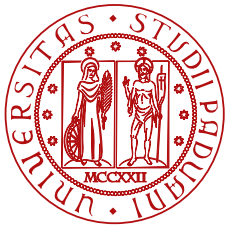

Università degli Studi di Padova

Dipartimento di Ingegneria dell'Informazione

Laurea Triennale in Ingegneria Informatica

Studio e caratterizzazione di un generatore quantistico di numeri casuali

Candidata:

Lisa Lando

Matricola: 1216407

Relatore:

Prof. Giuseppe Vallone

Correlatori:

Dr. Tommaso Bertapelle

Dr. Marco Avesani

Anno Accademico
2021/2022

Nella teoria della relatività non esiste un unico tempo assoluto,
ma ogni singolo individuo ha una propria personale misura del tempo,
che dipende da dove si trova e da come si sta muovendo.
Stephen Hawking

Abstract

A Random Number Generator is a device capable of producing random numbers, which are a fundamental element of cyber-security because they guarantee security in many applications. The generator that satisfies the hypothesis of true randomness is the Quantum Random Number Generator which, as its name suggests, uses Quantum Mechanics to generate random numbers. In practical terms, there are many caveats to be considered in the realisation of these devices: the generator only works correctly if the assumptions made in the respective theoretical model are fulfilled.

This work aims to present the study and characterisation of a continuous variable homodyne-based QRNG. These schemes make use of commercial components (COTS) for reduced implementation costs, and 1550 nm optical components.

Sommario

Un Random Number Generator è un dispositivo in grado di produrre numeri casuali, i quali sono un elemento fondamentale della cyber-security perché garantiscono la sicurezza in molte applicazioni. Il generatore che soddisfa lipotesi della vera randomicità è il Quantum Random Number Generator che, come suggerisce il nome, utilizza la Meccanica Quantistica per generare numeri casuali. Nella praticità, ci sono molti accorgimenti da prendere in considerazione per la realizzazione di questi dispositivi: il generatore funziona correttamente solo se vengono rispettate delle ipotesi formulate nel rispettivo modello teorico.

Questo lavoro vuole presentare lo studio e la caratterizzazione di un QRNG a variabili continue di tipo omodina. Questi schemi sfruttano componenti commerciali (COTS) per una riduzione dei costi di realizzazione, e componenti ottici a 1550 nm.

Contenuti

Lista delle figure

1

Introduzione ai QRNG

I numeri casuali sono un elemento principale in molte applicazioni, come simulazioni di fenomeni fisici, finanza e *cyber-securety*, che rappresenta il campo principale in cui questo tipo di numeri è utilizzato.

I RNG (*Random Number Generator*) sono, come suggerisce il nome stesso, sistemi in grado di generare numeri casuali. Tuttavia, la maggior parte di questi sono predicibili [5] in quanto basati su algoritmi (PRNG, *Pseudo RNG*) o fenomeni fisici classici (TRNG, *True RNG*) che essendo deterministici generano sequenze di numeri aventi proprietà statistiche molto simili a quelle dei numeri casuali. Nel caso dei PRNG, la casualità non è garantita perchè gli algoritmi da essi utilizzati si basano sull'espansione di un valore di inizializzazione, detto seme, da cui si genera una sequenza di numeri che si ripeterà periodicamente i cui elementi potrebbero essere correlati tra loro.

I QRNG (*Quantum Random Number Generator*) utilizzano la teoria della Meccanica Quantistica, intrinsecamente probabilistica e quindi generano numeri casuali risolvendo il problema della pseudo casualità [11]. Nonostante ciò, possono esserci delle vulnerabilità, come la non idealità nella realizzazzione della sorgente quantistica e dell'apparato di misura del QRNG, che andrebbe a interferire con la causalità pura dei numeri.

I generatori quantistici di numeri casuali sono formati principalmente da due parti: una sorgente di casualità e un sistema di misura. Questo tipo di generatore può essere collocato in tre diverse categorie a seconda del livello di fiducia attribuito alle due parti: *trusted-device*, *device-independent* e *semi-device-*

independent QRNG [11]. Si ricorda che il livello di fiducia attribuita alla sorgente o al sistema di misura dipende dai dispositivi utilizzati per costruire il generatore e dal fenomeno quantistico utilizzato per la generazione dei numeri.

I *trusted-device* QRNG sono i dispositivi solitamente più semplici e con più elevate prestazioni, i quali si basano sulla completa fiducia dei loro componenti, data dalla costruzione di un modello teorico ben definito e preciso in cui tutte le ipotesi devono essere soddisfatte: quest'ultimo fornisce un limite all'entropia, che indica il livello di incertezza intrinseca di uno stato quantistico.

In una delle possibili implementazioni del *trusted-device* QRNG, un singolo fotone alla volta [11], va ad incidere in uno specchio semiriflettente (un *beam splitter* 50:50), il quale rifletterà o trasmetterà il fotone con il 50% di probabilità. È fondamentale che le due probabilità siano uguali essendo un'ipotesi del *trusted-device* QRNG, altrimenti la casualità verrebbe compromessa e i numeri generati considerati non sicuri.

I *device-independent* QRNG implementano la situazione opposta ai *trusted-device* QRNG e in particolare non ci si fida nè della sorgente, nè del sistema di misura. Ciò significa che la casualità del risultato è totalmente indipendente dalla realizzazione del sistema [11]. Questo tipo di QRNG si basa sulla violazione della disuguaglianza di Bell: per questo motivo sono molto difficili da realizzare perché richiedono un'implementazione *loop-hole free* della disuguaglianza [11], [16], [14].

I semi-device-independent QRNG sono una categoria intermedia tra *trusted* e *device-independent* QRNG in termini di velocità di generazione dei numeri e della loro sicurezza.

In questo tipo di generatore, entrambe le parti possono essere caratterizzate da un modello teorico, ma ciò che lo differenzia dagli altri QRNG è il fatto che le ipotesi da rispettare sono rese meno stringenti. È importante precisare che ci sono *semi-device-independent* QRNG in cui solo una delle due parti è ben caratterizzata: si parla quindi di *source-independent* [3] o *measurement-device-independent* [11] QRNG quando a non essere caratterizzati sono rispettivamente la sorgente di casualità e il sistema di misura.

L'output di un QRNG è una stringa indipendente di bit non correlati con distribuzione di probabilità uniforme. Si precisa che per indipendente si intende che non ci sono legami tra stringhe di numeri diverse generate in precedenza, o tra quelle che potrebbero essere associate da un eventuale attaccante.

In generale, mediante delle tecniche di *post-processing*, è possibile ottenere una stringa di numeri con le proprietà sopra riportate. Le procedure più comuni si basano su tecniche di hashing di tipo 2-universal [17]. L'implementazione più comune sfrutta la moltiplicazione modulo 2 di una matrice di binaria casuale con un sotto-blocco della stringa grezza. La matrice grezza può anche avere una struttura di tipo Toeplitz [2] senza compromettere le proprietà di indipendenza cercate. È possibile eseguire dei test per valutare a posteriori la qualità della casualità generata, ricercando modelli e correlazioni nei dati in uscita [9].

La suite test più comune comprende 16 tests ed è redatta dal NIST (National Institute of Standards and Technology): essa va a testare la randomicità di sequenze arbitrariamente lunghe prodotte dal generatore quantistico [15], le quali sono raccolte in un file binario generato dopo aver scelto il punto di lavoro migliore del dispositivo attraverso una calibrazione.

È importante specificare che la suite test redatta dal NIST è stata ideata principalmente per i PRNG, e per tradizione si effettuano i test anche sui QRNG per avere una certificazione formale della randomicità.

Il risultato dei test su un generatore quantistico di numeri casuali non certifica la casualità dei numeri, presente a priori, ma può essere uno spunto per capire se il dispositivo è stato implementato nel modo corretto: per esempio, se un determinato test fallisce ripetutamente è opportuno rivedere come sono state implementate le ipotesi, lo stato dei vari dispositivi, etc.

In questo lavoro il generatore quantistico di numeri casuali è di tipo *trusted*, costruito con componenti di tipo COTS ed implementazione di tipo omodina per la misurazione di una delle quadrature del campo elettromagnetico.

Il QRNG sfrutta osservabili a variabili continue perché la quantizzazione del campo elettromagnetico e la misurazione delle sue quadrature hanno bisogno di uno spazio di Hilbert di dimensione infinita [10].

Infine, l'acronimo COTS riporta alle parole Commercial-Off-the-Shelf, e si riferisce ai componenti hardware disponibili sul mercato per l'acquisto da parte di aziende interessate allo sviluppo dei propri progetti. Ciò significa che i componenti sono prodotti in serie e i costi da sostenere, sia per l'acquisto che per la manutenzione, non sono troppo elevati.

Ciò che in generale si cerca di ottenere è una veloce generazione di numeri casuali con il minor sforzo possibile, sia economico che computazionale, e con

un alto livello di velocità e casualità. Un rate di generazione elevato è garantito dallo schema a variabili continue (CV) basato sulla misura di osservabili in quadratura del campo elettromagnetico [13].

2

Gli assiomi della Meccanica Quantistica

Un generatore quantistico di numeri casuali utilizza le leggi della Meccanica Quantistica come fonte di casualità. È opportuno perciò descriverne i concetti fondamentali e le leggi che la governano: di seguito sono elencati i principali assiomi della Meccanica Quantistica, che faranno da base alla spiegazione teorica dei sistemi utilizzati in questo lavoro.

2.1 Stati nello spazio di Hilbert

Ad ogni sistema fisico è associato uno spazio di Hilbert, il quale è uno spazio vettoriale separabile nel campo dei numeri complessi dotato di un prodotto scalare interno. Un sistema fisico corrisponde nello spazio di Hilbert ad un raggio vettore, un vettore normalizzato $|\psi\rangle$ avente norma unitaria.

Lo stato rappresentato dal vettore $|\psi\rangle$ appare in due diverse configurazioni: lo stesso $|\psi\rangle$ è detto "ket "ed equivale ad un vettore colonna, mentre $\langle\psi|$ è detto "bra "ed equivale ad un vettore riga i cui elementi sono i complessi coniugati di quelli di $|\psi\rangle$: questa di configurazione fa parte della notazione Braket.

Questo vettore rappresenta uno stato puro, il quale contiene al suo interno la massima quantità di informazione sul sistema fisico. La norma di un vettore appartenente allo spazio di Hilbert è data dal prodotto scalare interno, il quale ha questa forma:

$$\langle\psi|\psi\rangle = 1 \tag{2.1}$$

Il sistema può anche assumere diversi stati distinti, i quali sono combinati linearmente secondo il principio di sovrapposizione:

$$|\psi\rangle = \alpha \cdot |\psi_1\rangle + \beta \cdot |\psi_2\rangle \tag{2.2}$$

in cui $|\alpha|^2 + |\beta|^2 = 1$ ($|\alpha|^2$ e $|\beta|^2$ sono le probabilità che lo stato $|\psi\rangle$ sia rispettivamente $|\psi_1\rangle$ e $|\psi_2\rangle$). Si noti che α e β sono due numeri complessi.

È importante puntualizzare che uno stato quantistico può trovarsi anche in un'altra configurazione: uno stato quantistico si definisce misto se l'informazione disponibile del sistema non è massima. Ciò significa che lo stato effettivo del sistema è preso dall'insieme $|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_N\rangle$ con probabilità $p_1, p_2, ..., p_N$, le quali soddisfano la condizione di unità [18].

2.2 Evoluzione di uno stato quantistico

Un sistema quantistico evolve nel tempo, e per capire come questo accade nella Meccanica Quantistica è fondamentale introdurre il concetto di operatore. Si definisce l'operatore A come una funzione lineare dello spazio vettoriale V di Hilbert tale che $A : \mathbb{V} \to \mathbb{V}$.

Formalmente, l'evoluzione nel tempo dello stato di un sistema quantistico è descritta dall'equazione di Shrödinger [18]:

$$i\hbar \frac{\mathrm{d}}{\mathrm{d}t} |\psi(t)\rangle = \hat{H(t)} |\psi(t)\rangle \tag{2.3}$$

in cui $\hat{H(t)}$ è un operatore Hermitiano, per cui vale per definizione $\hat{H} = \hat{H^\dagger}$.
Inoltre, $\hat{H(t)}$ è l'Hamiltoniana del sistema, che in Meccanica Classica è definita come la funzione che descrive lo stato dell'energia totale del sistema, la quale comprende l'energia cinetica e potenziale [8].

Lo spettro dell'Hamiltoniana rappresenta l'insieme dei possibili risultati di una misura del livello energetico del sistema.

2.3 Operatore di densità

Gli stati quantistici possono essere descritti attraverso l'operatore di densità. Nel caso di uno stato misto, esso descrive una mistura statistica di più stati [18]:

$$\hat{\rho} = \sum_i p_i \left|\psi_i\right\rangle\!\left\langle\psi_i\right| \tag{2.4}$$

Se invece si considera uno stato quantistico puro, esiste un unico $\left|\psi_i\right\rangle$ che lo descrive, e che quindi ha probabilità unitaria. In questo caso l'espressione dell'operatore di densità è la seguente:

$$\hat{\rho} = \left|\psi\right\rangle\!\left\langle\psi\right| \tag{2.5}$$

Senza fare distinzioni dal tipo di stato quantistico considerato, esso soddisfa le seguenti proprietà:

- È un operatore Hermitiano;
- Ha traccia unitaria;
- È un operatore non negativo (i suoi autovalori sono sempre positivi). Ciò significa che per ogni stato $\left|\psi\right\rangle$ appartenente allo spazio di Hilbert $\mathcal{H}$ si ha che $\left\langle\psi\right|\hat{\rho}\left|\psi\right\rangle \geq 0$.

L'operatore di densità può descrivere anche uno stato quantistico puro se e solo se $\hat{\rho}^2 = \hat{\rho}$. Se lo stato rappresentato dall'operatore di densità è misto, allora $\mathrm{Tr}(\hat{\rho}^2) < 1$ [18].

2.4 Osservabile

Un osservabile è una quantità fisica misurabile ed è rappresentato da un operatore Hermitiano che agisce sullo spazio di Hilbert.

Il risultato di una misurazione di un osservabile corrisponde ad un autovalore a_n [18] dello stesso ed è perciò un numero reale: l'insieme di tutti gli autovalori relativi ad un osservabile $\hat{A}$ è chiamato spettro di $\hat{A}$.

Nel caso degli stati puri con spettro discreto, ogni stato può essere considerato, come detto in precedenza, una combinazione lineare di altri stati: considerando i vettori di una base ortonormale di uno spazio di Hilbert $\{\left|u_n^i\right\rangle\}$, il generico stato $\left|\psi\right\rangle$ può essere scritto come:

$$\left|\psi\right\rangle = \sum_n c_n \left|u_n\right\rangle \tag{2.6}$$

in cui la probabilità di ottenere l'autovalore a_n misurando l'osservabile è:

$$P(a_n) = |c_n|^2 = |\left\langle u_n|\psi\right\rangle|^2 \tag{2.7}$$

Nel caso di uno spettro continuo, invece, lo stato $\left|\psi\right\rangle$ e la probabilità di ottenere un valore tra a e $a + da$, dPa [18], sono rispettivamente:

$$\left|\psi\right\rangle = \int c(a) \left|w_a\right\rangle \mathrm{d}a \tag{2.8}$$

$$P(a_n) = |c_a|^2 \mathrm{d}a = |\left\langle w_a|\psi\right\rangle|^2 \mathrm{d}a \tag{2.9}$$

Inoltre, se si è in presenza di uno spettro discreto, un osservabile Hermitiano $\hat{A}$ [18] può essere scritto in questo modo:

$$\hat{A} = \sum_n a_n \hat{P}_n \tag{2.10}$$

dove a_n è un autovalore e $\hat{P_n}$ è un proiettore [18], il quale, dato uno stato $\left|\psi\right\rangle$ che appartiene ad uno spazio di Hilbert H, è l'operatore $\left|\psi\right\rangle\left\langle\psi\right|$. Esso soddisfa le due seguenti proprietà:

- $\hat{P}^2 = \hat{P}$;
- $\hat{P}^\dagger = \hat{P}$.

Dopo la misurazione dell'osservabile, la quale porta ad un risultato r_n, lo stato puro $\left|\psi\right\rangle$ del sistema quantistico collassa in $\left|\psi'\right\rangle$ [18]:

$$\left|\psi'\right\rangle = \frac{\hat{P_n}\left|\psi\right\rangle}{\sqrt{\left\langle\psi|\hat{P_n}|\psi\right\rangle}} \tag{2.11}$$

Questo nuovo stato è la proiezione normalizzata di $\left|\psi\right\rangle$ nell'autospazio relativo all'autovalore proveniente dalla misurazione r_n [8]. $\left|\psi'\right\rangle$ prende il nome di autostato.

Per quanto riguarda gli stati misti, si può dimostrare che la probabilità di ottenere l'autovalore a_n misurando l'osservabile [18] è:

$$P(a_n) = \mathrm{Tr}(\hat{\rho}\hat{P}_n) \tag{2.12}$$

È possibile parlare di collasso dello stato anche per quanto riguarda gli stati misti: è un discorso analogo a quello fatto in precedenza, ma ciò che va a modificarsi è l'operatore di densità. Dopo la misura dell'osservabile quest'ultimo sarà dato da:

$$\hat{\rho}' = \frac{\hat{P}_n \hat{\rho} \hat{P}_n}{\mathrm{Tr}(\hat{\rho}\hat{P}_n)} \tag{2.13}$$

2.5 Principio di indeterminazione di Heisenberg

Due concetti fondamentali per la Meccanica Quantistica sono quelli di posizione e momento. Ad essi sono associati degli operatori che non commutano, rispettivamente $\hat{p}$ e $\hat{q}$, i quali sono anche osservabili [18].

$$\left[\hat{q}, \hat{p}\right] = \hat{q}\hat{p} - \hat{p}\hat{q} = i\hbar\hat{\mathcal{I}} \tag{2.14}$$

Il Principio di Indeterminazione di Heisenberg [6] è una delle conseguenze più importanti della Meccanica Quantistica, ed esso stabilisce un limite alla misurazione di grandezze fisiche coniugate. Ciò che stabilisce Heisenberg è che la posizione e la quantità di moto di una particella non possono essere misurate simultaneamente e con precisione arbitraria:

$$\Delta q_{|\psi\rangle} \Delta p_{|\psi\rangle} \geq \frac{1}{2} |\left\langle \left[\hat{q}, \hat{p}\right] \right\rangle_{|\psi\rangle}| = \frac{1}{2} i\hbar \left\langle \psi | 1 | \psi \right\rangle = \frac{\hbar}{2} \tag{2.15}$$

3

Base teorica dei sistemi di misura

3.1 Concetti basilari per la misurazione

Di seguito sono elencati i principali risultati della quantizzazione del campo elettromagnetico [8] utili allo svolgimento di questo lavoro. Per una trattazione più completa si rimanda a quanto descritto da Ulf Leonhard nel suo libro *Measuring the Quantum States of Light* [8].

Considerando un'onda piana polarizzata linearmente, l'Hamiltoniana (classica) associata si dimostra essere la seguente [4]:

$$\hat{H} = \frac{1}{2} \cdot \left(q^2 + p^2\right) \tag{3.1}$$

dove q e p sono rispettivamente le variabili di posizione e momento. È possibile esprimere l'Hemiltoniana anche in funzione della pulsazione dell'onda ω: in questo modo si rende evidente l'analogia con l'oscillatore armonico unidimensionale [18], oggetto che permette di trattare la descrizione quantistica del campo elettromagnetico.

La versione quantistica dell'Hamiltoniana, indicata con $\hat{H}$, si ottiene tramite la procedura di quantizzazione canonica [4]. Pertanto, promuovendo le variabili q e p ad operatori:

$$q \longrightarrow \hat{q} \tag{3.2}$$

$$p \longrightarrow \hat{p} \tag{3.3}$$

si ottiene:

$$\hat{H} = \frac{1}{2} \cdot (\hat{q}^2 + \hat{p}^2) \tag{3.4}$$

Definendo una coppia di operatori $\hat{a}^\dagger$ e $\hat{a}$ [8], chiamati rispettivamente di creazione e distruzione, come segue:

$$\hat{a}^\dagger = \sqrt{\frac{1}{2}}\left(\hat{q} + i\hat{p}\right) \tag{3.5}$$

$$\hat{a} = \sqrt{\frac{1}{2}}\left(\hat{q} - i\hat{p}\right) \tag{3.6}$$

L'Hamiltoniana quantistica può essere riscritta:

$$\hat{H} = \left(\hat{a}^\dagger \hat{a} + \frac{\hat{\mathbb{I}}}{2}\right) \tag{3.7}$$

dove il prodotto $\hat{a}^\dagger \hat{a}$ è definito come operatore numero $\hat{n}$ [12]. Gli autostati di $\hat{H}$, espressi come $|n\rangle$, indicano il numero di fotoni (quanti di energia) presenti nel sistema. Questi sono infiniti numerabili con n naturale.

Nella trattazione della quantizzazione del campo elettromagnetico [8], di rilevante importanza per la tesi sono autostati dell'operatore di distruzione, chiamati stati coerenti, derivanti dalla soluzione della seguente equazione degli autovalori [8]:

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle \tag{3.8}$$

con α numero complesso. In particolare si pone interesse al caso $|\alpha = 0\rangle$ corrispondente allo stato coerente del vuoto e alla sua scomposizione nella base delle posizioni q. Pertanto, partendo dall'equazione (3.8) si ha [18]:

$$\left\langle q\middle|\hat{a}\middle|\alpha\right\rangle = \alpha \cdot \left\langle q\middle|\alpha\right\rangle = \alpha \cdot \psi_\alpha(q) \tag{3.9}$$

Ponendo $\left\langle q\middle|\alpha\right\rangle = \psi_\alpha(q)$ e sviluppando il primo membro si ricava che:

$$\langle q|\hat{a}|\alpha\rangle = \langle q|\hat{q}|\alpha\rangle + i\langle q|\hat{p}|\alpha\rangle = \tag{3.10}$$

$$= q\psi_\alpha(q) + i\Big(-\frac{1}{2}\frac{\mathrm{d}}{\mathrm{d}q}\psi_\alpha(q)\Big) = \tag{3.11}$$

$$= q\cdot\psi_\alpha(q) + \frac{1}{2}\frac{\mathrm{d}}{\mathrm{d}q}\psi_\alpha(q) \tag{3.12}$$

mentre il secondo è pari a zero visto che si considera il caso in cui $\alpha = 0$ [18]. Combinando il tutto si ottiene:

$$q\cdot\psi_\alpha(q) + \frac{1}{2}\frac{\mathrm{d}}{\mathrm{d}q}\psi_\alpha(q) = 0 \tag{3.13}$$

L'equazione differenziale ottenuta ha come soluzione la seguente funzione d'onda:

$$\psi_\alpha(q) = c\cdot e^{-q^2} \tag{3.14}$$

Le probabilità associate sono ottenute attraverso il modulo quadro di $\psi_\alpha(q)$: la soluzione ha una densità di probabilità gaussiana a meno di una costante c^2. Tale costante si determina imponendo la condizione di normalizzazione:

$$\int_{-\infty}^{+\infty} dq\,\big|\psi_\alpha(q)\big|^2 = 1 \tag{3.15}$$

tale per cui:

$$c = \sqrt{\frac{2}{\pi}} \tag{3.16}$$

Da ciò si evince che la funzione d'onda è:

$$\psi_\alpha(q) = \sqrt{\frac{2}{\pi}}\cdot e^{-q^2} \tag{3.17}$$

e la distribuzione di probabilità è:

$$\big|\psi_\alpha(q)\big|^2 = \frac{2}{\pi}\cdot e^{-2q^2} \tag{3.18}$$

In particolare si nota che la distribuzione di probabilità ha media nulla e varianza $\frac{1}{2}$.

3.2 Misurazione della gaussiana del vuoto quantistico

Un dispositivo tramite cui misurare uno stato quantistico del campo elettromagnetico nella base delle posizioni è il ricevitore ottico omodina, il cui schema è riportato in Figura (3.1). Tale dispositivo è composto da un *Beam*

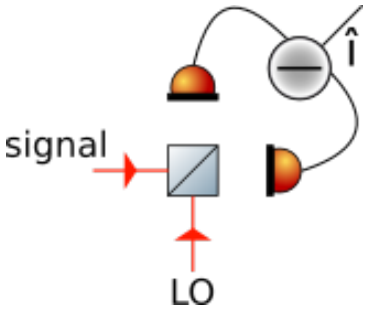

Figure 3.1: Schema che raffigura il sistema di misura omodina ottica che utilizza fotodiodi bilanciati.

Splitter (BS) 50:50, un laser ed una coppia di fotodiodi. Dei due ingressi del BS (P1, P2), uno è occupato dallo stato quantistico da misurare, mentre l'altro dal laser (che si assume sufficientemente intenso in modo da poterne considerare l'approssimazione classica). Da notare che la relazione input-output [18] di un BS in generale è:

$$v_{out} = S_{SB} v_{in} = \begin{bmatrix} \tau & -\rho \\ \rho & \tau \end{bmatrix} v_{in} \qquad \tau^2 + \rho^2 = 1 \tag{3.19}$$

dove v_{out} e v_{in} sono rispettivamente le porte di uscita ed ingresso del dispositivo, S_{SB} la matrice di scattering e τ e ρ la transmittanza e riflettanza del BS stesso (nota che nel caso 50:50, $\tau = \rho = 1/\sqrt{2}$) [18]. L'output del dispositivo è rappresentato, invece, dalla differenza delle due correnti derivanti dai fotorivelatori, dispositivi che convertono i fotoni in un impulso elettrico.

Quest'ultimo, come dimostrato in maggior dettaglio in [8], risulta essere proporzionale a:

$$\hat{I} \propto \hat{n}_{21} = \hat{n_2} - \hat{n_1} \tag{3.20}$$

Per la definizione di operatore numero, la presenza del BS 50:50 e l'approssimazione classica del laser, $\hat{n_1}$ e $\hat{n_2}$ risultano:

$$\hat{n_1} = \hat{a}_1^\dagger \hat{a}_1 = \frac{1}{2}\Big(\hat{a}^\dagger + \alpha_{LO}^*\Big)\Big(\hat{a} + \alpha_{LO}\Big) \tag{3.21}$$

$$\hat{n_2} = \hat{a}_2^\dagger \hat{a}_2 = \frac{1}{2}\Big(\hat{a}^\dagger + \alpha_{LO}^*\Big)\Big(\hat{a} + \alpha_{LO}\Big) \tag{3.22}$$

Pertanto $\hat{n}_{21}$ è dato dalla seguente espressione:

$$\hat{n}_{21} = \alpha_{LO}^* \hat{a} + \alpha_{LO}^* \hat{a}^\dagger \tag{3.23}$$

Richiamando le equazioni (3.5) e (3.6), in cui si esprimono gli operatori di creazione e distruzione in funzione di $\hat{q}$ e $\hat{p}$, si ha che:

$$\hat{n}_{21} = \alpha_{LO}^* \cdot \hat{a} + \alpha_{LO} \cdot \hat{a}^\dagger = \tag{3.24}$$

$$= \frac{1}{\sqrt{2}}\alpha_{LO} \cdot (\hat{q} + i\hat{p}) + \frac{1}{\sqrt{2}}\alpha_{LO} \cdot (\hat{q} - i\hat{p}) = \tag{3.25}$$

$$= \frac{1}{\sqrt{2}} \cdot 2 \cdot \mathrm{Re}\big\{\alpha_{LO}(\hat{q} - i\hat{p})\big\} = \tag{3.26}$$

$$= \sqrt{2} \cdot \mathrm{Re}\big\{|\alpha_{LO}|e^{\theta_{LO}}(\hat{q} - i\hat{p})\big\} \tag{3.27}$$

Ricordando la notazione di Eulero $e^\theta = \cos\theta + i\sin\theta$:

$$\sqrt{2} \cdot \mathrm{Re}\big\{|\alpha_{LO}|e^{\theta_{LO}}(\hat{q} - i\hat{p})\big\} = \sqrt{2}|\alpha_{LO}| \cdot \mathrm{Re}\big\{e^{\theta_{LO}}(\hat{q} - i\hat{p})\big\} = \tag{3.28}$$

$$= \sqrt{2}|\alpha_{LO}| \cdot (\hat{q}\cos\theta_{LO} + \hat{p}\sin\theta_{LO}) = \tag{3.29}$$

$$= \sqrt{2}|\alpha_{LO}|\hat{q}_\theta \tag{3.30}$$

Il termine θ_{LO} è la fase fornita dal laser. Da notare che ponendo $\theta_{LO} = 0$, si ottiene che $\hat{I} \propto \hat{q}$, che corrisponde alla misura della quadratura.

3.3 Misura simultanea di posizione e momento

Per completezza di riporta anche lo schema ottico standard utilizzato per la misura simultanea di entrambe le quadrature del campo elettromagnetico. Per misurare simultaneamente le quadrature $\hat{q}$ e $\hat{p}$, si può utilizzare un dispositivo eterodina [1], il quale è composto da un BS 50:50 per creare due copie dello stato

quantistico da misurare. Queste saranno successivamente analizzate da due omodine distinte per la determinazione della posizione e momento in maniera separata, ma simultanea [8]. Per ottenere ciò, gli oscillatori locali delle omodine risultano essere sfasate di 90 gradi. Infatti, ponendo la fase dell'omodina H1 $\theta_{LO} = 0$, la corrente uscente sarà proporzionale alla quadratura $\hat{q}$; di conseguenza la fase dell'omodina H2 sarà $\theta_{LO} = \frac{\pi}{2}$ e la misura risulterà direttamente proporzionale alla quadratura $\hat{p}$.

Poiché $\hat{q}$ e $\hat{p}$ non sono operatori commutabili [8], secondo il Principio di Indeterminazione di Heisenberg non è possibile misurarli simultaneamente con precisione arbitraria. Da ciò si conclude che la misura delle quadrature utilizzando l'eterodina [8] è caratterizzata anche da del rumore aggiuntivo, e ciò è tangibile nel beam splitter che esegue la copia del segnale: oltre allo stato quantistico da misurare presente in uno degli ingressi, nell'altro è presente il vuoto $|0\rangle$. Sebbene intuitivamente in tale ingresso si era assunto non ci fosse nulla (perfettamente legittimo in fisica classica), in termini quantistici questo non è possibile, ci deve essere qualcosa ed in questo caso è il vuoto. Pertanto lo stato quantistico da misurare risulta essere miscelato con uno stato quantistico non voluto determinando la componente di rumore aggiuntiva nelle misure.

Il dispositivo appena descritto può essere implementato dall'eterodina a otto porte, il cui schema è riportato qui sotto in figura (3.2).

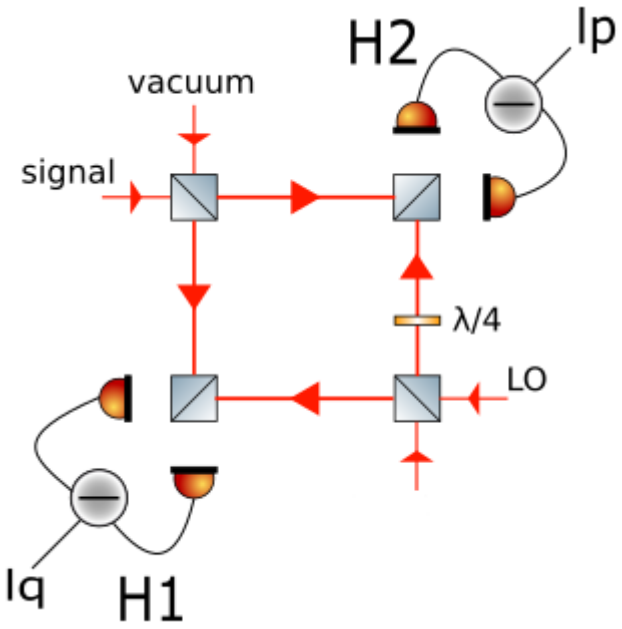

Figure 3.2: Schema che raffigura il sistema di misura eterodina a otto porte che utilizza fotodiodi bilanciati.

4

Realizzazione dell'omodina ottica

In questo capitolo si espone l'implementazione sperimentale dell'omodina ottica introdotta nel capitolo precedente caratterizzandone i componenti utilizzati e verificando il corretto funzionamento dello stesso quando lo stato del vuoto viene iniettato. Inoltre verrà stimata la randomicità estraibile da un QRNG basato su tale schema.

Poiché in questa configurazione, il QRNG è di tipo *fully-trusted*, che si ricorda essere caratterizzato dalla completa conoscenza dei componenti utilizzati e dal particolare stato quantistico impiegato (il vuoto in questo caso).

4.1 Setup

Lo schema seguito per la realizzazione del *setup* sperimentale dell'omodina è riportato in Figura (4.1), il quale fa riferimento a quello teorico esposto nel capitolo precedente, Figura (3.1), con l'aggiunta di ulteriori componenti necessaria alla caratterizzazione dell'omodina stessa.

La parte ottica del set-up è realizzata interamente con componenti in fibra discreti. Fotodiodi e Laser (Kohereon LPD100) sono invece integrati in un'unica scheda in modo da favorire la compattazione del set-up.

Al fine di evitare che la luce riflessa dei componenti utilizzati rientri nel laser causando problemi di funzionamento ed instabilità, un isolatore ottico [7] è stato posizionato all'uscita di quest'ultimo.

Ai fini delle analisi sul funzionamento dell'apparato omodina, un BS 99:1 è stato utilizzato per convogliare il 99% della luce del laser verso l'omodina

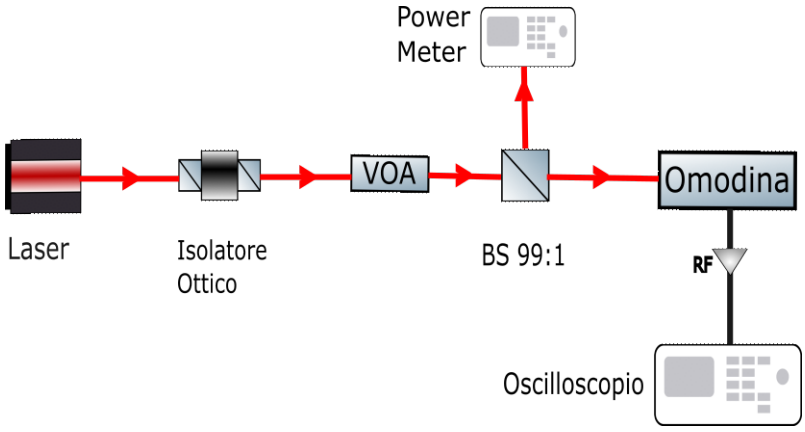

Figure 4.1: Setup dell'omodina ottica.

vera e propria; il restante 1% viene direzionato verso un *Power Meter* (Thorlabs PMD100D) per monitorare la risposta dell'omodina in funzione della potenza ottica in entrata.

Tra l'isolatore ottico e il BS 99:1 è stato posizionato anche un VOA (*Variable Optical Attenuator*, marca Thorlabs VOA50-APC), un dispositivo in grado di regolare la potenza ottica del laser attenuando il segnale.

Il segnale in uscita dai fotodiodi bilanciati è acquisito dall'oscilloscopio (Siglent SDS1000X), il quale converte, tramite il suo ADC, la foto-corrente in uno *stream* digitale per ulteriori analisi.

Tra l'omodina e l'oscilloscopio è posizionato un amplificatore RF (Minicircuit ZFL-500+), che serve per far corrispondere il *range* del segnale elettrico in uscita all'omodina con quello dell'ADC dell'oscilloscopio.

Si vuole inoltre riportare che i BS utilizzati soddisfano i rispettivi dati di targa. Infatti è stato determinato sperimentalmente che le potenze in uscita, quando i componenti vengono attaccati ad un laser, al BS 50:50 sono $P_{50,1} = 2,000\,mW$ e $P_{50,2} = 2,072\,mW$ e il rapporto tra potenze è circa 1; invece, per il BS 99:1, le potenze in uscita sono $P_{99} = 4,022\,mW$ e $P_1 = 45,59\,nW$ e il loro rapporto è circa 0,010, che corrisponde a $\frac{1}{99}$.

Si vuole infine puntualizzare che per ottenere il vuoto quantistico necessario all'esperimento, è stata chiusa la rispettiva porta di input: questa operazione è un modo semplice per ottenere lo stato quantistico in questione.

4.2 CMRR

CMRR è l'acronimo di *Common Mode Rejection Ratio* e indica la tendenza del dispositivo a rigettare i segnali d'ingresso comuni a entrambi gli ingressi. Il funzionamento dell'omodina richiede che agli ingressi dei fotodiodi ci sia esattamente lo stesso segnale, ma il *beam splitter* 50:50 utilizzato non lo garantisce a causa di non idealità nella costruzione. Altre forme di sbilanciamento sono sono causate da non idealità nella realizzazione dei fotodiodi stessi oltre al fatto di non essere perfettamente uguali dovute a tolleranze nei processi produttivi.

Sperimentalmente, si cerca di valutare tale condizione di sbilanciamento iniettando all'ingresso dell'omodina (porta usata poi per misurare gli stati quantistici), un laser la cui intensità è modulata, tramite *intensity modulator*, con una sinusoide di frequenza $f_0 \approx 2\,MHz$, e misurando l'uscita dei fotodiodi con un analizzatore di spettro.

Le misure vengono fatte in due condizioni, nella prima si considera l'apparato totalmente sbilanciato (si scollega una delle porte di uscita del BS), nella seconda lo si considera bilanciato (questa è la configurazione normale di funzionamento dell'omodina). In Figura (4.2) si riportano gli spettri ottenuti nelle due configurazioni. Dalla figura si nota il picco a $2MHz$ corrispondente alla frequenza della modulante. La differenza nelle ampiezze ($A_{ubl} = -22.05\,dBm$ caso sbilanciato, $A_{bl} = -72.69\,dBm$ caso bilanciato) di tali picchi ci fornisce un stima del CMRR che nel caso specifico risulta:

$$CMRR = A_{ubl} - A_{bl} = 50.64\,dBm \tag{4.1}$$

Si fa notare infine che, se i fotodiodi fossero perfettamente identici, i picchi in f_0 non esisterebbero perchè l'output dell'omodina è una differenza delle foto-correnti provenienti dai due fotodiodi. Di conseguenza, essendo le foto-correnti identiche, la loro differenza porterebbe all'annullamento dei picchi di sbilanciamento.

4.3 Caratterizzazione del dispositivo omodina

Ai fini pratici, il dispositivo omodina realizzato richiede di essere calibrato. Per fare ciò lo stato quantistico del vuoto viene iniettato e, per diversi valori della potenza dell'oscillatore locale (variata tramite un VOA e misurata tramite

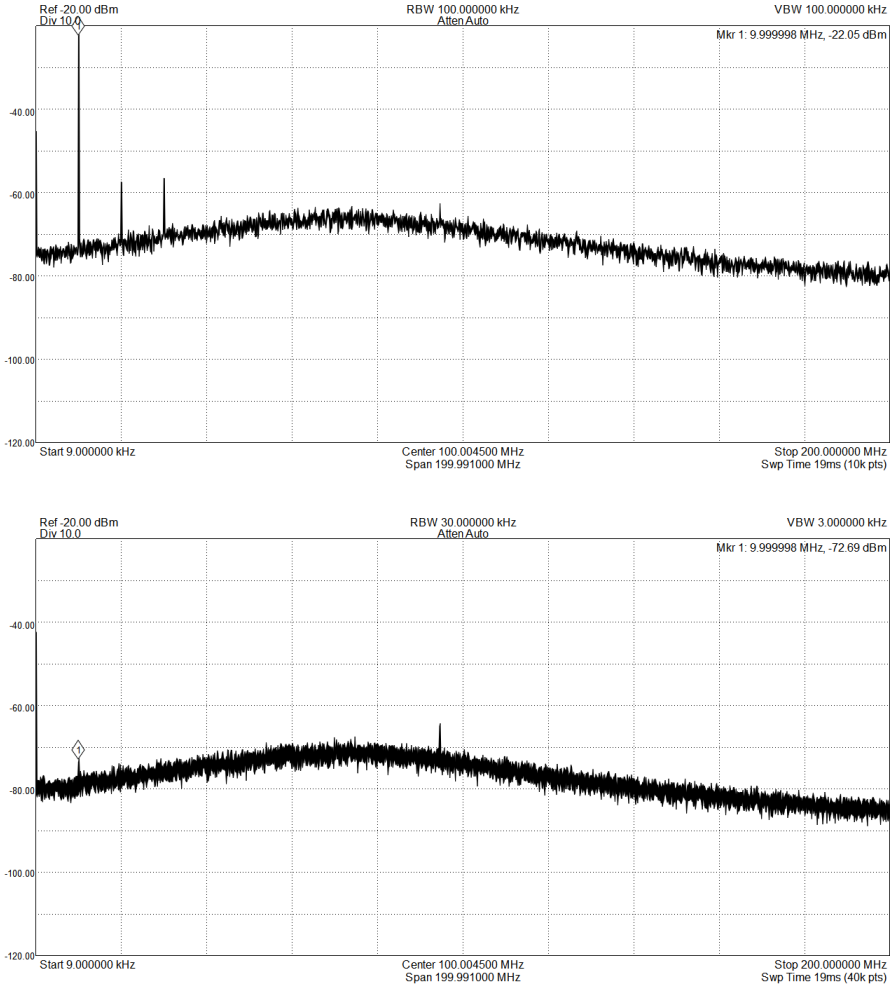

Figure 4.2: Sopra FFT del segnale ottenuto dal completo sbilanciamento del sistema, l'ampiezza del picco è di -22.05 dBm, sotto FFT del segnale ottenuto dal completo bilanciamento del sistema, l'ampiezza del picco è di -72.69 dBm.

il Power-Meter), l'uscita dei fotodiodi viene acquisita da un oscilloscopio per poi essere analizzata al computer. Per lo scopo, per ogni valore della potenza di LO usata, sono stati usati acquisiti 2 milioni di punti a 2 GSps con un risoluzione di 8 bit (ADC dell'oscilloscopio).

Delle tracce acquisite ne è stata stimata la varianza statistica e riportata in un grafico, in Figura (4.3), in funzione della potenza ottica associata.

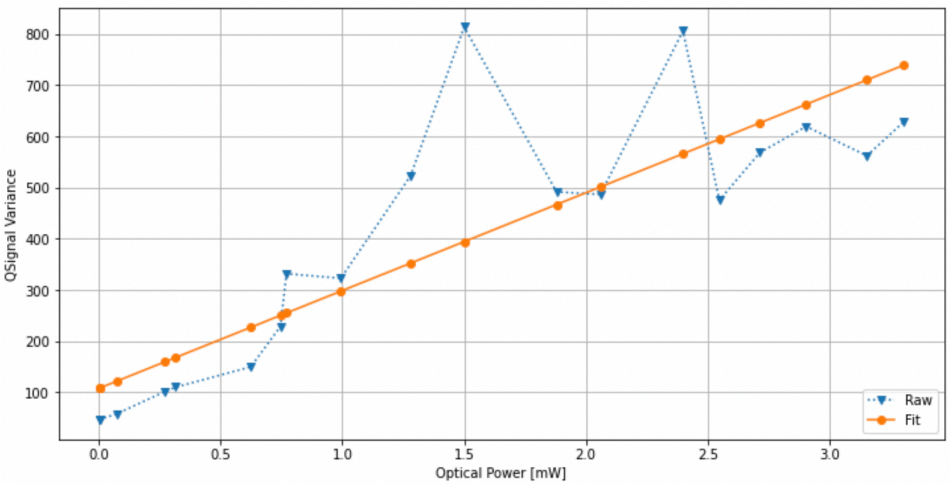

Figure 4.3: Relazione tra la potenza ottica del laser integrato e la varianza del segnale dello stesso.

Dalla figura, si evince che l'andamento dei dati grezzi si discosta di molto da quello lineare. La causa si è riscontrato essere dovuta al laser integrato adottato: la potenza di quest'ultimo fluttuava considerevolmente al variare della temperatura in tempi confrontabili con il tempo di acquisizione di una traccia dell'oscilloscopio (da notare che viene richiesta una stabilità della durata pari al tempo richiesto per effettuare la scansione delle potenze di LO, dell'ordine delle decine di minuti). Pertanto il laser non si è dimostrato adatto allo scopo e si è dovuta cercare una soluzione alternativa. Adattare un TEmperature Controller (TEC) commerciale al laser integrato nella scheda non era un'opzione valida nei tempi previsti. Per questo motivo, si è optato per l'utilizzo di un laser esterno dotato di controllo di temperatura già presente in laboratorio: un Fabry Perrot (Thorlabs) dotato di TEC esterno e il Santec (WSL-110) sono stati presi in considerazione (entrambi i laser sono dotati di una lunghezza d'onda di 1550 nm, parametro standard per le telecomunicazioni). Per entrambi è stata eseguita la procedura elencata in precedenza e i risultati sono riportati in Figura (4.4).
Tra i due il Santec è quello che presenta l'andamento più lineare, pertanto si è

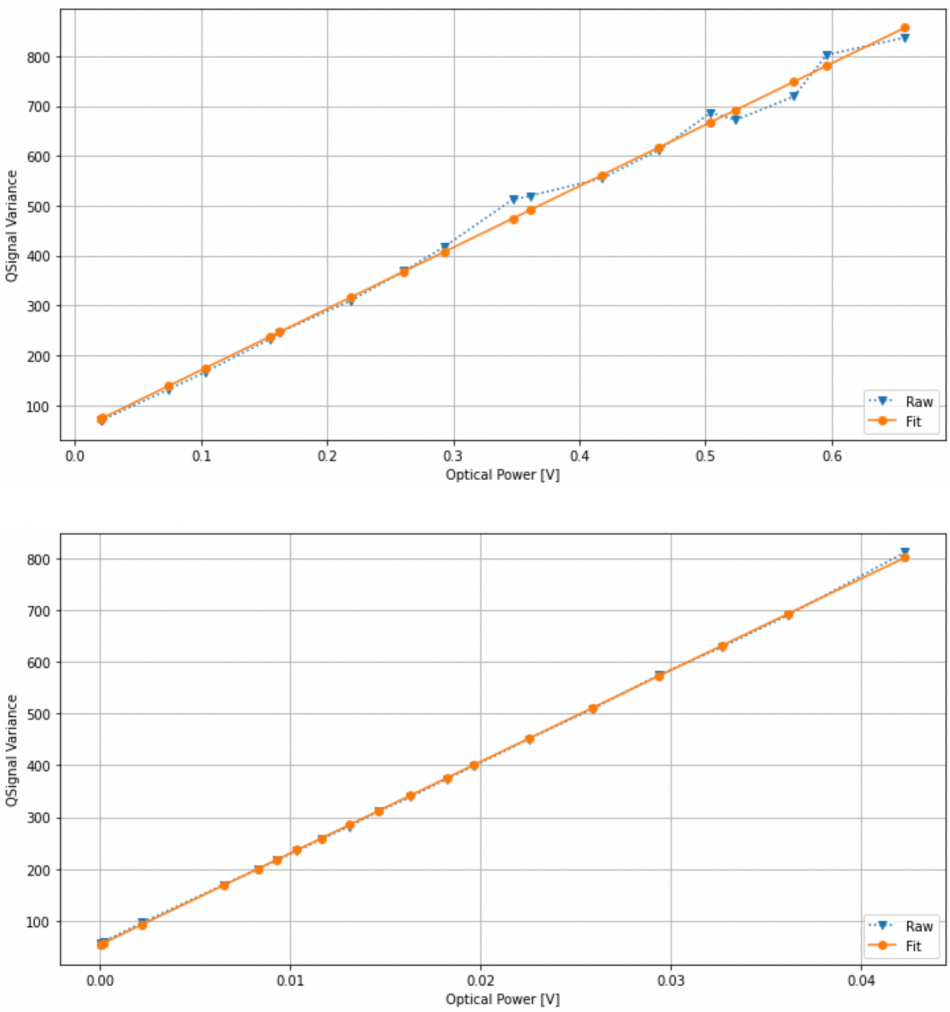

Figure 4.4: Sopra si presenta la relazione varianza-potenza ottica del laser Fabbry Perrot, sotto la stessa relazione ma relativa al laser Santec.

deciso di adottare questo per tutti gli esperimenti successivi.

Di seguito è esposto il grafico della trasformata di Fourier del segnale della risposta dell'omodina (4.5), in cui si utilizza la massima potenza di LO. Si può concludere che non si notano interferenze o picchi spuri nella banda di interesse, e ciò è ulteriore indice della qualità della catena elettronica usata. Per poter

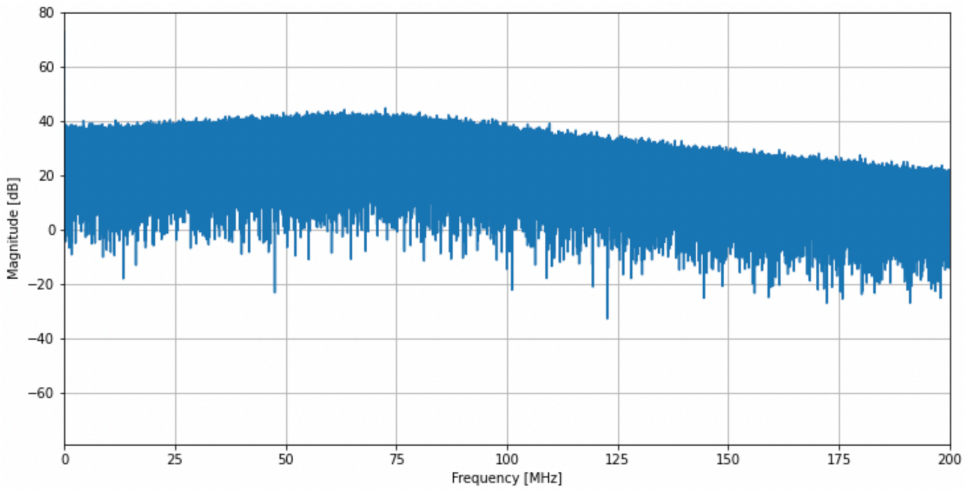

Figure 4.5: Trasformata di Fourier del segnale dato dal laser Santec.

stimare il rapporto tra il segnale quantistico e il rumore elettronico si considera la Clearance, la quale è riportata in Figura (4.6), dove si può notare che, nella

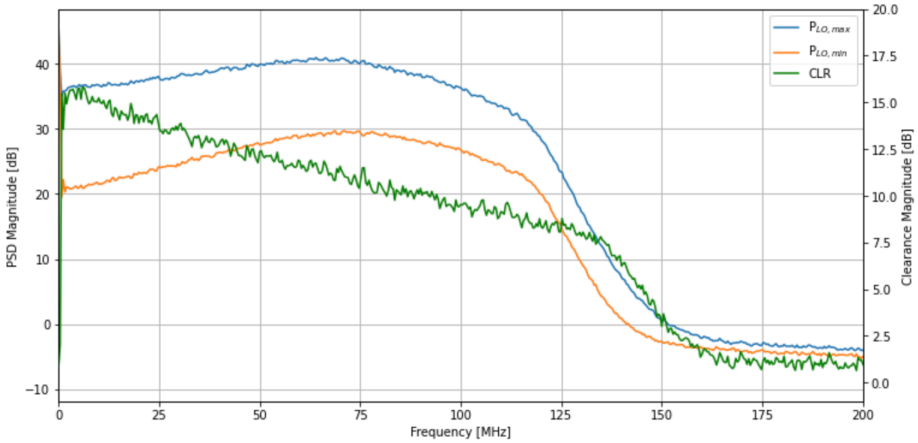

Figure 4.6: Grafico che stima la clearance, andamento che dà informazione sul rapporto tra il segnale quantistico e il rumore elettronico.

banda di interesse, questa va circa da 8 dB a 15 dB.

4.4 Analisi statistiche

In questa sezione si vuole verificare che, misurando il vuoto quantistico, si ottenga una distribuzione gaussiana e che la varianza sia pari a $\frac{1}{2}$, come dimostrato teoricamente nel capitolo precedente. Per quanto riguarda il laser questa ipotesi non è richiesta, in quanto esso viene considerato come una sorgente luminosa classica.

Poiché non si dovrà lavorare con l'intero spettro ma solamente con una sua porzione (fino a 100 MHz, frequenza che delinea la banda del fotodiodo bilanciato), i dati analizzati saranno quelli filtrati e non grezzi, i quali presentano anche delle correlazioni. Queste ultime sono dovute alla risposta limitata del sistema (passa banda o passa basso).

Per lavorare con i dati filtrati, si effettua una procedura di resampling, che consiste nell'utilizzare solo alcuni dei dati a disposizione, e corrisponde al filtraggio dei dati grezzi. Il fattore di *resampling* RF rappresenta il passaggio dalla frequenza di campionamento dell'oscilloscopio a quella di interesse (100 MHz), in questo lavoro il esso è pari a:

$$RP = \frac{f_{OSC}}{2 \cdot 100MHz} = \frac{1}{10} \tag{4.2}$$

Di seguito, in figura (4.7) si mostra l'andamento del segnale omodina tenendo conto del *resampling*: il segnale non riporta picchi dovuti ad interferenze.

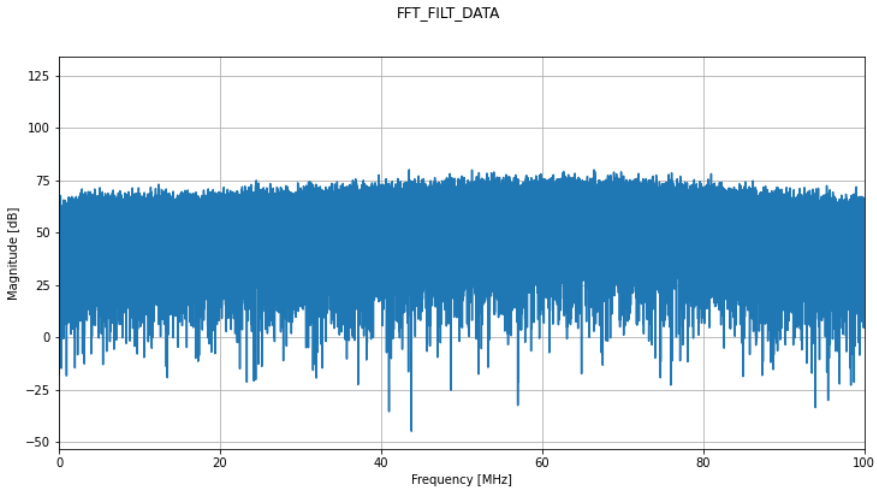

Figure 4.7: FFT del segnale omodina dopo aver effettuato il resampling.

In figura (4.8) si mostrano i risultati del laser Santec: l'istogramma rappresenta i valori di tensioni nella rappresentazione binaria dell'ADC dell'oscilloscopio per poter comprendere la distribuzione di probabilità delle misure ottenute.

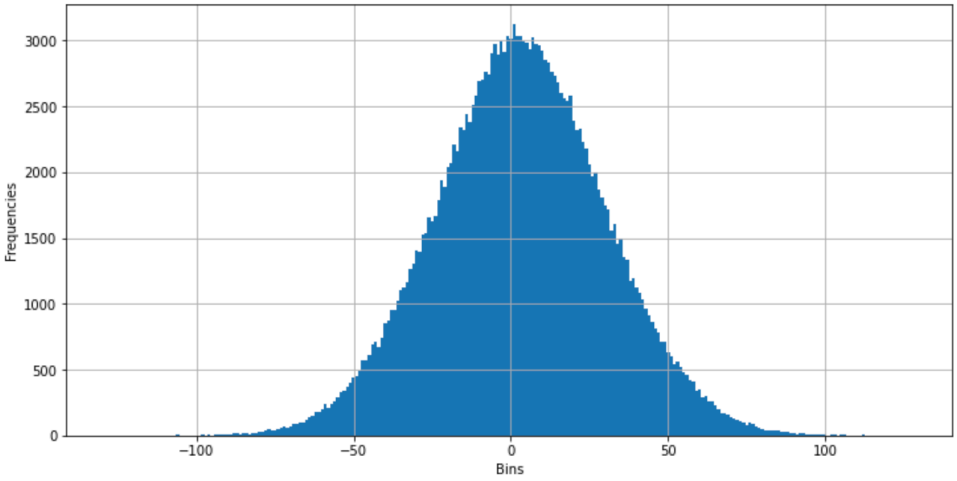

Figure 4.8: Gaussiana dei dati filtrati relativa al vuoto quantistico nel caso dell'utilizzo del laser Santec.

Per verificare che la varianza della distribuzione appena trovata sia pari a $\frac{1}{2}$, si deve effettuare una conversione in unità di vuoto della gaussiana. Si effettua la conversione perchè i dati analizzati fino ad ora sono proporzionali alla tensione del segnale elettrico.
Convertendo il segnale in unità di vuoto si va a modificare la varianza del segnale attraverso questa relazione [1]:

$$\sigma^2_{VU,p,q} = \frac{\sigma^2_{PU,p,q}}{k_{p,q} \cdot P_{LO}} \tag{4.3}$$

$k_{q,p}$ è un fattore di conversione pari a $k_{q,p} = 2 \cdot m_{p,q}$, dove $m_{p,q}$ è il coefficiente angolare che si utilizza per effettuare la conversione, e proviene dalla procedura di calibrazione; P_{LO} è invece la potenza misurata dell'Oscillatore Locale. Il coefficiente angolare della retta in basso in figura (4.4) è $m = 15945,02\, bit^2/mW$. Di seguito si mostra la relativa gaussiana convertita in unità di vuoto (4.9): In questo caso la varianza è pari a $\sigma^2 = 0.54$ in unità di vuoto. In questo caso la varianza risulta maggiore al valore trovato nel capitolo precedente perché c'è un fattore aggiuntivo proporzionale all'intercetta della retta nella formula della varianza espressa in unità di vuoto.

Per ovviare a ciò, è possibile fare la conversione in unità di vuoto delle

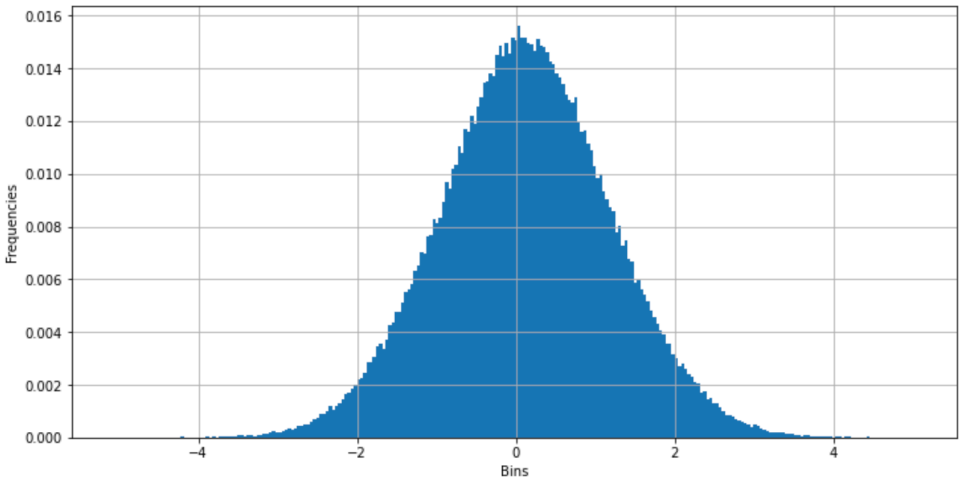

Figure 4.9: Gaussiana convertita in unità di vuoto relativa al caso dell'utilizzo del laser Santec. Il coefficiente angolare della retta è $m = 15945,02\, bit^2/mW$ e l'intercetta è pari a $q = 45.14\, bit^2/mW$.

gaussiane utilizzando anche l'intercetta, la quale è un parametro dovuto dal rumore elettronico, e non solo il coefficiente angolare della retta di calibrazione. In questo modo, il fattore aggiuntivo citato in precedenza andrebbe ad annullarsi avvicinando il valore della varianza del segnale a $\frac{1}{2}$. L'intercetta della retta in basso in figura (4.4) è $q = 53.944\, bit^2/mW$. Considerando anche l'intercetta $q_{p,q}$, l'espressione di $k_{q,p}$ diventa:

$$k_{q,p} = 2 \cdot \left(m_{p,q} + \frac{q_{p,q}}{P_{LO}} \right) \tag{4.4}$$

dove P_{LO} è la potenza ottica del laser misurata. I dati convertiti con questo nuovo fattore di conversione portano ad una statistica gaussiana di varianza pari a $\sigma^2 = 0.506$ in unità di vuoto come riportato in Figura (4.10).
La varianza delle due gaussiane convertite cambia a causa della considerazione dell'intercetta. Essa cambia perché si sta tenendo conto del rumore elettronico, il quale è un elemento che influenza le prestazioni dell'omodina.

4.5 Risultati

In questa sezione si vuole mettere in luce le proprietà dell'omodina in ambito del *fully-trusted* QRNG.

Dalla conversione in unità di vuoto è possibile ottenere la massima probabilità della statistica, dalla quale si ricava la min-entropy classica del QRNG (nel

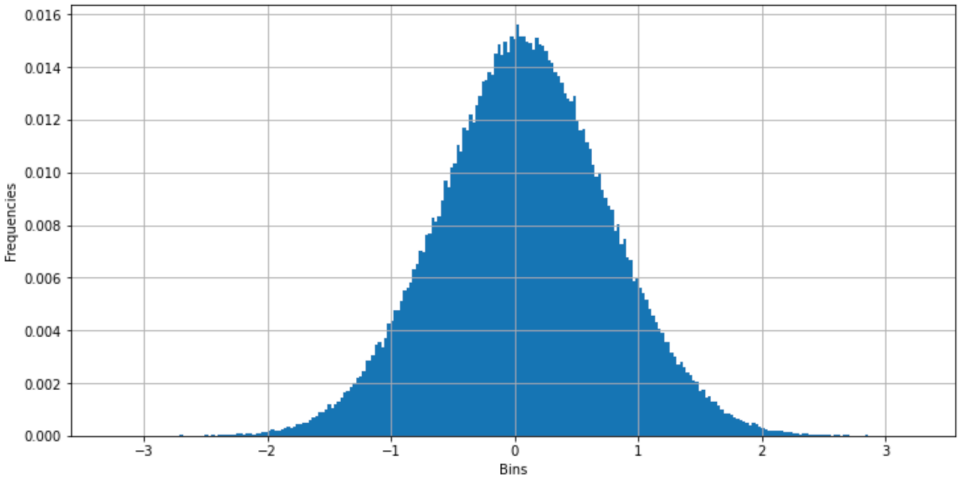

Figure 4.10: Gaussiana convertita in unità di vuoto utilizzando il laser Santec facendo uso dell'intercetta. Il coefficiente angolare della retta è $m = 15945,02\,bit^2/mW$ e l'intercetta è pari a $q = 45.14\,bit^2/mW$.

caso dell'omodina ottica, rappresenta il numero di bit veramente casuali nella configurazione *fully-trusted* QRNG. In altre parole la min-entropy indica la probabilità di indovinare il risultato della misura quando questa viene effettuata. La min-entropy si calcola nel seguente modo [1]:

$$h_{min} = -\log_2(P_{max}) \tag{4.5}$$

dove P_{max} è la probabilità massima della statistica, e cioè del bin più probabile.

In questo caso si vuole stimare la min-entropy nel caso della conversione in unità di vuoto e $P_{max} = 0.01538$. Di conseguenza $h_{min} = 6.02\,bit$.

Dalla min-entropy si può ricavare anche il il rate di generazione del QRNG mediante la seguente formula:

$$R_{omodina} = h_{MIN} \cdot f_{OSC} \cdot RF \tag{4.6}$$

Come si può notare dalla formula, il rate di generazione dell'omodina è il prodotto di tre fattori, che sono la min-entropy, la frequenza di campionamento dell'oscilloscopio e il fattore di resampling RF. A questo punto, il rate di generazione del *fully-trusted* QRNG è:

$$R_{omodina} = 1.204\,Gbps \tag{4.7}$$

5

Realizzazione omodina ottica con mixer elettronico

In questo capitolo si espone l'implementazione sperimentale di un ricevitore omodina con in cascata un mixer analogico con cui selezionare (filtrare) una porzione dello spettro fornito da quest'ultimo. Infatti, oltre al segnale omodino, il rumore di fase del laser (sempre presente a basse frequenze) ed eventuali interferenze accoppiatesi con il segnale omodino stesso possono impattare negativamente sul sistema QRNG.

5.1 Setup

In questa sezione si vuole descrivere il *setup* sperimentale, schematizzato in figura (5.1), con cui è stato testato il sistema di filtraggio proposto. Dalla figura, il *setup* utilizzato è molto simile a quello precedente (ricevitore omodina). Le uniche differenze sono l'aggiunta del mixer analogico (Demo Board DC1670A basato su chip LTC5584), il quale lavora ad una frequenza di 50 MHz e di un generatore di funzioni (Siglent SDG6000X) che fornisce il segnale sinusoidale per quest'ultimo. Con la portante generata si va a selezionare la porzione di spettro che va da 50 a 100 MHz del segnale omodino originale.

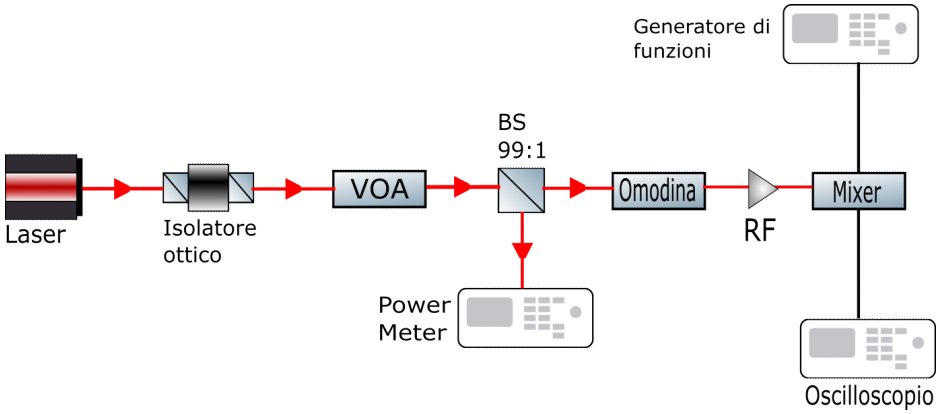

Figure 5.1: Setup del sistema di filtraggio.

5.2 Caratterizzazione del dispositivo omodina con mixer elettronico

Per quanto riguarda la calibrazione del dispositivo, la procedura utilizzata è la stessa di quella descritta nel capitolo precedente. Ai fini della calibrazione sono stati acquisiti per ciascuna potenza dell'oscillatore locale usato 2 milioni di punti con una risoluzione di 8 bit.

In figura (5.2) è riportato l'andamento della varianza del canale acquisito grezzo (miscelato con la portante a 50 MHz) rispetto alla potenza dell'oscillatore locale.

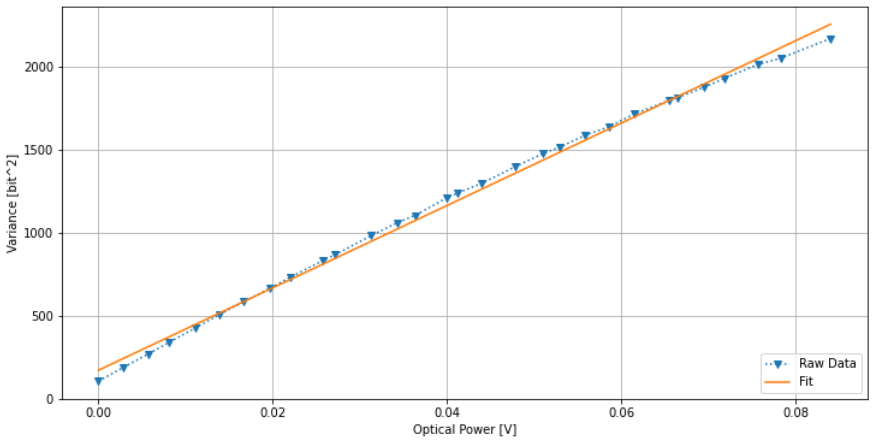

Figure 5.2: Grafico che mostra l'andamento della varianza del segnale grezzo in funzione della potenza ottica.

Inoltre, in Figura (5.3) è riportato il grafico della FFT del segnale relativo ai dati grezzi (miscelato con la portante a 50 MHz), quando la potenza dell'oscillatore locale è massima: si possono notare delle interferenze e in particolare un picco a $50\,MHz$, dovuto alla frequenza con cui il mixer è pilotato. Ai fini della calibrazione vera e propria, solamente la porzione di banda tra 0 e $50\,MHz$ del segnale miscelato viene tenuta (il resto va eliminato). A tal fine si effettua un filtraggio passa basso da 0 a 50 MHz seguito da un *resampling* con fattore $RF = \frac{1}{20}$. In Figura (5.4), si riporta il *fit* delle relazioni tra la potenza ottica

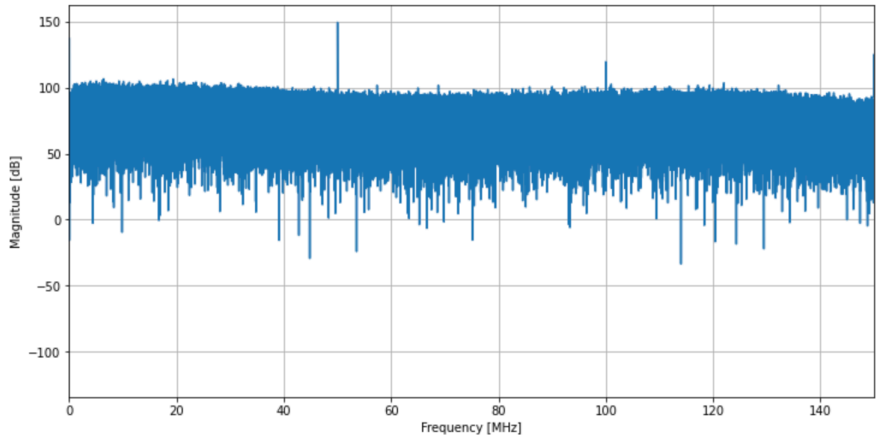

Figure 5.3: FFT del segnale grezzo, non elaborato.

e la varianza del canale dopo aver filtrato ed effettuato il *resampling* dei dati. In questo modo si potranno ricavare il coefficiente angolare e l'intercetta per la conversione in unità di vuoto. Dalla figura sono evidenti delle fluttuazioni, le quali potrebbero essere dovute probabilmente dal mixer.

Infine, in Figura (5.5) si mostra la FFT del segnale del canale dopo il filtraggio ed il *resampling*.

Anche in questo caso si vuole stimare il rapporto tra il segnale quantistico e il rumore elettronico attraverso la Clearance, mostrata in Figura (5.6) È evidente il picco a $50\,MHz$ dovuto alla frequenza su cui è tarato il mixer. Si nota la Clearance è circa di 14 dB nella banda di interesse (che va da 0 a $50\,MHz$). Non si considerano frequenze superiori perché si è in presenza di *aliasing*.

5.3 Analisi statistiche

Di seguito è riportata la statistica del segnale acquisito. Come nel paragrafo (3.1), il vuoto quantistico è stato iniettato nel ricevitore in esame. Pertanto ci si

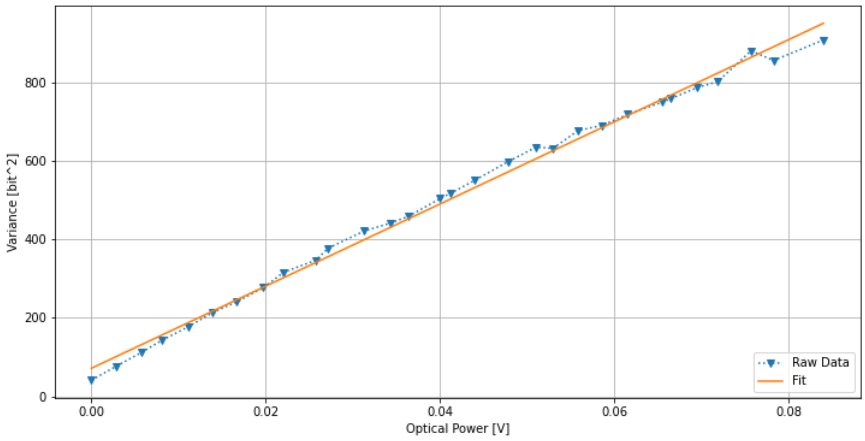

Figure 5.4: Fit del canale processato. Il coefficiente angolare è $m = 10469.93\, bit^2/mW$ mentre l'intercetta $q = 71.67\, bit^2/mW$.

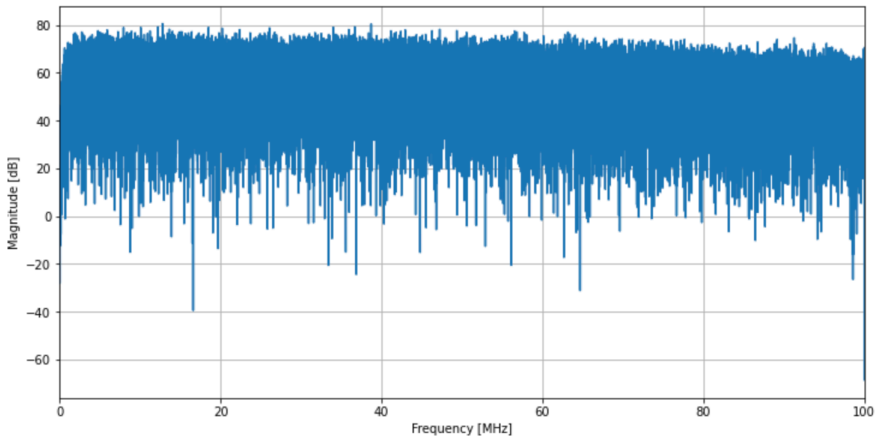

Figure 5.5: FFT del segnale dopo il filtraggio ed il *resampling*.

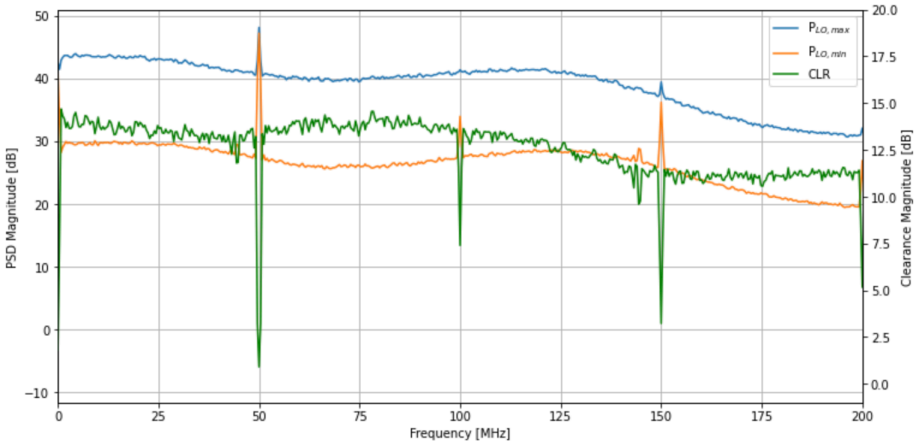

Figure 5.6: Grafico che rappresenta il rapporto tra il segnale quantistico e il rumore elettronico.

aspetta una gaussiana di varianza $\frac{1}{2}$.

La gaussiana non convertita in unità di vuoto è riportata in Figura (5.7).

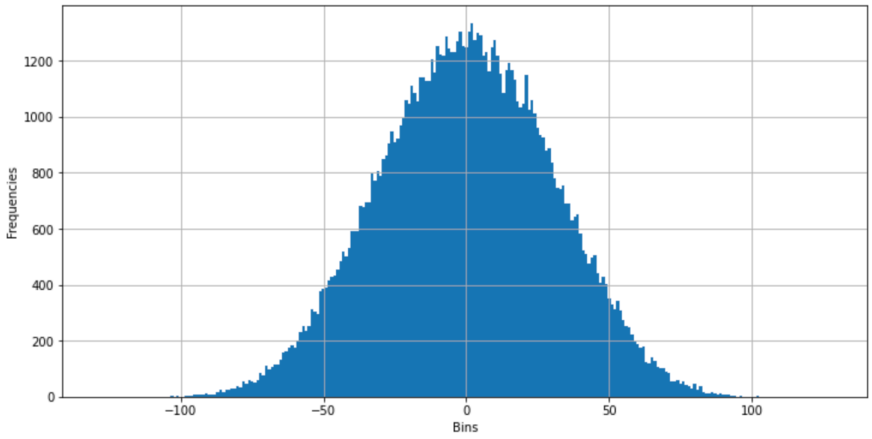

Figure 5.7: Gaussiana non convertita relativa al vuoto quantistico.

In Figura (5.8), si riporta la gaussiana convertita in unità di vuoto utilizzando $m = 10469.93\, bit^2/mW$.

In questo caso la varianza ottenuta è, $\sigma^2 = 0.51$, in unità di vuoto.

Dalla conversione in unità di vuoto mediante l'utilizzo dell'intercetta sono emersi dei dati problematici. La varianza del vuoto quantistico risulta essere minore di $\frac{1}{2}$: ciò non corrisponde a nessun stato quantistico esistente, in quanto è violato il Principio di Indeterminazione di Heisenberg.

Questo risultato può essere dovuto ad un fit lineare non pesato, il quale ha portato ad una sovrastima del rumore elettronico e di conseguenza una

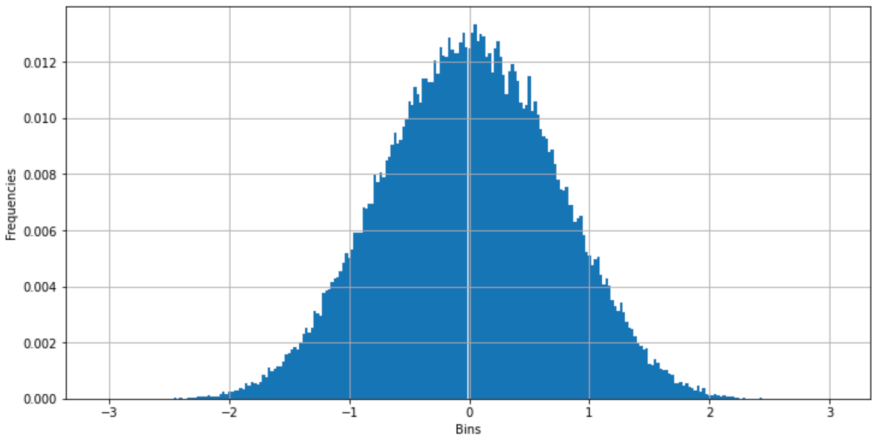

Figure 5.8: Gaussiana relativa al vuoto quantistico convertito in unità di vuoto.

sottostima della varianza. Per questo motivo, da questo punto in poi verrà considerato solamente il caso della conversione in unità di vuoto con il solo utilizzo del coefficiente angolare.

5.4 Risultati

Questa sezione fornisce i risultati dell'analisi dell'omodina con il sistema di filtraggio proposto in ambito del QRNG.

La *classical min-entropy* è stata stimata, in questo caso $h_{min}(X) \approx 6.23\,bit$. Rispetto al setup precedente, si ha un aumento della *min-entropy*. Le motivazioni sono dovute al minor contributo del rumore elettronico (l'intercetta presenta un minore valore nel caso del sistema con mixer) ed una Clearance complessivamente maggiore e costante lungo tutta la finestra di 50 MHz. Il *rate* di generazione che si è in grado di raggiungere con questo setup è di $\approx 623 Mbps$. Questa è minore del caso senza mixer per il fatto che la banda in esame è minore. Tuttavia si è confidenti che con una maggiore attenzione nella taratura del mixer si riesce ad aumentare la banda disponibile arrivando ad un *rate* maggiore. Tuttavia, le fluttuazioni mostrate nella Figura (5.4) non devono essere trascurate e, poiché l'andamento della relazione tra varianza e potenza ottica non è propriamente lineare, i risultati sono da considerarsi non conclusivi ma un'indicazione di ciò che si può raggiungere caratterizzando e calibrando meglio il dispositivo.

6

Conclusioni

L'obiettivo di questo lavoro è la caratterizzazione dei dispositivi omodina ed omodina con mixer elettronico ai fini di utilizzo in ambito dei QRNG. I componenti utilizzati sono tutti disponibili in commercio in modo da contenere i costi di realizzazione e sviluppo.

Lo schema utilizzato è di semplice implementazione ed è formato da una parte in fibra che sfrutta lunghezze d'onda di 1550 nm, e da una scheda che integra laser e fotodiodi. Tutto ciò è utile per una questione di spazio, poiché ci sono vari componenti fissati sulla scheda e perciò un minor ingombro del sistema.

Nell'analisi dell'omodina ottica, il laser della scheda integrata ha presentato dei problemi di stabilità di potenza dovuti alle fluttuazioni di temperatura. Per questo motivo, per motivi di tempo si è preferito utilizzare un laser esterno dotato di TEC per caratterizzare i fotodiodi, dispositivi che si occupano della conversione delle misure quantistiche in grandezze elettriche.

Come sviluppo futuro, si potrebbe dotare il laser della scheda integrata un TEC in modo da stabilizzare la potenza del laser rendendolo più robusto rispetto alle variazioni della temperatura ambientale.

Per quanto riguarda la parte di ricezione, si è verificata la linearità dei fotodiodi e si è riusciti a realizzare un QRNG trusted sfruttando lo stato quantistico del vuoto elettromagnetico come sorgente di randomicià. In questa configurazione, impiegando l'intera banda di 100 MHz messa a disposizione dal ricevitore, si è stimata una *classical un-conditional min-entropy* di 6,02 bit, permettendo di rag-

giungere ha un rate di generazione pari a $R_{omodina} = 1,204\,Gbps$.

Nel caso dell'omodina con mixer analogico, lo schema implementato sfrutta le proprietà di quest'ultimo per la selezionare, insieme alle procedure di *processing* digitale, una porzione dello spettro messo a disposizione della pura omodina (evitando in questo modo eventuali interferenze e/o considerare una porzione dello spettro che sia il più piatta possibile).

In questo caso, invece, sono sorti dei problemi per quanto riguarda la caratterizzazione del ricevitore stesso, dove la retta di calibrazione presentava delle variabilità non aspettate (soprattutto se si considera che si utilizza la stessa omodina che era molto stabile con il laser esterno da laboratorio) probabilmente introdotte dal mixer. In particolare, per motivi di tempo non si è testato in dettaglio il mixer, ma direttamente utilizzato.

In termini di QRNG, è stata stimata la *classical min-entropy* di 6,23 bit e si è ottenuto un rate di generazione pari a $R_{omodina,mixer} = 623\,Mbps$. Tuttavia, questo risultato non è da considerarsi affidabile perché, nonostante la distribuzione gaussiana del vuoto quantistico, l'ipotesi di linearità non viene propriamente rispettata a causa delle fluttuazioni citate in precedenza.

A tal proposito, un'analisi e dei test più approfonditi riguardanti il mixer può fare da spunto per un futuro approfondimento di questo lavoro.

Bibliografia

[1] Marco Avesani et al. "Source-device-independent heterodyne-based quantum random number generator at 17 Gbps". In: *Nature Communications* 9.1 (Dec. 2018), p. 5365. ISSN: 2041-1723. DOI: 10.1038/s41467-018-07585-0. URL: https://doi.org/10.1038/s41467-018-07585-0.

[2] Albrecht Böttcher and Bernd Silbermann. *Introduction to large truncated Toeplitz matrices*. Springer Science & Business Media, 2012.

[3] Zhu Cao et al. "Source-independent quantum random number generation". In: *Physical Review X* 6.1 (Feb. 2016), p. 011020. ISSN: 21603308. DOI: 10.1103/PhysRevX.6.011020. arXiv: 1508.04880. URL: https://journals.aps.org/prx/abstract/10.1103/PhysRevX.6.011020.

[4] Christopher Gerry, Peter Knight, and Peter L Knight. *Introductory quantum optics*. Cambridge university press, 2005.

[5] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. "Quantum random number generators". In: *Reviews of Modern Physics* 89.1 (2017). ISSN: 15390756. DOI: 10.1103/RevModPhys.89.015004. arXiv: 1604.03304.

[6] Jan Hilgevoord and Jos Uffink. "The uncertainty principle". In: (2001).

[7] Dirk Jalas et al. "What isand what is notan optical isolator". In: *Nature Photonics* 7.8 (2013), pp. 579–582.

[8] Ulf Leonhardt. *Measuring the quantum state of light*. Vol. 22. Cambridge university press, 1997.

[9] Tommaso Lunghi et al. "Self-testing quantum random number generator". In: *Physical review letters* 114.15 (2015), p. 150501.

[10] Tommaso Lunghi et al. "Self-testing quantum random number generator". In: *Physical Review Letters* 114.15 (Apr. 2015), p. 150501. ISSN: 10797114. DOI: 10.1103/PhysRevLett.114.150501. arXiv: 1410.2790. URL: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.114.150501.

[11] Xiongfeng Ma et al. "Quantum random number generation". In: *npj Quantum Information* 2.1 (2016), pp. 1–9.

[12] L Mandel. "Configuration-space photon number operators in quantum optics". In: *Physical Review* 144.4 (1966), p. 1071.

[13] Davide G Marangon, Giuseppe Vallone, and Paolo Villoresi. "Source-device-independent ultrafast quantum random number generation". In: *Physical review letters* 118.6 (2017), p. 060503.

[14] S. Pironio et al. "Random numbers certified by Bell's theorem". In: *Nature* 464.7291 (2010), pp. 1021–1024. ISSN: 00280836. DOI: 10.1038/nature09008. arXiv: 0911.3427.

[15] Andrew Rukhin et al. *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. Tech. rep. Booz-allen and hamilton inc mclean va, 2001.

[16] Yutaka Shikano. "Unpredictable random number generator". In: *AIP Conference Proceedings*. Vol. 2286. 1. AIP Publishing LLC. 2020, p. 040004.

[17] Victor Shoup. "On fast and provably secure message authentication based on universal hashing". In: *Annual International Cryptology Conference*. Springer. 1996, pp. 313–328.

[18] Francesco Vedovato. *Quantum Methods for ICT*. Vol. 1. Università di Padova, 2021.

Ringraziamenti

Ci tengo a ringraziare il Prof. Vallone per avermi dato la possibilità di conoscere e approfondire argomenti che ritengo molto interessanti e stimolanti, il dottorando Tommaso Bertapelle che mi ha guidata in tutto questo percorso e che ha risposto pazientemente a tutte le mie domande. Inoltre, ringrazio tutte le persone che ho incontrato all'interno del laboratorio Luxor, in particolare il Dr. Francesco Vedovato e il Post-Doc Marco Avesani, i quali mi aiutata e mi hanno fatto scoprire un ambiente lavorativo e di studio in cui si vivono momenti di stima.

Voglio ringraziare i miei genitori che mi hanno permesso di poter affrontare il mio primo percorso universitario, e che mi hanno sostenuto in tutte le mie scelte. Sono stati di vitale importanza per me.

Un ringraziamento speciale lo merita il mio fidanzato Alberto, il quale mi ha supportato in ogni momento, dato forza quando ne avevo più bisogno e gioito per i miei traguardi raggiunti. Ha tutta la mia stima e gli auguro un futuro radioso e colmo di opportunità.

Infine, ringrazio tutte le altre persone che mi hanno accompagnato in questo mio percorso, supportandomi e facendomi capire che la mia persona non è definita solo dall'università, ma che questa è solo un valore aggiunto.