione (cioè minima dimensione) che si può applicare ad un messaggio senza perderne il contenuto (source coding theorem [8]). Tale compressione si ottiene a livello di codifica, di solito binaria, traducendo ogni carattere con più o meno bit a seconda della sua probabilità.

Tuttavia, nel contesto di questa tesi è più interessante un secondo uso di S: dalla definizione si nota subito la somiglianza con l'entropia di Gibbs di un sistema termodinamico

ed in effetti entrambe sono profondamente collegate con il disordine dell'oggetto cui si riferiscono: in particolare per un messaggio, con la sua impredicibilità. Si pensi al risultato del lancio di una moneta: esso può avere due soli valori, testa o croce. Se la moneta è equa $p(T) = p(C) = \frac{1}{2}$ e l'entropia è massima $S = 1$, se invece la moneta è truccata e mostra solo croci, allora $p(T) = 0,\ p(C) = 1 \Rightarrow S = 0$. Intuitivamente a maggior entropia corrisponde maggior casualità.

A seguito dei lavori di Shannon sono state proposte numerose estensioni di questa prima definizione e sono state usate nuove grandezze per quantificare i vari aspetti dell'informazione. Innanzitutto una generalizzazione è offerta dall'entropia di Rényi, definita come

$$H_\alpha(X) = \frac{1}{1-\alpha} \sum_i \Big(p(x_i)\Big)^\alpha \qquad \alpha \geq 0,\ \alpha \neq 1$$

che va a coincidere con $S(X)$ per $\alpha \to 1$. Per $\alpha \to \infty$ si ha invece la min-entropy:

$$H_\infty(X) = -\log\Big(\max_i p(x_i)\Big) \tag{2.1}$$

il cui significato intuitivo è collegato alla probabilità di indovinare il messaggio con una strategia ottimale

$$p_{guess}(X) = \max_i p(x_i) = 2^{-H_\infty(X)}$$

2.1.1 Entropie in informazione quantistica

Volendo portare tutto ciò in ambito quantistico, la prima grandezza da tenere a mente è l'entropia di Von Neumann, pensata in realtà quindici anni prima di quella di Shannon come estensione dell'entropia termodinamica. Per uno stato descritto dalla matrice densità ϱ, essa è definita:

$$S(\varrho) = -Tr\,\varrho \ln(\varrho)$$

oppure, scrivendo ϱ in termine degli autostati $\varrho = \sum_{k=1}^{l} a_k |k\rangle\langle k|$,

$$S(\varrho) = -\sum_{k=1}^{l} a_k \ln a_k$$

L'entropia di Von Neumann è essenzialmente una misura di quanto lo stato sia lontano dalla purezza: se ϱ è puro allora $l = 1,\ a_1 = 1 \Rightarrow S(\varrho) = 0$. Tuttavia, essa è chiaramente legata all'entropia di Shannon, infatti una conseguenza della purezza è l'esistenza di una base in cui una misura proiettiva porta ad un certo risultato con probabilità 1: lo stato è in qualche modo prevedibile.

Nondimeno, più interessante è il corrispondente quantistico della min-entropy, in particolare nella sua versione condizionata. Per capire il motivo di ciò, si ricordi l'idea di "randomicità vera" accennata nell'introduzione: una sequenza è veramente casuale se è uniforme e scorrelata da ogni informazione esterna. Pensando ad un avversario (Eve) intenzionato ad indovinare la stringa di bit partendo da una qualche informazione in suo possesso, è fondamentale capire quanto il QRNG sia vulnerabile, ed è qui che interviene la min-entropy condizionata. Per uno stato quantistico bipartito ϱ_{AE} si definisce:

$$H_{min}(A|E)_{\varrho_{AE}} = \max_{\sigma_E} \sup \left\{ \lambda \in \mathbb{R} | \frac{\mathbb{I}_A \bigotimes \sigma_E}{2^\lambda} \geq \varrho_{AE} \right\}$$

in cui σ_E è un qualsiasi operatore densità normalizzato su E. Come si dimostra in [9] e in accordo con la definizione classica (2.1), se Eve controlla E, la sua probabilità di conoscere A usando la strategia ottimale è

$$p_{guess}(A|E) = 2^{-H_{min}(A|E)}$$

Per un singolo bit casuale sarebbe dunque ottimo avvicinare H_{min} a 1, in modo che p_{guess} non si allontani da $\frac{1}{2}$.

Un ultimo valore importante da segnalare prima di procedere è la max-entropy, che non è altro che il duale della min-entropy. Sempre nel formalismo delle entropie condizionate in ambiente quantistico, se ϱ_{AEC} è una purificazione di ϱ_{AE} allora

$$H_{max}(A|E)_{\varrho_{AE}} = -H_{min}(A|C)_{\varrho_{AE}}$$

2.1.2 Il principio di indeterminazione

Al fine di quantificare e controllare H_{min}, si può usare il principio di indeterminazione, come proposto in [5]. Come si è chiarito con l'esempio in sezione 1.2, la stringa casuale non è altro che il risultato di una misura quantistica (indicata da ora con Z); se si affianca ad essa una seconda misura X allora, per il principio di indeterminazione, vale

$$H_{min}(Z|E)_\varrho + H_{max}(X|B)_\varrho \geq -\log c =: q$$

(in cui si è usato $(Z|E)$ invece di $(A|E)$ solo per porre l'accento sul fatto che ci si sta riferendo ad una misura e non ad un generico sistema). A partire dagli spettri $\{x_i\}$ e $\{z_j\}$, $c := \max_{i,j} ||x_i^{\frac{1}{2}} z_j^{\frac{1}{2}}||$ [10] è l'overlap fra le due misure, mentre q rappresenta l'incompatibilità fra le basi di X e Z: se queste sono complementari su uno spazio di

dimensione d, allora $c = \frac{1}{d} \Rightarrow q = \log d$. Sostituendo a B uno spazio unidimensionale, si può trovare il limite inferiore:

$$H_{min}(Z|E)_\varrho \geq q - H_{max}(X)_\varrho \tag{2.2}$$

In pratica si è riportato il problema della randomicità del risultato di Z alla max-entropy della misura X. Minimizzando questa si massimizza $H_{min}(Z|E)_\varrho$ e quindi si toglie informazione a Eve, rendendo la stringa quanto più possibile casuale. $H_{max}(X)$ va calcolata sullo stato ottenuto dopo la misura di X, cioè $\varrho_X = \sum_x p_x |x\rangle\langle x|$. Seguendo i passi riportati in [5] si trova $H_{max}(X) = 2 \log \sum_x \sqrt{p_x}$, che per altro coincide con l'entropia di Rényi di ordine $\frac{1}{2}$ del risultato di X ed è pertanto facilmente stimabile.

È importante notare che molto spesso, per valutare i risultati di un QRNG, viene usata la min-entropy classica di (2.1), tuttavia la bontà di questo estimatore si basa sull'assunzione di purezza dello stato rivelato, che all'atto pratico non è mai verificata. Inoltre, si pensi al solito esempio di sezione 1.2: se l'avversario Eve agisse come lì proposto, Alice riceverebbe la miscela statistica di matrice densità $\frac{1}{2}\mathbb{I}_2$ e calcolerebbe $H_\infty = -\log(\frac{1}{2}) = 1$, non accorgendosi dell'intrusione. Invece, se utilizzasse come misura di controllo X la polarizzazione nella base $\{+45°; -45°\}$ noterebbe subito che lo stato in ingresso non è $|+45°\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ e potrebbe scartare i numeri generati. Questo si rifletterebbe nella (2.2) come $H_{max}(X)_\varrho \approx 1 \Rightarrow H_{min}(Z|E)_\varrho \geq 0$.

2.1.3 Estensione al caso di spettro continuo

L'apparato sperimentale di cui si parlerà nel prossimo capitolo utilizza una misura a spettro continuo, per cui è necessario modificare le precedenti relazioni al fine di eliminare il ruolo di d. Come spiegato in [10], non si può eseguire una diretta estensione al continuo senza perdere molte proprietà utili; invece è bene considerare discretizzazioni sempre più fini dello spettro. In tal maniera continua a valere la relazione

$$H_{min}(Z|E)_\varrho + H_{max}(X)_\varrho \geq -\log c$$

ma non è più possibile collegare c alla dimensione dello spazio, visto che $d \to \infty$. Comunque, se δ_Z e δ_X indicano le spaziature fra i valori spettrali di Z e X, l'overlap è comunque computabile come:

$$c(\delta_Z, \delta_X) = \tfrac{\delta_Z \delta_X}{2} \cdot S_0^{(1)}\left(1, \tfrac{\delta_Z \delta_X}{4}\right)^2$$

in cui con $S_0^{(1)}$ si è denotata la funzione d'onda prolata sferoidale del primo tipo. Analizzare il comportamento di tale funzione va oltre gli obiettivi di questa tesi, ma il suo

valore permette di fornire il limite inferiore sulla min-entropy:

$$H_{min}(Z|E)_\varrho \geq -\log\left\{\frac{\delta_Z\delta_X}{2}\cdot S_0^{(1)}\Big(1,\frac{\delta_Z\delta_X}{4}\Big)^2\right\} - H_{max}(X)_\varrho \tag{2.3}$$

che viene usato per stimare la quantità di bit veramente casuali estraibili dalla misura Z. A livello sperimentale, δ_Z e δ_X sono collegate alla precisione dello strumento utilizzato e sono quindi note.

2.2 La quantizzazione del campo elettromagnetico

Conclusa la parte legata alla teoria dell'informazione, si passa ora a temi più fisici. La trattazione quantistica del campo elettromagnetico nacque negli anni '20 ad opera di Paul Dirac e fu uno dei punti chiave nello sviluppo della fisica del secolo scorso. Se ne presenta qui un'introduzione, soffermandosi sui risultati salienti di un'analisi formalmente eseguita in maggior dettaglio in appendice A.

Vi sia una regione di spazio di volume L^3 pervasa da un campo elettromagnetico. L'hamiltoniana del sistema è

$$H = \frac{\varepsilon_0}{2}\int_{L^3}\Big(\|\vec{E}(\vec{r},t)\|^2 + \|c\vec{B}(\vec{r},t)\|^2\Big)d^3r$$

Il concetto di fondamentale importanza è la possibilità di vedere tale campo come un insieme di oscillatori armonici, il che non dovrebbe stupire vista la natura ondulatoria della luce. Eseguendo uno sviluppo in serie di Fourier delle varie grandezze, se $\vec{k}$ indica un modo di oscillazione, e quindi un vettore d'onda, l'hamiltoniana risulta essere:

$$H = \frac{\varepsilon_0 L^3}{2}\sum_{\vec{k}}\Big(\|\vec{E}_{\vec{k}}\|^2 + \|\omega_{\vec{k}}\vec{A}_{\vec{k}}\|^2\Big)$$

(in cui si è usato il potenziale vettore $\vec{A}_{\vec{k}}$ in luogo del campo magnetico $\vec{B}_{\vec{k}}$). $\vec{A}_{\vec{k}}$ ed $\vec{E}_{\vec{k}}$ sono sempre ortogonali alla direzione di propagazione $\hat{k}$, per cui sono descrivibili ciascuno con due componenti $A_{\vec{k},s}$, $E_{\vec{k},s}$ con $s = 1, 2$. Una volta introdotti gli operatori di distruzione $a_{\vec{k},s} = \sqrt{\frac{\varepsilon_0 L^3}{2\hbar\omega_{\vec{k}}}}(\omega_{\vec{k}}A_{\vec{k},s} - iE_{\vec{k},s})$, creazione $a^+_{\vec{k},s} = \sqrt{\frac{\varepsilon_0 L^3}{2\hbar\omega_{\vec{k}}}}(\omega_{\vec{k}}A_{\vec{k},s} + iE_{\vec{k},s})$ e numero $N_{\vec{k},s} = a^+_{\vec{k},s}a_{\vec{k},s}$, H si scrive

$$H = \sum_{\vec{k},s}H_{\vec{k},s} = \sum_{\vec{k},s}\hbar\omega_{\vec{k}}(N_{\vec{k},s} + \frac{1}{2})$$

Gli autovalori di $N_{\vec{k},s}$ sono interi $n_{\vec{k},s} = 0, 1, 2 \ldots$ ed $n_{\vec{k},s}$ indica il numero di fotoni nel modo di oscillazione descritto da $\vec{k}$ e polarizzati lungo il versore indicato da s. Per studiare gli autovettori $|\varphi_n\rangle$ di questo operatore (che lo sono anche di $H_{\vec{k},s}$), si introducono le grandezze quadrature $X_{\vec{k},s} = \frac{a_{\vec{k},s} + a^+_{\vec{k},s}}{\sqrt{2}}$ e $P_{\vec{k},s} = i\frac{a^+_{\vec{k},s} - a_{\vec{k},s}}{\sqrt{2}}$ (assieme anche alla variante $X_{\vec{k},s}(\theta) = \frac{a_{\vec{k},s} + e^{i\theta} a^+_{\vec{k},s}}{\sqrt{2}}$). Lo stato del campo in cui tutti gli $n_{\vec{k},s}$ sono nulli, cioè quello in cui vi è totale assenza di fotoni, è detto stato di vuoto elettromagnetico ed è di particolare interesse. Infatti, la sua funzione d'onda $\varphi_0(X)$ nella rappresentazione in coordinate di X è una gaussiana centrata in 0, e tale è quindi la densità di probabilità $|\varphi_0(X)|^2$: una misura di X, pur avendo valor medio nullo, produce risultati dispersi normalmente attorno a 0, con quelle che si chiamano fluttuazioni dello stato di vuoto.

$$\varphi(X) = (\tfrac{1}{\pi})^{\frac{1}{4}} e^{-\frac{1}{2}X^2}$$

$$|\varphi(X)|^2 = \tfrac{1}{\sqrt{\pi}} e^{-X^2}$$

$$\langle X \rangle_{\varphi_0} = 0$$

$$(\Delta X)^2_{\varphi_0} = \tfrac{1}{2}$$

Altri stati importanti sono gli autostati dell'operatore di distruzione, essi sono detti stati coerenti ed hanno la forma $|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_n \frac{\alpha^n}{\sqrt{n!}} |\varphi_n\rangle$. Per questi valgono le relazioni

- $a|\alpha\rangle = \alpha|\alpha\rangle$
- $\langle\alpha|a|\alpha\rangle = \alpha$
- $\langle\alpha|aa|\alpha\rangle = \alpha^2$
- $\langle\alpha|a^+|\alpha\rangle = \alpha^\star$
- $\langle\alpha|a^+a^+|\alpha\rangle = \alpha^{\star 2}$

2.3 La rivelazione omodina

Le tecniche di rivelazione omodina ed eterodina vengono utilizzate in telecomunicazioni (classiche) per ricevere ed analizzare segnali, tuttavia recentemente hanno anche trovato impiego in ambito quantistico, soprattutto allo scopo di ricostruire l'operatore densità di uno stato.

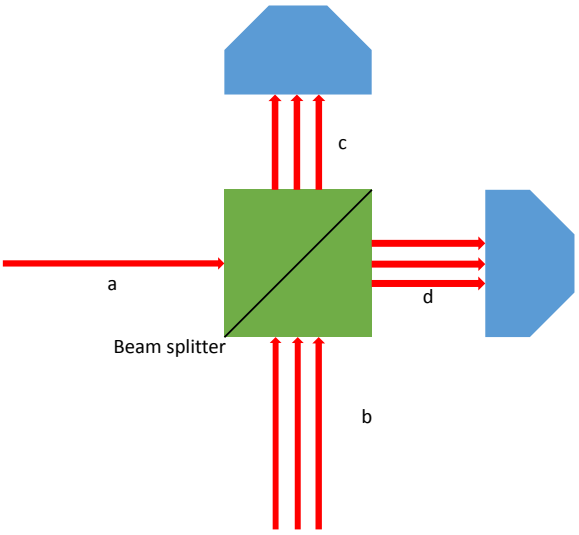

FIGURA 2.1: Schema di un apparato per rivelazione omodina

Un debole segnale indicato con ϱ (raggio a) viene fatto interferire in un mixer con un fascio più forte (b) detto oscillatore locale (LO, dall'inglese Local Oscillator), le due uscite risultanti vengono ricevute da altrettanti fotodiodi (c, d) che le convertono in un segnale in corrente facilmente studiabile. Nell'omodina segnale e LO hanno la stessa frequenza, tuttavia la fase relativa può essere modificata con un phase shifter. Normalmente si misura la differenza delle correnti in uscita dai fotodiodi, che, in condizioni di idealità di questi, riflette la differenza nel numero di fotoni $N_- = N_c - N_d$: questa grandezza è importante perché è equivalente ad una misura di X per il segnale ϱ. Infatti, indicando con a, b, c, d gli operatori di distruzione rispettivamente di ϱ, LO e della luce in entrata ai due fotodiodi, si ha $c = \frac{b+ia}{\sqrt{2}}$, $d = \frac{a+ib}{\sqrt{2}}$, per cui

$$N_- = N_c - N_d = c^+c - d^+d = \frac{(b^+ - ia^+)(b+ia)}{2} - \frac{(a^+ - ib^+)(a+ib)}{2} = iab^+ - ia^+b$$

Si pone ora che il Local Oscillator sia uno stato coerente $\beta = |\beta|e^{i\phi}$ in cui ϕ indica la fase relativa a ϱ. Allora risulta:

$$\langle \varrho \bigotimes \beta | N_- | \varrho \bigotimes \beta \rangle = i(\langle \varrho | a | \varrho \rangle \cdot \langle \beta | b^+ | \beta \rangle - \langle \varrho | a^+ | \varrho \rangle \cdot \langle \beta | b | \beta \rangle) = \sqrt{2}|\beta| e^{i(\frac{\pi}{2} - \phi)} \langle \frac{a + e^{i(2\phi - \pi)} a^+}{\sqrt{2}} \rangle_\varrho = \sqrt{2}|\beta| e^{i(\frac{\pi}{2} - \phi)} \langle X(\theta = 2\phi - \pi) \rangle_\varrho$$

Anche la fluttuazione ΔN_- è direttamente collegata a quella di $X(\theta)$:

$$(\Delta N_-)^2_{\varrho \bigotimes \beta} = \langle a^+ a \rangle_\varrho + \frac{2|\beta|^2 (1 + 2\langle a^+ a \rangle_\varrho - e^{2i\phi} \langle a^+ a^+ \rangle_\varrho - e^{-2i\phi} \langle aa \rangle_\varrho)}{2} + 2|\beta|^2 e^{-2i\phi} \langle X(2\phi - \pi) \rangle_\varrho$$

È chiaro che N_- ha molto in comune con $N' := \sqrt{2}|\beta|e^{i(\frac{\pi}{2}-\phi)}X(2\phi-\pi)$, in effetti:

$$\langle N_- \rangle_{\varrho \bigotimes \beta} = \langle N' \rangle_{\varrho \bigotimes \beta} \tag{2.4}$$

$$(\Delta N_-)^2_{\varrho \bigotimes \beta} = (\Delta N')^2_{\varrho \bigotimes \beta} + \langle a^+ a \rangle_\varrho \tag{2.5}$$

ma quest'ultimo addendo $\langle a^+ a \rangle_\varrho$ è trascurabile nel limite $|\beta| \to \infty$. In questo senso misurare N_- fornisce informazioni su N' e quindi su $X(2\phi-\pi)$. (In appendice B questi calcoli sono riportati in maniera più dettagliata).

Nell'esperimento di interesse a questa tesi si pone che ϱ sia lo stato di vuoto elettromagnetico e che $\phi = \frac{\pi}{2}$, in modo da considerare semplicemente $X(\theta = 0) = X$. La quadratura di questo stato è particolarmente interessante perché, come accennato sopra, la sua densità di probabilità $|\varphi_0(x)|^2$ è una gaussiana centrata in $\langle X \rangle_\varrho = 0$ e di ampiezza $(\Delta X)_\varrho$. Ne consegue che i conteggi di misure ripetute di N_- su un segnale pulsato si disporranno in prima approssimazione in modo simile a tale gaussiana.

È qui che questa tecnica si rende utile per la generazione di numeri casuali. Il risultato stesso della misura di X è un evento casuale per via della fluttuazione del vuoto elettromagnetico. Si può dividere la densità di probabilità in 2^n bin di uguale area ed associare a ciascuno di essi una stringa di n bit. Allora ad ogni misura inserita nell'istogramma corrisponde una nuova stringa casuale e la distribuzione complessiva di 0 e 1 risulta uniforme. In alternativa, ed è quello che si farà nel prossimo capitolo, si possono usare bin di larghezza fissa e ottenere una sequenza non uniforme da modificare in fase di post-processing.

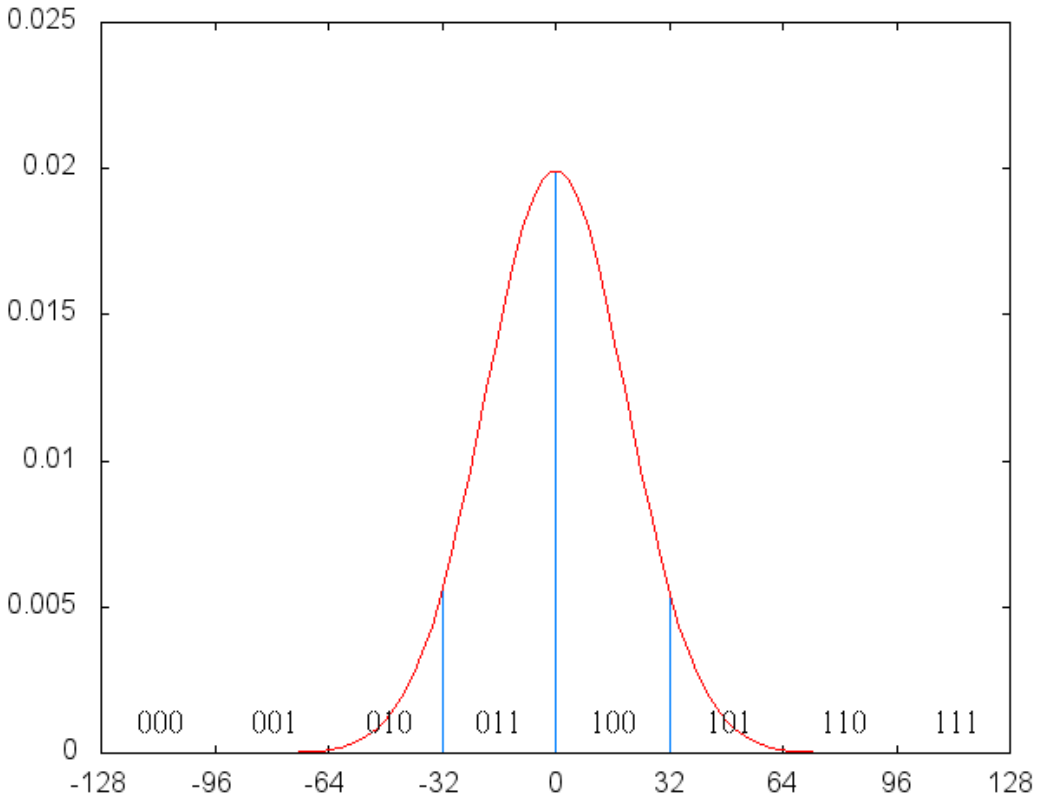

FIGURA 2.2: Associazione di una densità di probabilità gaussiana a sequenze di 3 bit

Chiaramente non si sta tenendo conto del fatto che la misura viene effettuata su una differenza di correnti ed è sporcata da vari effetti al di là della fluttuazione quantistica di X, tuttavia il contributo di questi sulla randomicità del risultato è relativamente piccolo [11].

Capitolo 3

L'apparato sperimentale

In questo capitolo si dettaglieranno la procedura sperimentale e la successiva analisi eseguite al fine di produrre numeri casuali con le tecniche di cui si è discusso finora.

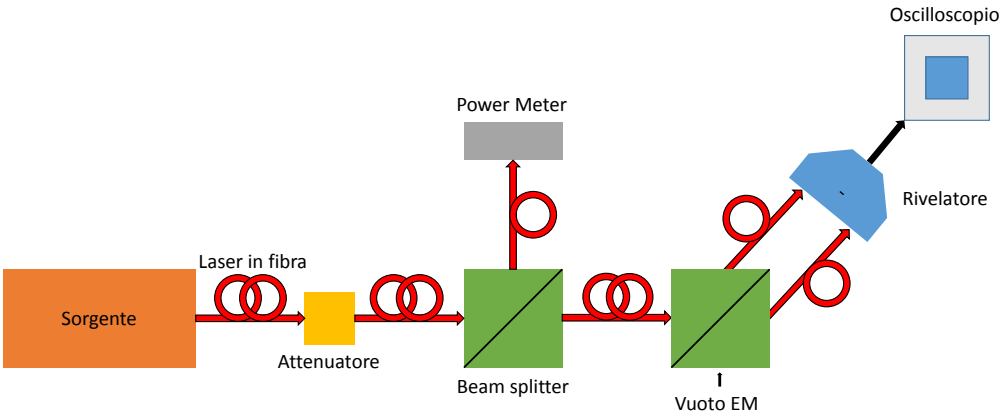

FIGURA 3.1: Schema dell'apparato

L'apparato è molto simile a quello schematizzato in figura 2.1. Una sorgente laser genera in fibra il fascio LO che viene prima attenuato e poi mixato con il segnale di vuoto elettromagnetico; le due uscite sono inviate ad un rivelatore che misura la differenza delle correnti prodotte dai suoi due fotodiodi e spedisce il segnale convertito in tensione ad un oscilloscopio a 8 bit per la sua analisi. Si noti che subito dopo l'attenuatore, il fascio viene diviso tramite un beam splitter bilanciato (50%-50%) e una delle due risultanti viene mandata ad un misuratore di potenza. In questo modo si può controllare l'intensità

emessa dalla sorgente e verificare che essa lavori nelle condizioni ottimali, inoltre si è a conoscenza di quanta potenza prosegue nel resto dell'apparato e si può essere sicuri che essa non superi i valori massimi di sopportazione dei vari componenti.

3.1 Calibrazione e misura

L'apparato funziona solo in condizioni di lavoro ben precise, che si sono ricavate nella fase iniziale dell'esperimento. Innanzitutto la sorgente laser è estremamente sensibile a variazioni di amperaggio e temperatura, e mentre il primo è facilmente controllabile, la seconda dipende anche dall'ambiente circostante e non può essere fissata con grande precisione. Si sono aggiustati tali parametri al fine di produrre un segnale il più casuale possibile, cioè privo di periodicità; queste si evidenziano come picchi in potenza della trasformata di Fourier del segnale nel dominio delle frequenze e sono quindi facilmente individuabili. Stabilizzando la temperatura a $25.95 \pm 0.05\ ^\circ C$ e con una corrente immessa dichiarata pari a 190 mA si è ottenuto il risultato voluto.

Ci si è quindi soffermati sul rivelatore, che non opera oltre un certo livello di potenza in entrata. Per visualizzare il suo comportamento si sono effettuate varie misurazioni a diversi valori di potenza e si è calcolata la varianza del segnale (si ricordi che con "segnale" si intende sempre differenza di correnti convertita in tensione).

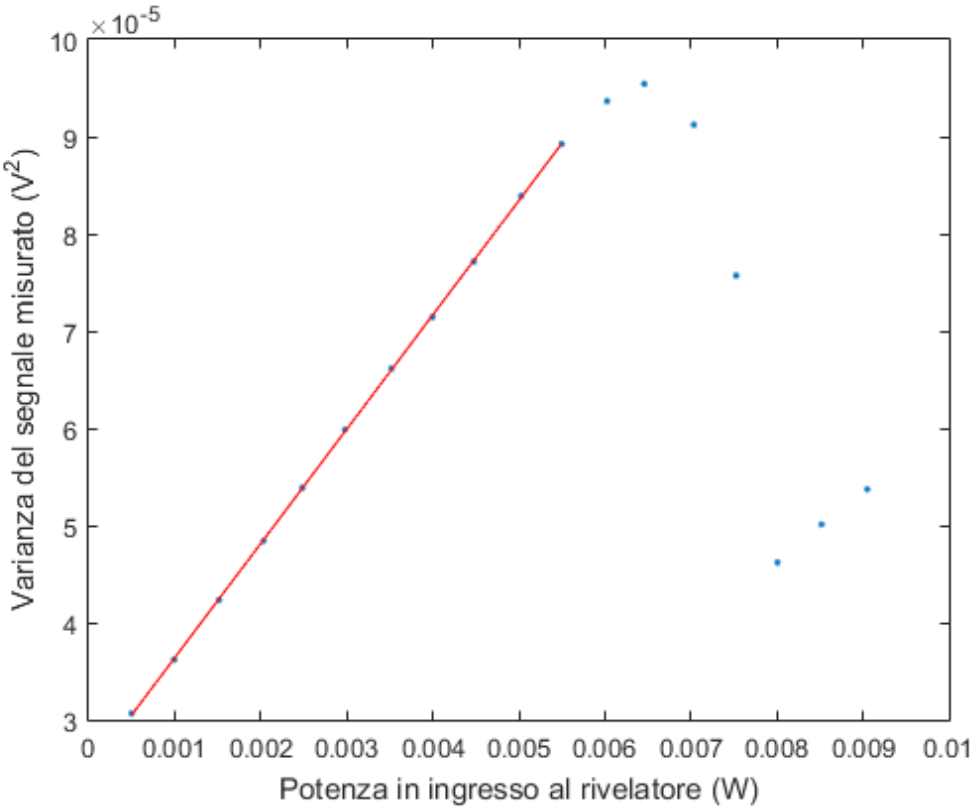

FIGURA 3.2: Curva di calibrazione

Si nota che oltre i 5.5 mW la relazione non è più lineare, il che indica una saturazione dell'apparecchio.

Una volta impostato l'apparato per fornire al rivelatore proprio 5.5 mW di potenza, si sono effettuate due ore di presa dati. Al fine di minimizzare l'autocorrelazione fra i risultati si è utilizzato un filtro digitale, in particolare si è traslata la trasformata di Fourier di 1050 MHz e si è scelto un range largo 625 MHz su cui lavorare.

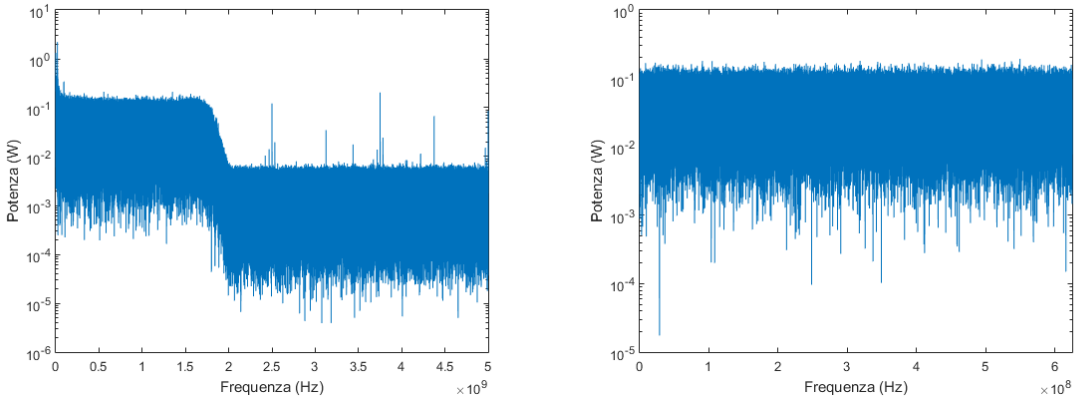

FIGURA 3.3: Lo spettro originario e il range di lavoro

Per facilitare l'applicazione di questo filtro e trovare il valore 1050 MHz, si è dovuto sovracampionare il segnale a 10 GS/s (10 miliardi di samples al secondo), e poi scartare sette misure ogni otto per scendere a 1.25 GS/s, frequenza oltre la quale il rivelatore non risponde più in maniera ottimale (come si nota dal rapido calo in potenza mostrato in Figura 3.3).

3.2 Il calcolo dell'entropia

Come discusso nella sezione 2.1, è importante trovare la massima quantità di bit veramente casuali estraibile dalla singola misura, e questo valore è fornito da H_{min} tramite il limite inferiore (2.3). Sono necessarie quindi due misure Z e X, una per generare i numeri casuali e l'altra come controllo dell'entropia. In questo caso Z e X coincidono entrambe con la quadratura del campo elettromagnetico $\frac{a+a^+}{\sqrt{2}}$ e il controllo è effettuato su un sottocampione casuale dei dati. Si noti che, come espresso in [5], visto che si fa uso di un seme per la scelta di tale sottocampione, l'intera procedura è più propriamente un'espansione indeterministica, che una generazione completamente autonoma di numeri casuali.

Per passare dalle misure di tensione a quelle di quadratura, si fa uso della relazione (2.4). Grazie ad essa si può dire che

$$\sigma_V^2 = \alpha I \sigma_X^2$$

dove σ_V^2 è la varianza della tensione, I la potenza del LO (cioè $|\beta|^2$), α un coefficiente di proporzionalità e σ_X^2 la varianza della quadratura del vuoto. A livello teorico, ponendo $\hbar = 1$ ci si aspetta $\sigma_X^2 = \frac{1}{2}$, per cui si può scrivere

$$\sigma_V^2 = \tfrac{1}{2} I \alpha$$

Ma Figura 3.2 fornisce anche

$$\sigma_V^2 = m \cdot I$$

dove m è il coefficiente angolare della retta di calibrazione. Quindi si conclude

$$\alpha = 2m$$

$$\sigma_X^2 = \frac{\sigma_V^2}{\alpha I} = \frac{\sigma_V^2}{2mI}$$

o in altre parole:

$$\delta_X = \frac{\delta_V}{\sqrt{2mI}}$$

Questa formula è utile perché c'è bisogno di δ_X per calcolare la min-entropy tramite (2.3), e perché assicura la proporzionalità fra le misure di tensione ottenute e quelle di quadratura volute.

L'ultimo passaggio è esprimere la max-entropy della misura di controllo. Essa è calcolata tramite l'estimatore Bayesiano

$$H_{max}(X) = 2\log_2\left(\frac{\Gamma(n_X+d)}{\Gamma(n_X+d+\frac{1}{2})}\sum_{x=0}^{d-1}\frac{\Gamma(n_x+\frac{3}{2})}{\Gamma(n_x+1)}\right)$$

dove Γ è la funzione di Eulero, n_X la lunghezza del sottocampione di controllo (che si è scelta pari alla radice quadrata della lunghezza totale della sequenza elaborata), n_x il numero di risultati pari a x e $d = 2^8 = 256$ il numero di possibili risultati dovuto all'ADC dell'oscilloscopio.

Utilizzando i dati specifici della misura, cioè $I = 5.47039 \pm 0.00004\, mW$, $m = 0.01176\, V^2/W^2$ e $\delta_V = 0.8\ mV$, si è trovato il valore

$$H_{min}(Z|E) = 4.0429 \pm 0.0002\ bit$$

che è ben inferiore a quello della min-entropy classica (2.1) $H_\infty(Z) = 4.826 \pm 0.001\ bit$ e soprattutto alla dimensione della singola misura, cioè 8 bit. Questa differenza si riflette anche nella varianza del campione convertito in quadratura, che invece di essere $\frac{1}{2}$ è circa 0.7.

3.3 Estrazione dei numeri casuali

L'ultimo passaggio è stata l'estrazione dei bit veri e propri. In primis si sono divise le misure per δ_V in modo da esprimerle con interi compresi fra -128 e 127 (8 bit).

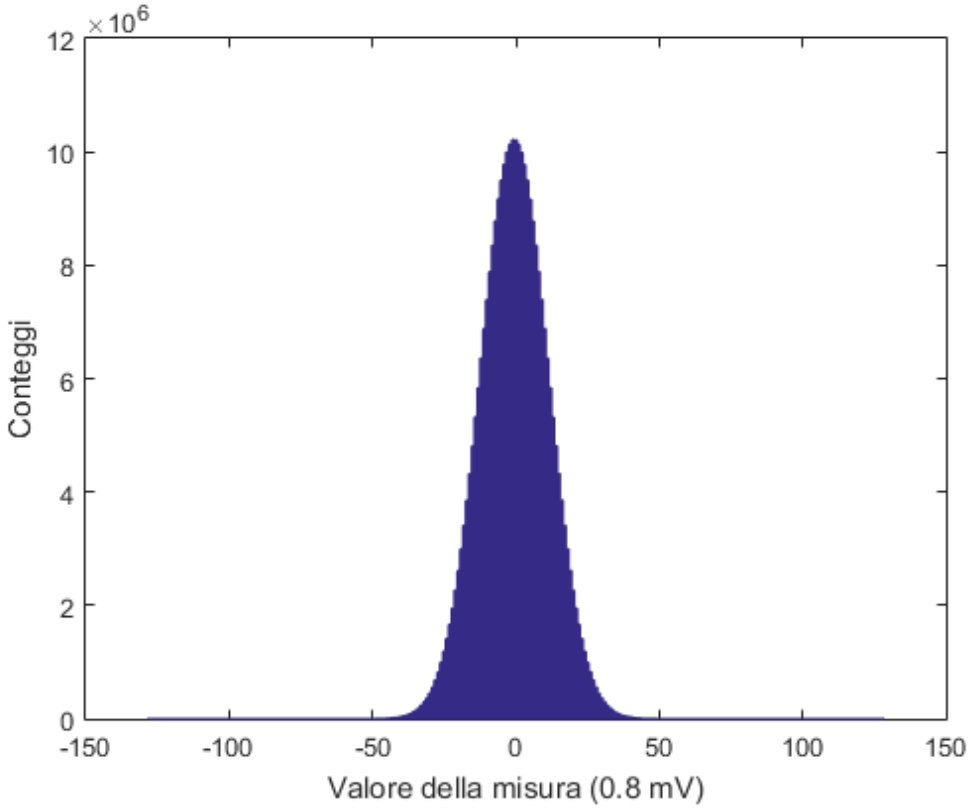

FIGURA 3.4: Istogramma delle misure espresse in 256 valori

Dopodiché si è ridotta la lunghezza della sequenza a 4.0429 *bit* per misura tramite un estrattore di randomicità, una matrice pseudo-casuale di dimensioni proporzionali a 8×4.0429, trovando il massimo di casualità vera ottenibile. Per completezza si sono sottoposti alcuni sottocampioni a test di randomicità (ent) riportando ottimi risultati (ad esempio un coefficiente di correlazione di 0.000143).

In conclusione questo esperimento ha mostrato come un fenomeno puramente quantistico, la fluttuazione del vuoto elettromagnetico, possa essere analizzato tramite una semplice misura di differenza di correnti, e come possa produrre numeri casuali di alta qualità. La sicurezza di questi è inoltre garantita dal valore di H_{min} che, a differenza della min-entropy classica H_∞, tiene conto sia delle inevitabili impurezze dello stato che di eventuali intrusioni esterne. È per tale motivo che l'estrattore è stato tarato su H_{min} e non su H_∞: anche se quest'ultima avrebbe permesso di ottenere un maggior numero di bit, essi non sarebbero stati "veramente" casuali.

Appendice A

Dettaglio sulla quantizzazione del campo EM

Questa appendice si occupa di espandere la trattazione quantistica del campo elettromagnetico introdotta in sezione 2.2 al fine di giustificare alcuni passaggi e di fornire maggior dettaglio al lettore interessato al rigore formale. L'analisi è simile a quella dell'oscillatore armonico quantistico, sia dal punto di vista dei ragionamenti eseguiti che da quello dei risultati.

L'obiettivo è studiare un sistema governato dall'hamiltoniana

$$H = \frac{\varepsilon_0}{2} \int_{L^3} \left(\|\vec{E}(\vec{r},t)\|^2 + \|c\vec{B}(\vec{r},t)\|^2 \right) d^3r \tag{A.1}$$

cioè soggetto ad un campo elettromagnetico in una regione cubica di volume L^3. Partendo dalle equazioni di Maxwell nel vuoto:

$$\vec{\nabla} \cdot \vec{E} = 0 \tag{A.2}$$

$$\vec{\nabla} \cdot \vec{B} = 0 \tag{A.3}$$

$$\vec{\nabla} \times \vec{E} = -\frac{\partial \vec{B}}{\partial t} \tag{A.4}$$

$$\vec{\nabla} \times \vec{B} = \frac{1}{c^2} \frac{\partial \vec{E}}{\partial t} \tag{A.5}$$

si derivino rispetto al tempo entrambi i membri dell'ultima equazione:

$$\vec{\nabla} \times \frac{\partial \vec{B}}{\partial t} = \frac{1}{c^2} \frac{\partial^2 \vec{E}}{\partial t^2} \Rightarrow -\vec{\nabla} \times \vec{\nabla} \times \vec{E} = \frac{1}{c^2} \frac{\partial^2 \vec{E}}{\partial t^2} \Rightarrow \nabla^2 \vec{E} - \vec{\nabla}(\vec{\nabla} \cdot \vec{E}) = \frac{1}{c^2} \frac{\partial^2 \vec{E}}{\partial t^2}$$

$$\nabla^2 \vec{E} - \frac{1}{c^2}\frac{\partial^2 \vec{E}}{\partial t^2} = 0$$

Analoghi passaggi si possono fare per B ottenendo

$$\nabla^2 \vec{B} - \frac{1}{c^2}\frac{\partial^2 \vec{B}}{\partial t^2} = 0$$

Queste sono equazioni di d'Alembert: in sostanza le equazioni di Maxwell ammettono come soluzione particolare campi elettrici e magnetici che si propagano come onde piane. Esse sono inoltre trasverse grazie a (A.2) e (A.3).

Si introducono ora i potenziali vettore e scalare $\vec{A}$ e V:

$$\vec{E} = -\nabla V - \frac{\partial A}{\partial t} \qquad\qquad \vec{B} = \vec{\nabla} \times \vec{A}$$

Questi non sono unici, infatti $\vec{E}$ e $\vec{B}$ rimangono invariati in una trasformazione di gauge del tipo

$$\vec{A} \to \vec{A}' = \vec{A} - \vec{\nabla}\Lambda \qquad\qquad V \to V' = V + \frac{\partial \Lambda}{\partial t}$$

essendo Λ una qualsiasi funzione scalare dello spazio e del tempo. Vista questa arbitrarietà dei potenziali, si può scegliere di porre $\vec{\nabla} \cdot \vec{A} = 0$; per di più in assenza di cariche si ha $V = 0$, quindi (A.5) diviene:

$$\vec{\nabla} \times \vec{\nabla} \times \vec{A} = -\tfrac{1}{c^2}\tfrac{\partial^2 \vec{A}}{\partial t^2} \Rightarrow \vec{\nabla}(\vec{\nabla} \cdot \vec{A}) - \nabla^2 \vec{A} = -\tfrac{1}{c^2}\tfrac{\partial^2 \vec{A}}{\partial t^2} \; \nabla^2 \vec{A} - \tfrac{1}{c^2}\tfrac{\partial^2 \vec{A}}{\partial t^2} = 0$$

cioè un'ulteriore equazione d'onda, questa volta per il potenziale vettore che risulta essere anch'esso un campo trasverso, sempre ortogonale al vettore d'onda $\vec{k}$.

È importante evidenziare la natura ondulatoria di $\vec{A}$, $\vec{E}$ e $\vec{B}$ per notare che ciascuna delle loro componenti di Fourier è caratterizzata da una precisa frequenza d'oscillazione e direzione di propagazione, codificate in $\vec{k}$, e da uno stato di polarizzazione.

$$\vec{F} = \sum_{\vec{k}} \vec{F}_{\vec{k}} = \sum_{\vec{k}} \sum_{s=1}^{2} \left(F_{\vec{k},s}\, \vec{u}_{\vec{k},s}\, e^{i(\vec{k}\cdot\vec{r} - \omega_{\vec{k}} t)} + F^{+}_{\vec{k},s}\, \vec{u}^{\star}_{\vec{k},s}\, e^{-i(\vec{k}\cdot\vec{r} - \omega_{\vec{k}} t)} \right) \tag{A.6}$$

in cui $\vec{u}_{\vec{k},1}$ e $\vec{u}_{\vec{k},2}$ sono due versori tali che $\vec{u}_{\vec{k},1} \perp \vec{k}$, $\vec{u}_{\vec{k},2} \perp \vec{k}$ e $\vec{u}_{\vec{k},1} \perp \vec{u}_{\vec{k},2}$, mentre $\vec{F}$ è alternativamente $\vec{A}$, $\vec{E}$ o $\vec{B}$. Le componenti sono solo due, e non tre come ci si potrebbe aspettare, perché la polarizzazione è limitata al piano ortogonale a $\vec{k}$. Ci si è spostati in un nuovo spazio in cui le equazioni di Maxwell diventano:

$$i\vec{k} \cdot \vec{E}_{\vec{k}} = 0$$

$$\vec{k} \cdot B_{\vec{k}} = 0$$

$$i\vec{k} \times \vec{E}_{\vec{k}} = -\frac{\partial \vec{B}_{\vec{k}}}{\partial t}$$

$$i\vec{k} \times \vec{B}_{\vec{k}} = \frac{1}{c^2}\frac{\partial \vec{E}_{\vec{k}}}{\partial t}$$

In assenza di cariche si ha:

$$\vec{B}_{\vec{k}} \perp \vec{k} \qquad \vec{E}_{\vec{k}} \perp \vec{k} \vec{B}_{\vec{k}} = i\vec{k} \times \vec{A}_{\vec{k}} \qquad \vec{E}_{\vec{k}} = -\frac{\partial \vec{A}_{\vec{k}}}{\partial t}$$

La trasformata dell'hamiltoniana iniziale (A.1) quindi è

$$H = \frac{\varepsilon_0 L^3}{2} \sum_k \left(\|\vec{E}_{\vec{k}}\|^2 + |c\vec{B}_{\vec{k}}\|^2 \right)$$

Ricordando che $\omega_{\vec{k}} = c|\vec{k}|$ e che $\|c\vec{B}_{\vec{k}}\|^2 = c^2\|i\vec{k} \times \vec{A}_{\vec{k}}\|^2 = \|\omega_{\vec{k}}\vec{A}_{\vec{k}}\|^2$ si può introdurre il potenziale vettore:

$$H = \frac{\varepsilon_0 L^3}{2} \sum_{\vec{k}} \left(\|\vec{E}_{\vec{k}}\|^2 + \|\omega_{\vec{k}}\vec{A}_{\vec{k}}\|^2 \right)$$

rendendo così evidente la somiglianza con l'oscillatore armonico

$$H_{OA} = \sum_{\vec{k}} \left(\frac{p_k^2}{2m} + \frac{1}{2} m\omega_{\vec{k}}^2 q_{\vec{k}}^2 \right)$$

In analogia ad esso, si possono definire gli operatori di distruzione e creazione:

$$a_{\vec{k},s} = \sqrt{\frac{\varepsilon_0 L^3}{2\hbar\omega_{\vec{k}}}} \left(\omega_{\vec{k}} A_{\vec{k},s} - iE_{\vec{k},s} \right)$$

$$a^+_{\vec{k},s} = \sqrt{\frac{\varepsilon_0 L^3}{2\hbar\omega_{\vec{k}}}} \left(\omega_{\vec{k}} A_{\vec{k},s} + iE_{\vec{k},s} \right)$$

in cui si sono scomposti i vettori nelle due componenti di polarizzazione. In accordo con (A.6) si può a questo punto dare un'espressione quantizzata dei campi $\vec{A}$, $\vec{E}$, $\vec{B}$:

$$\begin{aligned}
\vec{A}(\vec{r},t) &= \sqrt{\tfrac{\hbar}{2\varepsilon_0 L^3}} \textstyle\sum_{\vec{k}} \sum_{s=1}^{2} \frac{1}{\sqrt{\omega_{\vec{k}}}} \left(a_{\vec{k},s} \vec{u}_{\vec{k},s} e^{i(\vec{k}\cdot\vec{r}-\omega_{\vec{k}}t)} + a^+_{\vec{k},s} \vec{u}^{\star}_{\vec{k},s} e^{-i(\vec{k}\cdot\vec{r}-\omega_{\vec{k}}t)} \right) \\
\vec{E}(\vec{r},t) &= i\sqrt{\tfrac{\hbar}{2\varepsilon_0 L^3}} \textstyle\sum_{\vec{k}} \sum_{s=1}^{2} \sqrt{\omega_{\vec{k}}} \left(a_{\vec{k},s} \vec{u}_{\vec{k},s} e^{i(\vec{k}\cdot\vec{r}-\omega_{\vec{k}}t)} + a^+_{\vec{k},s} \vec{u}^{\star}_{\vec{k},s} e^{-i(\vec{k}\cdot\vec{r}-\omega_{\vec{k}}t)} \right) \\
\vec{B}(\vec{r},t) &= \tfrac{i}{c}\sqrt{\tfrac{\hbar}{2\varepsilon_0 L^3}} \textstyle\sum_{\vec{k}} \sum_{s=1}^{2} \sqrt{\omega_{\vec{k}}} \hat{k} \times \left(a_{\vec{k},s} \vec{u}_{\vec{k},s} e^{i(\vec{k}\cdot\vec{r}-\omega_{\vec{k}}t)} + a^+_{\vec{k},s} \vec{u}^{\star}_{\vec{k},s} e^{-i(\vec{k}\cdot\vec{r}-\omega_{\vec{k}}t)} \right)
\end{aligned}$$

Mentre l'hamiltoniana diventa

$$H = \sum_{\vec{k},s} H_{\vec{k},s} = \sum_{\vec{k},s} \hbar\omega_{\vec{k}} (a^+_{\vec{k},s} a_{\vec{k},s} + \frac{1}{2})$$

Generalmente si indica $N_{\vec{k},s} = a^+_{\vec{k},s} a_{\vec{k},s}$. È bene studiare meglio questi operatori. In quel che segue, per semplicità, si considera un solo modo di oscillazione e una direzione di polarizzazione fissata. Innanzitutto si noti che:

- $[a, a^+] = aa^+ - a^+a = 1$
- $[N, a] = Na - aN = a^+aa - aa^+a = (a^+a - aa^+)a = -a$
- $[N, a^+] = Na^+ - a^+N = a^+aa^+ - a^+a^+a = a^+(aa^+ - a^+a) = a^+$

Inoltre, data l'equazione agli autovalori

$$N|\varphi_n\rangle = n|\varphi_n\rangle$$

si ha che:

1. $n \geq 0$
2. $n = 0 \Rightarrow a|\varphi_n\rangle = a|\varphi_0\rangle = 0$
3. $n \neq 0 \Rightarrow a|\varphi_n\rangle \propto |\varphi_{n-1}\rangle$
4. $n \neq 0 \Rightarrow a^+|\varphi_n\rangle \propto |\varphi_{n+1}\rangle$
5. $n \in \mathbb{N}$

La dimostrazione è assai semplice:

1. $\|a\varphi_n\|^2 = \langle\varphi_n|a^+a|\varphi_n\rangle = \langle\varphi_n|n|\varphi_n\rangle = n\|\varphi_n\|^2$. Dato che $\|a\varphi_n\|^2 \geq 0$ e $\|\varphi_n\|^2 \geq 0$ allora evidentemente $n \geq 0$
2. Da 1 segue $\|a\varphi_n\|^2 = n\|\varphi_n\|^2$ per cui se $n = 0$ si ha $\|a\varphi_0\|^2 = 0$ e quindi $a\|\varphi_0\rangle = 0$
3. $Na|\varphi_n\rangle = (Na - aN + aN)|\varphi_n\rangle = ([N, a] + aN)|\varphi_n\rangle = (-a + an)|\varphi_n\rangle = (n-1)a|\varphi_n\rangle$ cioè
$$N(a|\varphi_n\rangle) = (n-1)a|\varphi_n\rangle$$
In altre parole, $a|\varphi_n\rangle$ è autostato di N corrispondente all'autovalore $n - 1$
4. $Na^+|\varphi_n\rangle = (Na^+ - a^+N + a^+N)|\varphi_n\rangle = ([N, a^+] + a^+N)|\varphi_n\rangle = (a^+ + a^+n)|\varphi_n\rangle = (n+1)a^+|\varphi_n\rangle$ cioè
$$N(a^+|\varphi_n\rangle) = (n+1)a^+|\varphi_n\rangle$$
In altre parole, $a^+|\varphi_n\rangle$ è autostato di N corrispondente all'autovalore $n + 1$

5. Se per assurdo fosse $n \notin \mathbb{N}$, sia allora $i \in \mathbb{N}$ la parte intera di n. Lo stato $a^i|\varphi_n\rangle$ è autostato di N corrispondente all'autovalore $n - i \in (0, 1)$. Quindi applicando un'ultima volta l'operatore di distruzione si ottiene un autostato corrispondente all'autovalore $n - i - 1 \in (-1, 0)$, da cui la contraddizione con 1.

Tornando al problema del campo elettromagnetico, e reintroducendo i pedici $\vec{k}, s$, si può affermare che

$$H_{\vec{k},s}|\varphi_{n_{\vec{k},s}}\rangle = \hbar\omega_{\vec{k}}(N_{\vec{k},s} + \frac{1}{2})|\varphi_{n_{\vec{k},s}}\rangle = \hbar\omega_{\vec{k}}(n_{\vec{k},s} + \frac{1}{2})|\varphi_{n_{\vec{k},s}}\rangle$$

Gli autostati di $H_{\vec{k},s}$ sono quindi gli stessi di $N_{\vec{k},s}$ e corrispondono ad autovalori del tipo $\hbar\omega_{\vec{k}}(n_{\vec{k},s} + \frac{1}{2})$. Nel caso dell'oscillatore armonico $n_{\vec{k},s}$=0 ,1,2... è un contatore del livello energetico, qui invece indica il numero di fotoni di vettore d'onda $\vec{k}$ e di polarizzazione s. $a^+_{\vec{k},s}$ e $a_{\vec{k},s}$ agiscono facendo crescere o diminuire tale valore secondo le leggi

$$a^+_{\vec{k},s}|\varphi_{n_{\vec{k},s}}\rangle = \sqrt{n_{\vec{k},s} + 1}|\varphi_{n_{\vec{k},s}+1}\rangle \qquad a_{\vec{k},s}|\varphi_{n_{\vec{k},s}}\rangle = \sqrt{n_{\vec{k},s}}|\varphi_{n_{\vec{k},s}-1}\rangle$$

Si possono infine definire le quadrature

$$X_{\vec{k},s} = \frac{a_{\vec{k},s} + a^+_{\vec{k},s}}{\sqrt{2}} \qquad P_{\vec{k},s} = \frac{a^+_{\vec{k},s} - a_{\vec{k},s}}{\sqrt{2}} \qquad X_{\vec{k},s}(\theta) = \frac{a_{\vec{k},s} + e^{i\theta}a^+_{\vec{k},s}}{\sqrt{2}}$$

Si passa ora ad un rapido studio di alcuni particolari stati del campo elettromagnetico.

1. Gli autostati dell'operatore a sono detti stati coerenti e hanno la forma

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_n \frac{\alpha^n}{\sqrt{n!}}|\varphi_n\rangle$$

   in cui α è in generale complesso, non essendo a un operatore hermitiano. Valgono le relazioni:

   (a) $a|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_n \frac{\alpha^n}{\sqrt{n!}}\sqrt{n}|\varphi_{n-1}\rangle = \alpha e^{-\frac{|\alpha|^2}{2}} \sum_{n-1} \frac{\alpha^{n-1}}{\sqrt{(n-1)!}}|\varphi_{n-1}\rangle = \alpha|\alpha\rangle$

   (b) $\langle\alpha|a|\alpha\rangle = \alpha$

   (c) $\langle\alpha|a^+|\alpha\rangle = e^{-|\alpha|^2} \sum_n \frac{(|\alpha|^2)^{n+1}(n+1)}{\alpha(n+1)!}\langle\alpha|\alpha\rangle = \alpha^\star e^{-|\alpha|^2} \sum_n \frac{|\alpha|^{2n}}{n!} = \alpha^\star e^{-|\alpha|^2} e^{|\alpha|^2} = \alpha^\star$

2. L'autostato $|\varphi_0\rangle$ di H è detto stato di vuoto. In rappresentazione in coordinate di X la sua funzione d'onda $\varphi_0(X)$ e la densità di probabilità $|\varphi_0(X)|^2$ sono entrambe gaussiane centrate in 0 e la seconda ha deviazione standard pari alla fluttuazione di X nello stato. Infatti

$$a|\varphi_0(X)\rangle = 0 \Rightarrow (\tfrac{d}{dX} + X)\varphi_0(X) = 0 \Rightarrow \varphi_0(X) = e^{-\frac{X^2}{2}}$$

$$|\varphi_0(X)|^2 = e^{-x^2} \Rightarrow \sigma^2_{PDF} = \tfrac{1}{2}$$

$$(\Delta X)^2 = \langle\varphi_0|X^2|\varphi_0\rangle - (\langle\varphi_0|X|\varphi_0\rangle)^2 = \tfrac{1}{2} - 0 = \tfrac{1}{2} \Rightarrow (\Delta X)^2 = \sigma^2_{PDF}$$

Appendice B

Dettaglio delle relazioni utili alla tecnica di rivelazione omodina

In questa appendice è presentato il dettaglio dei conti relativi all'apparato di rivelazione omodina della sezione 2.3.

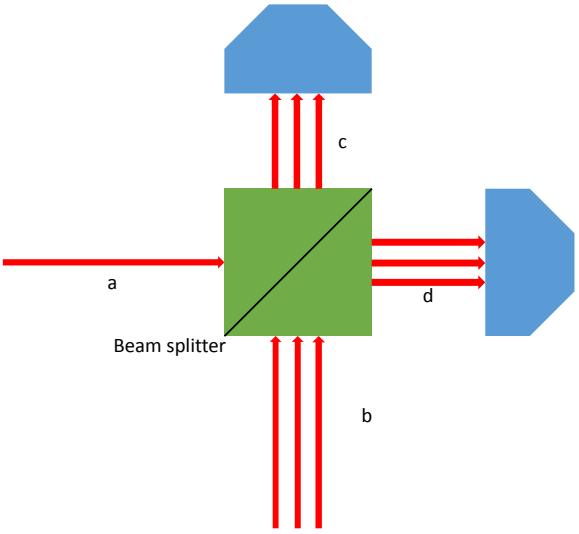

FIGURA B.1: Schema di un apparato per rivelazione omodina

In accordo con le notazioni precedentemente usate, si indicano con a, b, c, d gli operatori di distruzione rispettivamente dei sistemi ϱ (segnale), LO (oscillatore locale), e raggi in entrata ai fotodiodi indicati in figura con c e d. Si è interessati alla grandezza $N_- = N_c - N_d$, cioè alla differenza nei numeri di fotoni contati dai due rivelatori, che può essere misurata come differenza di correnti.

Per prima cosa si nota che valgono le relazioni

$$c = \frac{b + ia}{\sqrt{2}} \qquad d = \frac{a + ib}{\sqrt{2}} \qquad c^+ = \frac{b^+ - ia^+}{\sqrt{2}} \qquad d^+ = \frac{a^+ - ib^+}{\sqrt{2}}$$

Per cui si può scivere

$$N_- = N_c - N_d = c^+c - d^+d = \tfrac{(b^+ - ia^+)(b+ia)}{2} - \tfrac{(a^+ - ib^+)(a+ib)}{2} = iab^+ - ia^+b$$

(si tenga conto del fatto che operatori relativi a ϱ e LO commutano fra loro). A questo punto si vogliono valutare valor medio e fluttuazione di N_- su uno stato in ingresso $\varrho \bigotimes \beta$ essendo β uno stato coerente (cioè autovettore di b) di fase relativa ϕ rispetto a ϱ, cioè $\beta = |\beta|e^{i\varphi}$.

$$\langle \varrho \bigotimes \beta | N_- | \varrho \bigotimes \beta \rangle = i\Big(\langle \varrho|a|\varrho\rangle \cdot \langle\beta|b^+|\beta\rangle - \langle\varrho|a^+|\varrho\rangle \cdot \langle\beta|b|\beta\rangle\Big) = i\Big(\beta^\star \langle a\rangle_\varrho - \beta\langle a^+\rangle_\varrho\Big) =$$
$$i|\beta|\langle e^{-i\phi}a - e^{i\phi}a^+\rangle_\varrho = ie^{-i\phi}|\beta|\langle a - e^{i2\phi}a^+\rangle_\varrho = \sqrt{2}|\beta|e^{i(\frac{\pi}{2}-\phi)}\Big\langle \frac{a + e^{i(2\phi-\pi)}a^+}{\sqrt{2}}\Big\rangle_\varrho \quad \text{(B.1)}$$

Riprendendo la definizione di $X(\theta)$ cioè $X(\theta) := \frac{a+e^{i\theta}a^+}{\sqrt{2}}$, allora $N := \sqrt{2}|\beta|e^{i(\frac{\pi}{2}-\phi)}X(2\phi - \pi)$ ed N_- hanno lo stesso valor medio:

$$\langle N_-\rangle_{\varrho\bigotimes\beta} = \langle N'\rangle_{\varrho\bigotimes\beta}$$

Per trovare la fluttuazione si sfrutta il fatto che $(\Delta N_-)^2 = \langle N_-^2\rangle - \langle N_-\rangle^2$, e che

$$\langle N_-^2\rangle = \langle -i(a^+b - ab^+)i(ab^+ - a^+b)\rangle = \langle a^+abb^+\rangle - \langle a^+a^+bb\rangle - \langle aab^+b^+\rangle + \langle aa^+b^+b\rangle \quad \text{(B.2)}$$

Calcolando i quattro valori medi uno a uno si ha:

- $\langle a^+abb^+\rangle = \langle a^+a\rangle_\varrho \cdot \langle\beta|bb^+|\beta\rangle = \langle a^+a\rangle_\varrho \cdot \langle\beta|1 + b^+b|\beta\rangle = \langle a^+a\rangle_\varrho \cdot (1 + \beta\langle\beta|b^+|\beta\rangle) = \langle a^+a\rangle_\varrho \cdot (1 + |\beta|^2)$
- $\langle a^+a^+bb\rangle = \langle a^+a^+\rangle_\varrho \cdot \langle\beta|bb|\beta\rangle = \langle a^+a^+\rangle_\varrho \cdot \beta^2$
- $\langle aab^+b^+\rangle = \langle aa\rangle_\varrho \cdot \langle\beta|b^+b^+|\beta\rangle = \langle aa\rangle_\varrho \cdot \beta^{\star 2}$
- $\langle aa^+b^+b\rangle = \langle aa^+\rangle_\varrho \cdot \langle\beta|b^+b|\beta\rangle = \langle aa^+\rangle_\varrho \cdot |\beta|^2 = (1 + \langle a^+a\rangle_\varrho) \cdot |\beta|^2$

In cui si è usata numerose volte la relazione di commutazione $[a, a^+] = 1 \Rightarrow aa^+ = 1 - a^+a$.

Inserendo queste nella (B.2) si trova:

$$\langle N_-^2\rangle_{\varrho\bigotimes\beta} = \langle a^+a\rangle_\varrho \cdot (1+|\beta|^2) - \langle a^+a^+\rangle_\varrho \cdot \beta^2 - \langle aa\rangle_\varrho \cdot \beta^{\star 2} + (1+\langle a^+a\rangle_\varrho)\cdot|\beta|^2 = \langle a^+a\rangle_\varrho \cdot (1+2|\beta|^2) + |\beta|^2 - \langle a^+a^+\rangle_\varrho \cdot \beta^2 - \langle aa\rangle_\varrho \cdot \beta^{\star 2} = \langle a^+a\rangle_\varrho + |\beta|^2\Big(1+2\langle a^+a\rangle_\varrho - e^{2i\phi}\langle a^+a^+\rangle_\varrho - e^{-2i\phi}\langle aa\rangle_\varrho\Big)$$

E quindi

$$(\Delta N_-)^2_{\varrho\bigotimes\beta} = \langle a^+a\rangle_\varrho + |\beta|^2\Big(1+2\langle a^+a\rangle_\varrho - e^{2i\phi}\langle a^+a^+\rangle_\varrho - e^{-2i\phi}\langle aa\rangle_\varrho\Big) - \left(\sqrt{2}|\beta|e^{i(\frac{\pi}{2}-\phi)}\left\langle \tfrac{a+e^{i(2\phi-\pi)}a^+}{\sqrt{2}}\right\rangle\right)^2$$

Ricordando da (B.1) che la somiglianza con $X(\theta)$ si ha per $\theta = 2\phi - \pi$ si può scrivere

$$(\Delta N_-)^2_{\varrho\bigotimes\beta} = \langle a^+a\rangle_\varrho + |\beta|^2\Big(1+2\langle a^+a\rangle_\varrho - e^{2i\phi}\langle a^+a^+\rangle_\varrho - e^{-2i\phi}\langle aa\rangle_\varrho\Big) + 2|\beta|^2 e^{-2i\phi}\langle X(2\phi-\pi)\rangle_\varrho \tag{B.3}$$

Utilizzando lo stesso tipo di ragionamento si può trovare la fluttuazione di $X(2\phi-\pi)$

$$(\Delta X(2\phi-\pi))^2 = \frac{1}{2}\Big(1+2\langle a^+a\rangle_\varrho - e^{2i\phi}\langle a^+a^+\rangle_\varrho - e^{-2i\phi}\langle aa\rangle_\varrho\Big) - \langle X(2\phi-\pi)\rangle^2$$

Quindi

$$(\Delta N')^2_{\varrho\bigotimes\beta} = 2|\beta|^2\cdot\frac{1}{2}\Big(1+2\langle a^+a\rangle_\varrho - e^{2i\phi}\langle a^+a^+\rangle_\varrho - e^{-2i\phi}\langle aa\rangle_\varrho\Big) + 2|\beta|^2 e^{-2i\phi}\langle X(2\phi-\pi)\rangle \tag{B.4}$$

Confrontando (B.3) e (B.4) si nota che

$$(\Delta N_-)^2_{\varrho\bigotimes\beta} = (\Delta N')^2_{\varrho\bigotimes\beta} + \langle a^+a\rangle_\varrho$$

Tuttavia, come già detto nella sezione 2.3, il termine $\langle a^+a\rangle_\varrho$ risulta trascurabile nel limite $\beta\to\infty$ nonché addirittura 0 se ϱ è lo stato di vuoto elettromagnetico.

Bibliografia

[1] D. J. Bennett. Oder in apparent chaos. In *Randomness*, chapter 7. Harvard University Press, 1999.

[2] D. J. Bennett. Wanted: Random numbers. In *Randomness*, chapter 8. Harvard University Press, 1999.

[3] D. J. Bennett. Chance or necessity? In *Randomness*, chapter 6. Harvard University Press, 1999.

[4] Aaldert Compagner. Definitions of randomness. *American Journal of Physics*, 59(8):700–705, 1991. doi: http://dx.doi.org/10.1119/1.16747. URL http://scitation.aip.org/content/aapt/journal/ajp/59/8/10.1119/1.16747.

[5] Giuseppe Vallone, Davide G. Marangon, Marco Tomasin, and Paolo Villoresi. Quantum randomness certified by the uncertainty principle. *Phys. Rev. A*, 90:052327, Nov 2014. doi: 10.1103/PhysRevA.90.052327. URL http://link.aps.org/doi/10.1103/PhysRevA.90.052327.

[6] Rosario Gennaro. An improved pseudo-random generator based on discrete log. In *Journal of Cryptology*, pages 469–481. Springer, 2000. URL http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.104.4843.

[7] M. Stipcevic. Quantum random number generators and their use in cryptography. In *MIPRO, 2011 Proceedings of the 34th International Convention*, pages 1474–1479, May 2011. URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5967293.

[8] C.E. Shannon. A mathematical theory of communication. *Bell System Technical Journal, The*, 27(3):379–423, July 1948. ISSN 0005-8580. doi: 10.1002/j.1538-7305.1948.tb01338.x. URL http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6773024.

[9] R. Konig, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *Information Theory, IEEE Transactions on*, 55(9):4337–4347, Sept 2009.

ISSN 0018-9448. doi: 10.1109/TIT.2009.2025545. URL http://arxiv.org/abs/0807.1338.

[10] Fabian Furrer, Mario Berta, Marco Tomamichel, Volkher B. Scholz, and Matthias Christandl. Position-momentum uncertainty relations in the presence of quantum memory. *Journal of Mathematical Physics*, 55(12), 2014. ISSN 0022-2488. doi: 10.1063/1.4903989. URL http://arxiv.org/abs/1308.4527.

[11] Horace P. Yuen and Vincent W. S. Chan. Noise in homodyne and heterodyne detection. *Opt. Lett.*, 8(3):177–179, Mar 1983. doi: 10.1364/OL.8.000177. URL http://ol.osa.org/abstract.cfm?URI=ol-8-3-177.