



UNIVERSITÀ
DEGLI STUDI
DI PADOVA



DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

Design optomeccanico di un sistema ottico per QKD in spazio libero

LAUREANDO

Guerrini Alberto

RELATORE

Prof. Vedovato Francesco

CORRELATORE

Dott. Rossi Edoardo

ANNO ACCADEMICO 2022/2023

DATA DI LAUREA: 21/07/2023

Abstract

Le reti per la distribuzione di chiavi quantistiche (QKD) necessitano di collegamenti ottici in free-space per coprire distanze superiori alla portata dei collegamenti in fibra ottica. Nel caso di reti intermodali (IM-QKD) questi due tipi di collegamento sono integrati nella stessa rete ma richiedono l'impiego di trasmettitori e ricevitori ottici in free-space. Il trasmettitore riceve in input un fascio laser in fibra ottica singolo-modo e si occupa di magnificare, collimare ed emettere quest'ultimo. Dopo la propagazione in free-space il ricevitore corregge le perturbazioni dovute alla turbolenza atmosferica e accoppia in fibra ottica singolo-modo il fascio ricevuto. Il gruppo Quantum Future dell'Università di Padova ha progettato un sistema per IM-QKD testato su un link in free-space di 620 metri tra il Dipartimento di Ingegneria dell'Informazione e il Dipartimento di Fisica e Astronomia.

Questa tesi si occupa di progettare un terminale optomeccanico per il sistema di IM-QKD citato precedentemente massimizzando la compattezza, la trasportabilità e l'automazione di alcuni apparati, contenendo i costi. Nello specifico è richiesta la progettazione meccanica dei contenitori, completi di tutti i componenti, utilizzati per trasmettitore e ricevitore ottico e per la strumentazione necessaria al loro corretto funzionamento. Inoltre, è stata svolta l'automazione della correzione tip-tilt di uno specchio a 45° utile per centrare il fascio nell'accoppiamento in fibra ottica massimizzandone l'efficienza. Infine, è stato studiato in laboratorio il funzionamento di quest'ultimo componente per caratterizzarne lo spostamento angolare in funzione del movimento lineare degli attuatori e per determinare la minima risoluzione angolare ripetibile.

Indice

1	Introduzione	1
2	Quantum Key Distribution	3
2.1	Protocollo BB84	4
3	Fasci gaussiani in free-space	7
3.1	Modello dei fasci gaussiani in free-space	7
3.2	Teoria della turbolenza di Kolmogorov	9
3.3	Propagazione in atmosfera e turbolenza	10
3.4	Efficienza di collezione ed accoppiamento in SMF.....	12
4	Link DEI-DFA per QKD in free-space	17
4.1	Descrizione del sistema free-space	17
4.1.1	Trasmittitore	17
4.1.2	Ricevitore	18
4.2	Design meccanico dei contenitori per trasmettitore e ricevitore	19
4.2.1	Scelta dei materiali.....	20
4.2.2	Design e assemblaggio dei componenti meccanici.....	20
5	Automazione tip-tilt di uno specchio a 45°	25
5.1	Design optomeccanico per l'automazione dello stage	25
5.2	Test e caratterizzazione del sistema automatizzato.....	27

1 Introduzione

La sicurezza dei dati e in particolare della loro trasmissione è una preoccupazione fondamentale per individui e aziende. I protocolli di crittografia classica sono stati e sono tuttora responsabili della sicurezza di qualsiasi comunicazione riservata e non solo. Nonostante la ricerca e il continuo miglioramento degli standard di sicurezza e dei protocolli di crittografia, con l'avvento di supercomputer sempre più performanti e della computazione quantistica, le tecniche di crittografia classica possono essere irrimediabilmente compromesse. Ciò è dovuto al fatto che queste tecniche sono basate sull'alta complessità computazionale di alcuni problemi matematici, come la fattorizzazione di numeri primi, problemi per cui il computer quantistico potrebbe velocizzare esponenzialmente la velocità di calcolo, per esempio con tramite l'algoritmo di Shor [1].

Per ovviare a questa vulnerabilità, è stata introdotta nel 1984 la distribuzione quantistica di chiave [2], in inglese Quantum Key Distribution (QKD). Questa tecnica è basata sulle proprietà quantistiche della luce, tra cui l'impossibilità di clonare uno stato quantistico senza alterare lo stato di partenza, il principio di sovrapposizione e il principio di indeterminazione di Heisenberg [3]. Nella QKD un qualsiasi tentativo non autorizzato di misurazione dello stato quantistico di un fotone, influirà inevitabilmente sulle proprietà della particella rendendo rilevabile al ricevitore il tentativo di intercettazione.

Per far sì che la QKD sia correttamente implementata è necessario manipolare e misurare la luce a livello di singolo fotone. Considerando l'elevata attenuazione del segnale che caratterizza i collegamenti in fibra ottica (~ 0.2 dB/km per fibre ottiche telecom singolo-modo), la massima distanza raggiungibile da un sistema di QKD è dell'ordine del centinaio di km per sistemi commerciali oggi disponibili. Per superare tale limitazione ed estendere le distanze raggiungibili è possibile implementare la QKD anche su canali in spazio libero (o *free-space*) tramite telescopi tra due punti a terra, o anche da satellite a terra, come dimostrato recentemente grazie all'utilizzo del satellite Micius lanciato nel 2016 [4].

Un altro punto importante è anche la possibilità di integrare i canali free-space con i canali in fibra ottica, utilizzando una tecnica intermodale (*intermodal QKD*). Il gruppo Quantum Future dell'Università di Padova ha progettato e testato un sistema intermodale fibra ottica/free-space per QKD caratterizzato da canale free-space di circa 620 metri - dalla sede del Dipartimento di Ingegneria dell'Informazione (DEI) alla sede del Dipartimento di Fisica e Astronomia (DFA) - e un collegamento in fibra ottica preinstallato di circa 500 metri tra il DEI e la sede del CNR-INO (Laboratori Luxor). Questo link intermodale fa parte del network in fibra ottica per comunicazioni quantistiche che collega vari dipartimenti e sedi dell'Università, uno dei progetti in corso è la realizzazione di questo link intermodale in modo stabile e automatizzato al fine di rendere più immediato e comodo il suo utilizzo per esperimenti di vario tipo.

Questa tesi quindi si inserisce in questo progetto con due attività utili al suo compimento. La prima consiste nella progettazione meccanica degli alloggiamenti destinati agli apparati trasmettitore e ricevitore del link in free-space che devono garantirne la protezione da agenti atmosferici e l'operatività da remoto. La seconda attività invece si focalizza sull'automazione di alcuni componenti ottici utili a facilitare le operazioni di allineamento e accoppiamento in fibra. Questa seconda attività richiede anche una serie di test per valutare le performance dell'apparato progettato.

2 Quantum Key Distribution

Per comprendere il potenziale dell'applicazione di tecniche di QKD è necessario introdurre uno schema di crittografia a chiave simmetrica chiamato One-Time Pad (OTP) [5]. Questa tecnica è basata sul fatto che le due parti comunicanti, Alice e Bob, dispongano di una chiave, generalmente una sequenza di bit, per criptare e decriptare i messaggi in modo tale che una terza parte, Eve, non sia in grado di ottenere alcuna informazione. La chiave è detta simmetrica se è uguale per entrambe le parti.

Al fine di inviare un messaggio a Bob, Alice cripta il messaggio M_A con la sua chiave K_A ottenendo un messaggio cifrato $C = M_A \oplus K_A$ eseguendo una somma binaria. Il messaggio cifrato è quindi inviato a Bob che può decriptarlo eseguendo a sua volta una somma binaria $M_B = C \oplus K_B$ con la chiave di cui dispone. Si può notare facilmente che, se le due chiavi sono simmetriche, allora il messaggio decriptato da Bob corrisponde a quello inviato da Alice.

Per provare la sicurezza dello schema OTP sono però necessarie alcune assunzioni sulla chiave. Nello specifico quest'ultima deve essere generata in modo *true random*, deve avere lunghezza maggiore o uguale a quella del messaggio da cifrare, non può essere riutilizzata e infine deve essere mantenuta completamente segreta. Considerando inoltre che le due parti sono localizzate nella maggior parte dei casi a distanze considerevoli, questo schema di crittografia risulta essere inutilizzabile nella pratica senza la presenza di un dispositivo che effettui la distribuzione delle chiavi simmetriche.

Di conseguenza l'obiettivo di un sistema per QKD consiste nell'implementazione di un dispositivo che fornisca chiavi sicure alle due parti e che si assicuri che essi non utilizzino chiavi corrotte. Nello specifico è richiesto che le chiavi possedute da Alice e Bob differiscano con probabilità vicina allo zero e che la chiave generata sia casuale in modo uniforme. Inoltre, nel caso in cui un potenziale attacco da parte di Eve venga rilevato, il dispositivo deve necessariamente interrompere la generazione della chiave evitando inoltre di distribuirla alle due parti.

Questo risulta possibile grazie a principi della meccanica quantistica, come la non clonabilità e il fatto che non risulta possibile misurare lo stato di un sistema quantistico

senza alterarne le proprietà in modo irreversibile (principio di Heisenberg). A differenza della teoria dell'informazione classica, in cui le comunicazioni digitali possono essere monitorate e copiate in modo passivo anche senza conoscerne effettivamente il contenuto, nel caso di comunicazioni quantistiche in cui l'informazione è codificata in stati quantistici non ortogonali è possibile quindi ottenere un canale che non permette di copiare l'informazione senza alterarne irreversibilmente il contenuto [2].

2.1 Protocollo BB84

La prima proposta di un protocollo per QKD è stata descritta nel 1984 quando Bennet e Brassard presentarono il BB84 [2]. Questo protocollo si basa sulla codifica di *bit* classici in *qubit* polarizzando i fotoni trasmessi. In breve, il bit 0 (1) viene fatto corrispondere ad un fotone polarizzato orizzontalmente (verticalmente), o ad un fotone polarizzato diagonalmente (antidiagonalmente). La codifica di ogni singolo bit in due possibili stati (orizzontale/diagonale o verticale/antidiagonale) è necessaria per la corretta implementazione del protocollo, che sfrutta quelle che vengono chiamate basi *mutually unbiased*, in questo caso la base orizzontale/verticale e la base diagonale/antidiagonale.

Il protocollo necessita di due canali tra le due parti comunicanti (Figura 1). Il primo deve essere un canale quantistico pubblico in cui le due parti inviano segnali quantistici (ovvero si scambiano fotoni) e su cui possono essere effettuate da parte di Eve tutte le possibili operazioni di intercettazione attiva permesse dalle leggi della Meccanica Quantistica. Il secondo invece deve essere un canale classico autentificato, che può essere soggetto ad intercettazioni passive, ed è utilizzato per permettere alle due parti di proseguire con le varie fasi del protocollo, ad esempio trasmettere informazioni utili a verificare la presenza di perturbazioni, e di conseguenza intercettazioni, sul canale quantistico.

Il protocollo consiste in due fasi principali: trasmissione quantistica e post-processing classico. La prima fase prevede la preparazione degli stati quantistici da parte di Alice, la loro trasmissione attraverso il canale e infine la loro ricezione e misurazione da parte di Bob.

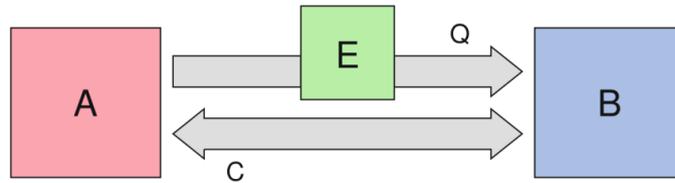


Figura 1: Rappresentazione di uno schema di comunicazione per il protocollo BB84 dove sono rappresentate le due parti Alice (A) e Bob (B) e un eventuale avversario Eve (E). Sono poi rappresentati i canali quantistico (Q) e classico (C).

La seconda fase invece è finalizzata a produrre una chiave sicura per Alice e Bob a partire dalla sequenza di bit correlati e insicuri che ottengono nella prima fase e si basa su una serie di procedure che richiedono trasmissioni sul canale classico. Una procedura è l'*error correction*, in cui vengono corretti i possibili errori tra le due stringhe di bit, seguita dalla procedura di *privacy amplification*, in cui si tiene conto dell'eventuale flusso di informazione verso Eve per far sì che le due stringhe siano anche sicure.

Per codificare i bit in qubit viene utilizzata la polarizzazione dei fotoni. La parte che deve codificare i bit, supponiamo Alice, può farlo utilizzando la base orizzontale/verticale $\{H, V\}$ oppure quella diagonale/antidiagonale $\{+45^\circ, -45^\circ\}$.

Per iniziare la fase di trasmissione quantistica, Alice genera due sequenze casuali di uguale lunghezza M . La prima, S_A contiene gli M bit che formano la stringa di Alice, mentre la seconda specifica, per ogni bit, la base con cui codificarlo. Successivamente, i fotoni preparati secondo la sequenza S_A vengono inviati tramite il canale quantistico. Quando Bob riceve la sequenza, sceglie in modo indipendente da Alice una sequenza casuale di M basi con cui decodificare i qubit, e ottiene una sequenza S_B di bit dalla misurazione della polarizzazione dei fotoni inviati da Alice. Alla fine di questa fase entrambe le parti dispongono di una sequenza, S_A e S_B rispettivamente, che viene chiamata *raw key*. Questa sequenza viene poi data in input al post-processing.

Nella fase di post-processing, la prima operazione detta *sifting* si svolge come segue. Bob annuncia sulla connessione classica la sequenza di basi utilizzate per la decodifica. Alice può quindi rispondere identificando quali di queste basi coincidono. In tutti i casi in cui le due basi non coincidono, i relativi bit vengono scartati da entrambe le sequenze S_A e S_B ottenendo una coppia di chiavi K_A e K_B di lunghezza $N \leq M$.

Considerando che la scelta delle basi è puramente casuale è facile notare che generalmente si ha $N \approx M/2$.

Successivamente si esegue la stima del tasso di errore sul canale quantistico. Le due parti confrontano alcuni bit delle chiavi comunicando sul canale classico. Questi bit sono scelti in modo casuale e sono scartati in seguito a questo passaggio per non compromettere la sicurezza della chiave. Nel caso di un'eventuale intercettazione da parte di Eve, ci si aspetta di rilevare un alto tasso di errore. In questa fase è quindi possibile identificare qualsiasi intervento (significativo) non autorizzato sul canale quantistico, semplicemente valutando il tasso di errore.

Infine, la fase di post-processing termina con le attività di *error correction* e di *privacy amplification* effettuate sulla chiave fornita in output dalla stima del tasso di errore.

Dopo aver compiuto interamente le fasi di trasmissione quantistica e post-processing, il protocollo BB84 fornisce in output una chiave segreta simmetrica ad entrambe le parti che può essere utilizzata per crittografare le comunicazioni su un canale classico, ad esempio sfruttando il protocollo OTP.

3 Fasci gaussiani in free-space

La comunicazione ottica fra trasmettitore e ricevitore nei link in free-space per QKD, avviene mediante l'utilizzo di fasci laser. Per lo scopo di questa tesi risulta quindi utile trattare da un punto di vista teorico la propagazione di un fascio gaussiano in free-space in quanto rappresenta la miglior approssimazione della propagazione di un fascio laser. Considerando inoltre che il mezzo attraverso cui si propaga il fascio nel link DEI-DFA, ovvero l'atmosfera, è affetto da turbolenza, risulta utile trattare anche gli effetti di quest'ultima sulla propagazione del fascio laser.

3.1 Modello dei fasci gaussiani in free-space

In assenza di turbolenza il fascio luminoso prodotto da un laser è ben modellizzato da un fascio Gaussiano. La propagazione di un fascio Gaussiano monocromatico $U(r, z)$, dove $r := \sqrt{x^2 + y^2}$ con (x, y) il sistema di coordinate trasverse e z la coordinata dell'asse di propagazione, è una delle soluzioni dell'equazione di Helmholtz considerando l'approssimazione a onde parassiali:

$$\nabla^2 U + k^2 U = 0 \quad (1)$$

Con $k = 2\pi/\lambda$ il numero d'onda e λ la lunghezza d'onda.

Ponendosi nel caso di un trasmettitore senza ostruzioni, il campo ottico di un fascio gaussiano all'apertura del trasmettitore ($z = 0$) risulta essere

$$U(r, 0) = A_0 \exp\left\{-\left(\frac{1}{W_0^2} + \frac{ik}{2R_0}\right)r^2\right\} \quad (2)$$

dove W_0 è la cintura (*waist*) del fascio e R_0 il raggio di curvatura del fronte d'onda entrambi misurati all'apertura del trasmettitore [6].

Considerando il caso di un fascio collimato al trasmettitore, ovvero in cui il fronte d'onda è piano, si ha che $R_0 = +\infty$ rendendo trascurabile la componente immaginaria dell'Equazione (2).

Il campo di un fascio collimato dopo una propagazione di distanza z è dato da

$$U(r, z) = A_0 \frac{W_0}{W(z)} \exp\{-ikz + i\zeta(z)\} \exp\left\{-\left(\frac{1}{W^2(z)} + \frac{ik}{2R(z)}\right)r^2\right\} \quad (3)$$

Dove il parametro $\zeta(z) = \tan^{-1}\left(\frac{z}{z_0}\right)$ è il ritardo longitudinale della fase dell'onda, mentre il raggio della dimensione dello spot $W(z)$ e il raggio di curvatura del fronte d'onda $R(z)$ del fascio propagato sono ottenuti nel seguente modo:

$$W(z) = W_0 \sqrt{1 + \left(\frac{z}{z_0}\right)^2} \quad (4)$$

$$R(z) = z \left[1 + \left(\frac{z_0}{z}\right)^2 \right] \quad (5)$$

Va notato che la minima larghezza del fascio è W_0 , ovvero la larghezza che si può misurare all'origine dell'asse di propagazione z , sempre sotto l'ipotesi di fascio collimato.

Infine, il parametro z_0 è chiamato lunghezza di Rayleigh ed è definito come

$$z_0 = \frac{\pi W_0^2}{\lambda} \quad (6)$$

È rilevante notare che z_0 assume il valore della distanza z lungo l'asse di propagazione in cui l'area della sezione del fascio è duplicata rispetto alla minima area del fascio, ovvero in $z = 0$ per un fascio collimato.

Un fascio Gaussiano ammette l'onda sferica e l'onda piana come casi limiti, utilizzando la distanza di Rayleigh come discriminante: per valori di $z \ll z_0$ si può approssimare il fascio ad un'onda piana, mentre ad un'onda sferica per $z \gg z_0$ [7].

È inoltre possibile definire un angolo di divergenza del fascio

$$\vartheta_0 = \frac{\lambda}{\pi W_0} = \frac{W_0}{z_0} \quad (7)$$

il quale risulta inversamente proporzionale dalla larghezza del fascio e direttamente proporzionale alla lunghezza d'onda.

Si deve però considerare che questa relazione vale solamente sotto le ipotesi di assenza di turbolenza e per distanze $z \gg z_0$. È quindi possibile approssimare la larghezza del fascio per $z \gg z_0$ nel seguente modo

$$W(z) \approx \vartheta_0 z \quad (8)$$

In Figura 2 è possibile notare come l'intensità del fascio Gaussiano si disperda su un'area maggiore all'aumentare della distanza lungo l'asse di propagazione.

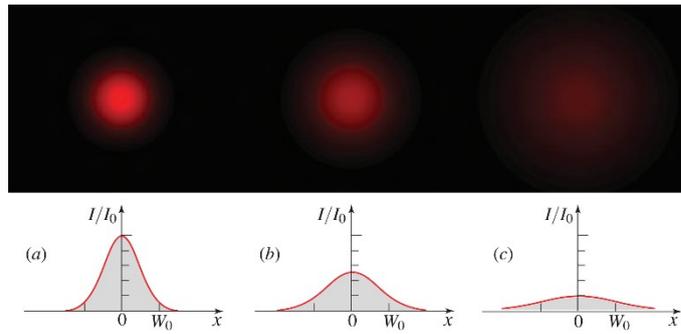


Figura 2: Intensità normalizzata di un fascio gaussiano in funzione della distanza radiale x a diverse distanze lungo l'asse z : a) $z = 0$, b) $z = z_0$, c) $z = 2z_0$.

3.2 Teoria della turbolenza di Kolmogorov

La turbolenza atmosferica è causata da fluttuazioni casuali della velocità di un fluido viscoso, nel caso di nostro interesse l'aria. Esse sono normalmente dovute a piccole variazioni di temperatura e causano a loro volta piccole variazioni della densità atmosferica, e infine dell'indice di rifrazione.

Studiando la differenza quadratica media della velocità del vento in due punti nello spazio, Kolmogorov propose la seguente forma per la funzione di struttura della velocità del vento

$$D_v(r) := \langle (v_1 - v_2)^2 \rangle = C_v^2 r^{2/3} \quad \text{per } l_0 \leq r \leq L_0 \quad (9)$$

Il parametro C_v^2 è la costante di struttura della velocità mentre r è la distanza tra i due punti nello spazio considerati. Va notato che questa equazione è valida per valori di r compresi tra la dimensione minima e massima, l_0 e L_0 rispettivamente, delle variazioni casuali della velocità del vento, tipicamente assunte essere 0 e $+\infty$ per facilitare la discussione.

Assumendo la stessa legge di potenza è possibile definire la funzione di struttura dell'indice di rifrazione

$$D_n(r) = C_n^2 r^{2/3} \quad (10)$$

Con C_n^2 la costante di struttura dell'indice di rifrazione. Questa equazione risulta di maggiore importanza nei casi in cui viene trattata la propagazione di un fascio luminoso attraverso l'atmosfera.

Trattando l'indice di rifrazione come un campo aleatorio

$$n(\mathbf{R}, t) \approx 1 + \delta n(\mathbf{R}, t) \quad (11)$$

con \mathbf{R} la distanza relativa tra i due punti e δn le fluttuazioni casuali dell'indice di rifrazione, è possibile provare che

$$D_n(r) = 2[B_n(0) - B_n(r)] \quad (12)$$

dove $B_n(r)$ è una funzione di covarianza. Applicando successivamente a $B_n(r)$ la trasformata di Fourier si ottiene un risultato largamente utilizzato nel calcolo teorico della turbolenza che descrive la densità spettrale di potenza per le fluttuazioni dell'indice di rifrazione come

$$\Phi_n(\kappa) = 0.033 C_n^2 \kappa^{-11/3} \quad \text{con } \frac{1}{L_0} \leq \kappa \leq \frac{1}{l_0} \quad (13)$$

dove κ è una frequenza spaziale. L'Equazione (13) è nota come spettro di Kolmogorov per la turbolenza atmosferica.

3.3 Propagazione in atmosfera e turbolenza

Nel caso di propagazione del fascio in aria, come nel caso del link DEI-DFA, è necessario utilizzare un modello che consideri anche gli effetti introdotti dalla turbolenza sulla propagazione del fascio luminoso.

Si risolve quindi l'equazione di Helmholtz (Equazione (1)) considerando anche le fluttuazioni dell'indice di rifrazione [7] che risulta

$$\nabla^2 U + k^2 n^2(R)U = 0 \quad (14)$$

Non esistendo una soluzione esatta dell'Equazione (14), uno dei metodi più utilizzati per determinare una soluzione approssimata sotto l'assunzione di fluttuazioni deboli è il metodo di Rytov [6], per cui il campo è approssimato come

$$U(r, L) = U_0(r, L)e^{\varphi(r, L)} \quad (15)$$

dove $U_0(r, L)$ è l'onda ottica in free-space dopo una lunghezza di propagazione L e $\varphi(r, L)$ è una perturbazione di fase complessa dovuta alla turbolenza.

Uno degli effetti della propagazione in atmosfera di un fascio è il cosiddetto allargamento del fascio (*beam broadening*).

Si può riscrivere la larghezza del fascio descritta dall'Equazione (4) considerando anche gli effetti della turbolenza come

$$W(L) = \sqrt{W_0^2 + L^2 \theta^2} \quad (16)$$

Dove θ è la divergenza totale del fascio ed è data dalla divergenza in condizioni ideali θ_0 sommata alla divergenza data dall'atmosfera θ_{atm}

$$\theta = \sqrt{\theta_0^2 + \theta_{atm}^2} \quad (17)$$

$$\theta_{atm} = \frac{\lambda}{\pi \rho_0} \quad (18)$$

È importante notare inoltre che nel calcolo della divergenza totale in caso di $L \gg 1$ il termine dovuto alla turbolenza atmosferica risulta dominante rispetto alla divergenza intrinseca in condizioni ideali [8].

Di conseguenza aumentare la larghezza del fascio al trasmettitore non limita in modo considerevole la divergenza. Nell'Equazione (18) il termine ρ_0 è una grandezza che misura la distanza di coerenza nel piano trasverso rispetto alla direzione di propagazione: due punti separati di una distanza maggiore di ρ_0 sono considerati incoerenti. Per un fascio Gaussiano senza turbolenza ρ_0 può essere considerato infinito, mentre per un fascio che si propaga nella turbolenza ρ_0 può assumere valori anche di pochi centimetri. In ambito astronomico e di ottica adattiva tipicamente si fa riferimento al *parametro di Fried* r_0 , legato a ρ_0 con $r_0 = 2.1\rho_0$.

Un altro importante effetto della propagazione attraverso l'atmosfera è l'introduzione di aberrazioni del fronte d'onda. Per descrivere il fronte d'onda istantaneo al telescopio ricevitore è possibile decomporre lo stesso in polinomi di Zernike, che sono tra di essi ortogonali rispetto al cerchio unitario

$$\varphi(r, \theta, t) = b_0 Z_0 + \sum_{j=1}^{\infty} b_j(t) Z_j \left(\frac{2r}{D_{Rx}}, \theta \right) \equiv \sum_{j=0}^{\infty} b_j(t) Z_j \quad (19)$$

La convenzione OSA/ANSI impone che j parta da 0 e l'utilizzo delle coordinate (r, θ) alla pupilla di entrata del telescopio ricevente [7]. I termini b_j sono i coefficienti di Zernike che pesano i relativi polinomi e ne quantificano l'intensità. I primi ordini di aberrazione sono descritti in Figura 3.

j	Aberration name	$Z_j(\rho, \varphi)$	
0	Piston	1	
1	Y-tilt	$2\rho \sin \varphi$	
2	X-tilt	$2\rho \cos \varphi$	
3	Oblique astigmatism	$\sqrt{6}\rho^2 \sin 2\varphi$	
4	Defocus	$\sqrt{3}(2\rho^2 - 1)$	
3	Vertical astigmatism	$\sqrt{6}\rho^2 \cos 2\varphi$	

Figura 3: Primi polinomi di Zernike fino al grado $j=3$.

Risulta quindi utile considerare la varianza dei coefficienti di Zernike

$$\langle b_j^2 \rangle = \langle b_{n,m}^2 \rangle = \left(\frac{D_{Rx}}{r_0} \right)^{\frac{5}{3}} \frac{n+1}{\pi} \frac{\Gamma\left(n - \frac{5}{6}\right) \Gamma\left(\frac{23}{6}\right) \Gamma\left(\frac{11}{6}\right) \sin\left(\frac{5}{6}\pi\right)}{\Gamma\left(n + \frac{23}{6}\right)} \quad (20)$$

Dove r_0 è il parametro di Fried, mentre la conversione tra gli indici (n, m) e j è ottenuta come $j = \frac{n(n+2)+m}{2}$. Si può quindi notare che la varianza dei coefficienti di Zernike è proporzionale al rapporto tra il diametro del telescopio ricevente e il parametro di Fried e il contributo dato dai diversi modi di Zernike decresce all'aumentare di n [9].

3.4 Efficienza di collezione ed accoppiamento in SMF

La divergenza del fascio in un link ottico è di importanza per la valutazione dell'efficienza di collezione al ricevitore η_{Rx} . Nel caso dell'utilizzo di un telescopio ricevente senza ostruzioni, come per il link considerato in questa tesi, e con apertura di diametro D_{Rx} finito vale la seguente relazione

$$\eta_{Rx} = 1 - \exp\left(-\frac{1}{2} \frac{D_{Rx}^2}{W^2(L)}\right) \quad (21)$$

Nel grafico in Figura 4 sono rappresentate delle stime di perdita in efficienza di collezione per il link DEI-DFA in funzione della lunghezza del link e per diversi valori di C_n^2 . Con l'apertura del telescopio ricevente $D_{Rx} = 2''$ e la larghezza del fascio al trasmettitore $W_0 = 25 \text{ mm}$ [10].

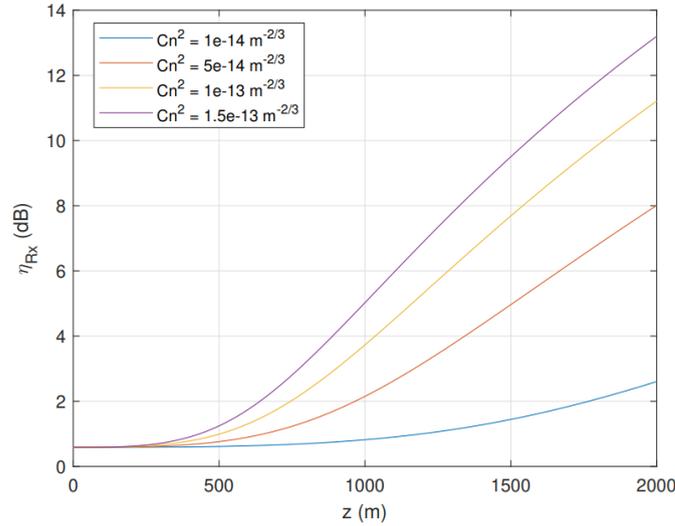


Figura 4: Stime dell'efficienza di collezione per il link DEI-DFA in funzione della distanza del link z e per diversi valori della costante di struttura dell'indice di rifrazione.

Trascurando la scintillazione atmosferica, l'efficienza di accoppiamento in SMF può essere descritta come

$$\eta_{SMF} = \eta_0 \eta_{AO} \quad (22)$$

dove il termine η_0 descrive l'efficienza ottica al ricevitore mentre η_{AO} l'efficienza data dall'ottica adattiva.

L'efficienza ottica al ricevitore può essere stimata trascurando gli effetti della turbolenza atmosferica essendo data dalla differenza tra il modo del campo all'ingresso del telescopio ricevente e quello all'ingresso della SMF. Il seguente risultato può essere utilizzato per determinarne il valore

$$\eta_0 = 2 \left[\frac{\exp(-\beta^2) - \exp(-\beta^2 \alpha^2)}{\beta \sqrt{1 - \alpha^2}} \right] \quad (23)$$

dove il parametro α è il rapporto tra il diametro dell'ostruzione e il diametro dell'apertura del telescopio, mentre $\beta = \frac{\pi D_{Rx} MFD}{4\lambda f}$ con MFD il mode-field-diameter della fibra può essere ottimizzato per ottenere l'efficienza ottica al ricevitore richiesta (Figura 5).

Dall'Equazione (23) si può derivare che per $\alpha = 0$ il valore ottimo è $\beta_{opt} = 1.12$ per ottenere la un'efficienza pari all' 81.5%. Questo valore è associato alla massima efficienza ottica possibile al ricevitore.

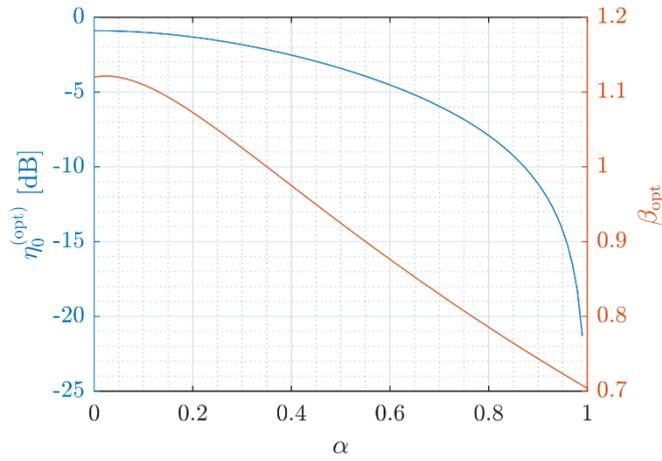


Figura 5: Massima efficienza di accoppiamento in SMF e valore ottimo di β in funzione del rapporto di oscurazione α [8].

Il termine relativo all'efficienza relativa all'ottica adattiva è descritto come

$$\eta_{AO} = e^{-\sigma_{res}^2} \quad (24)$$

Dove σ_{res}^2 è l'errore residuo del fronte d'onda dopo che esso è stato perfettamente corretto dal sistema di ottica adattiva (AO) fino al modo di Zernike J_{max} , e può essere definito come

$$\sigma_{res}^2 := \sum_{j=J_{max}+1}^{\infty} \langle b_j^2 \rangle \quad (25)$$

La valutazione del valore di J_{max} può essere effettuata seguendo il criterio di Rayleigh per valutare l'impatto di una particolare aberrazione sulla qualità del sistema ottico. Il suddetto criterio afferma che, se la RMS della differenza tra un fronte d'onda aberrato e un fronte d'onda ideale è inferiore a $0,05\lambda$, allora le prestazioni del sistema aberrato sono virtualmente indistinguibili da quelle di un sistema non aberrato [8]. In Figura 6 è possibile notare il limite dato dal criterio di Rayleigh e va interpretato come segue. Prendendo ad esempio il caso $\frac{D_{Rx}}{r_0} = 1$, il criterio definisce che è sufficiente correggere fino al modo $J_{max} = 2$ per avere performance idealmente equivalenti ad un fascio non aberrato, cosa che si può ottenere anche correggendo solo per il tip-tilt, ovvero utilizzando uno specchio tipo fast-steering-mirror al ricevitore.

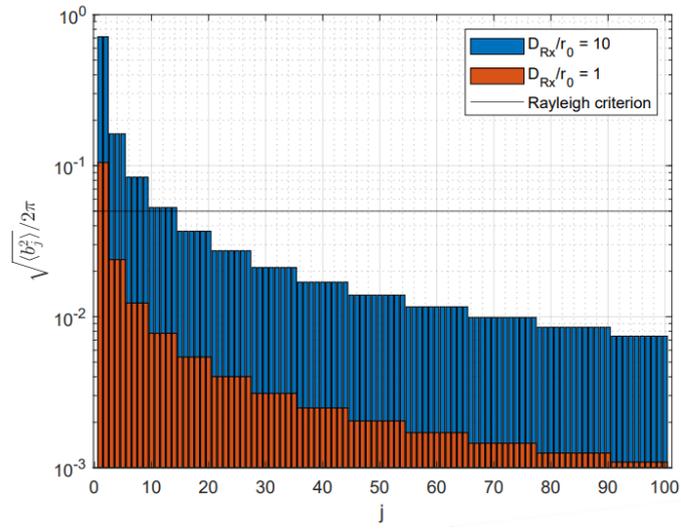


Figura 6: Varianza dei coefficienti di Zernike in funzione dell'ordine j con indicato il limite del criterio di Rayleigh

4 Link DEI-DFA per QKD in free-space

La realizzazione del link stabile DEI-DFA necessita primariamente del sistema ottico di comunicazione in free-space realizzato dal gruppo Quantum Future e della progettazione di una soluzione compatta, trasportabile e low-cost per contenere il sistema ottico e la relativa strumentazione. Al fine di fornire una visione generale, in questo capitolo innanzitutto si descrive il sistema ottico utilizzato e successivamente le attività di progettazione dei contenitori per il sistema stesso di cui mi sono occupato.

4.1 Descrizione del sistema free-space

Il sistema ottico per comunicazioni free-space utilizzato è stato progettato per lavorare entro distanze di 2 km, sfruttando componenti ottici disponibili in commercio. I telescopi principali di trasmettitore e ricevitore sono basati su ottiche da 2 pollici (50.8 mm) mentre gli altri componenti utilizzati sono da 1 pollice. Al fine di operare anche durante il giorno e di sfruttare l'infrastruttura in fibra ottica preesistente, la lunghezza d'onda del fascio utilizzato per QKD è stata scelta a $\lambda = 1550 \text{ nm}$ nella banda telecom C.

Il fascio al trasmettitore è caratterizzato da una larghezza $W_0 = 24 \text{ mm}$, mentre il valore della costante di struttura dell'indice di rifrazione misurata durante il test di questo link è $C_n^2 = 1.15 \cdot 10^{-13} \text{ m}^{-2/3}$. Con questi dati, la perdita in efficienza del canale è risultata pari a 14 dB, con $\eta_{Rx} = 2 \text{ dB}$ ottenuta con l'Equazione (21) e $\eta_{SMF} = 12 \text{ dB}$ dall'Equazione (22) [10].

Oltre al fascio a $\lambda = 1550 \text{ nm}$, utilizzato per QKD, il sistema ottico free-space necessita di altri due fasci laser. Il primo, con una lunghezza d'onda $\lambda = 980 \text{ nm}$, è utilizzato per l'allineamento *fine* dei due telescopi, mentre il secondo, con $\lambda = 1545 \text{ nm}$, è utilizzato per monitorare in real-time l'efficienza di accoppiamento in fibra.

4.1.1 Trasmettitore

Come accennato, il trasmettitore è caratterizzato da un telescopio principale con ottiche da 2 pollici (Figura 7.a), che è utilizzato per produrre un fascio gaussiano collimato di larghezza $W_0 \approx 24 \text{ mm}$, all'incirca metà dell'apertura ottica dei telescopi

utilizzati. Sul fuoco posteriore del telescopio principale è posto un adattatore FC/PC (*Fiber Connector/Physical Contact*) utilizzato per propagare in free-space il fascio convogliato dal cavo in fibra ottica entrante nel trasmettitore (Figura 7.b). Questo adattatore è montato su un traslatore lineare (lungo l'asse z) automatizzato da un attuatore. In questo modo è possibile un più preciso posizionamento del terminatore della fibra ottica sul fuoco del telescopio principale (Figura 7.c). Infine, una camera CMOS con la relativa ottica è stata assemblata al trasmettitore per effettuare l'allineamento *coarse* (Figura 7.d). L'intero sistema ottico è stato assemblato in un sistema *caged* per garantirne la stabilità, la compattezza e l'agganciamento ad una montatura mobile utilizzata per l'attuazione dell'allineamento *coarse*.

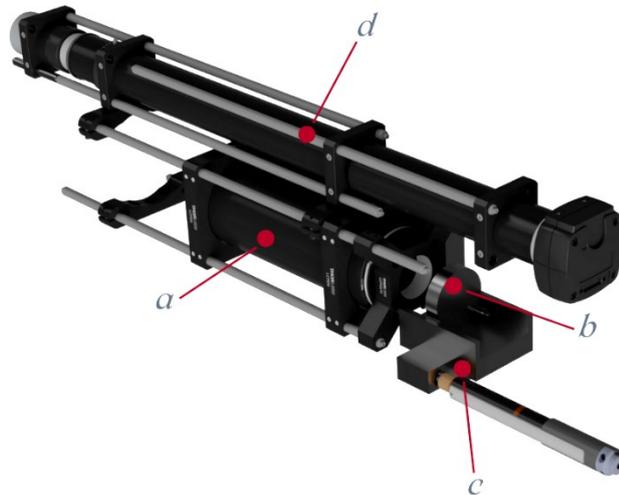


Figura 7: Render del sistema ottico al trasmettitore. a) Telescopio principale, b) Adattatore FC/PC, c) Stage lineare automatizzato per la messa a fuoco, d) Camera CMOS e ottiche per l'allineamento *coarse*.

4.1.2 Ricevitore

Allo stesso modo, anche il ricevitore è caratterizzato da un telescopio principale con ottiche da 2 pollici (Figura 9.a) che applica al fascio una riduzione $6\times$. Al termine del tubo ottico che contiene le ottiche del telescopio principale è posizionato un *fast-steering-mirror* (FSM) (Figura 9.b) utilizzato per la correzione adattiva dell'angolo di arrivo (AoA) del fascio, dovuto alla turbolenza del mezzo atmosferico. Successivamente i fasci entranti attraversano uno specchio dicroico (DM) (Figura 9.c) utilizzato per separare il fascio a $\lambda = 980\text{ nm}$ per l'allineamento *fine* dagli altri fasci. Questo fascio è quindi direzionato, attraverso una lente di focale $f = 300\text{ mm}$, verso un sensore di posizione (PSD) (Figura 9.d) che è utilizzato per il controllo in feedback

del FSM. I due fasci rimanenti sono quindi riflessi da uno specchio a 45° (Figura 9.e) e infine accoppiati in SMF tramite un adattatore FC/PC (Figura 9.f). Come nel caso del trasmettitore, una camera CMOS è stata assemblata al sistema ricevitore per effettuare l'allineamento *coarse* (Figura 9.g).

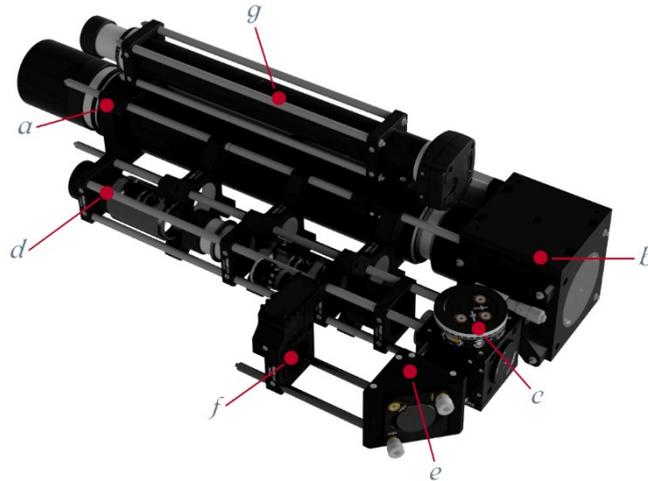


Figura 8: Render del sistema ottico al ricevitore. a) Telescopio principale, b) FSM per la correzione fine tip-tilt, c) DM, d) PSD, e) Specchio a 45°, f) Adattatore FC/PC, g) Camera CMOS e ottiche per l'allineamento coarse.

4.2 Design meccanico dei contenitori per trasmettitore e ricevitore

La necessità di rendere stabile il link DEI-DFA per effettuare esperimenti di IM-QKD implica la progettazione degli alloggiamenti per contenere il trasmettitore, il ricevitore e la relativa strumentazione che ne garantisce il corretto funzionamento. Nello specifico è necessario trattare la scelta dei componenti che formano i contenitori, la loro eventuale modifica, il loro assemblaggio e infine l'automazione di alcuni componenti meccanici per garantire l'operatività con controllo a distanza.

I due contenitori per trasmettitore e ricevitore differiscono solo nelle dimensioni in quanto l'ingombro del sistema ottico al ricevitore è maggiore. Di conseguenza le fasi di design risultano pressoché identiche e per questo motivo la loro descrizione nei seguenti paragrafi è generica dal punto di vista di trasmettitore e ricevitore. Nei casi che lo richiedono, eventuali dissimilarità tra i due contenitori sono descritte in dettaglio.

Il design meccanico è stato interamente svolto con il supporto del software CAD Fusion 360 sviluppato da Autodesk, e basandosi su alcuni progetti prodotti per il link Montegrande-DEI dal gruppo Quantum Future. Inoltre, sono stati utilizzati i modelli CAD dei componenti Thorlabs e Rittal resi disponibili dai relativi produttori.

4.2.1 Scelta dei materiali

Il collegamento ottico in free-space deve essere installato in ambiente outdoor, più precisamente il trasmettitore verrà posto all'esterno della torre appartenente al Dipartimento di Fisica e Astronomia (DFA), mentre il ricevitore sarà posizionato sul tetto del Dipartimento di Ingegneria dell'Informazione (DEI). Prevedendo quindi che i contenitori saranno esposti ad agenti atmosferici per un periodo di tempo indeterminato, la progettazione deve tener conto di alcuni requisiti vitali per limitarne il deterioramento e soprattutto per evitare il danneggiamento della strumentazione contenuta.

A questo fine, la scelta dei materiali utilizzati per i contenitori deve restringersi a quelle leghe che non subiscono ossidazione o corrosione dovute ad agenti atmosferici. Si è quindi optato per l'acciaio inossidabile e l'alluminio: il primo per i componenti sui quali gravano maggiormente il carico e le sollecitazioni, il secondo invece per i componenti meccanici mobili o che devono avere una massa contenuta.

Le scatole utilizzate sono destinate per l'uso all'esterno e certificate con un grado di protezione IP66 contro polvere e spruzzi d'acqua ad alta pressione, il che le rende adatte per lo scopo di questo progetto.

4.2.2 Design e assemblaggio dei componenti meccanici

Il design dei contenitori segue una procedura sequenziale, partendo da una scatola standard effettuando ad essa lavorazioni per poter installare i componenti necessari.

Le scatole utilizzate sono i modelli AX1339 e AX1360, rispettivamente per trasmettitore e ricevitore, prodotti dall'azienda Rittal e destinate all'alloggiamento di apparecchiature elettriche. Sono dotate di un coperchio con serratura che per il fine di questo progetto è orientato sulla faccia superiore.

In Figura 9 e Figura 10 è possibile trovare i render dei contenitori progettati per contenere rispettivamente il trasmettitore e il ricevitore. Per esplicitare il possibile

funzionamento dello shutter meccanico, esso è raffigurato in posizione aperta nel primo caso, mentre in posizione chiusa nel secondo.

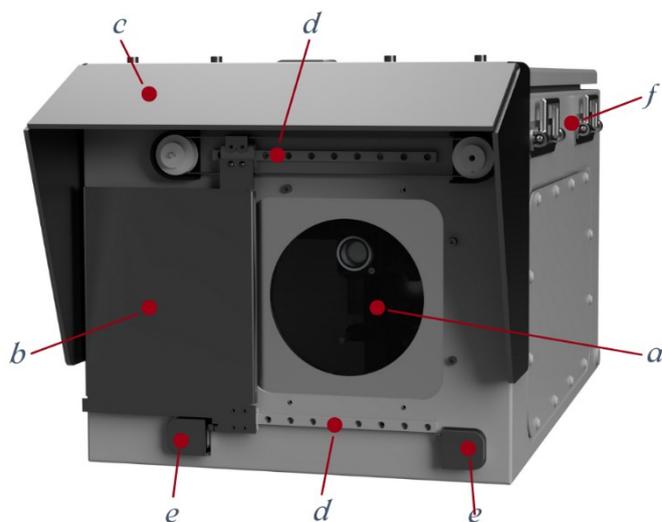


Figura 9: Render del contenitore progettato per il trasmettitore, con shutter meccanico aperto. a) Finestra ottica, b) Shutter meccanico, c) Tettoia superiore e laterale, d) Sistema motorizzato per la movimentazione dello shutter, e) Finecorsa per la movimentazione dello shutter.

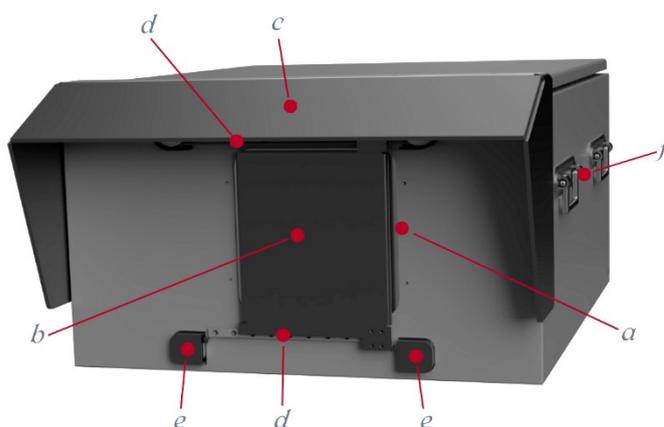


Figura 10: Render del contenitore progettato per il ricevitore, con shutter meccanico chiuso. a) Finestra ottica, b) Shutter meccanico, c) Tettoia superiore e laterale, d) Sistema motorizzato per la movimentazione dello shutter, e) Finecorsa per la movimentazione dello shutter.

La prima modifica da effettuare è l'installazione di una finestra ottica sul fronte della scatola per permettere le operazioni di trasmissione e ricezione (Figura 9.a). Il telaio per la finestra ottica è ottenuto dalla lavorazione di due lastre in alluminio. Tra le lastre è poi posizionata la finestra ottica in vetro di geometria circolare e diametro 150 mm, con l'aiuto di due o-ring, utili sia per garantire l'impermeabilità dell'installazione che per evitare il danneggiamento della finestra stessa. È inoltre necessario effettuare un foro di geometria simile al telaio della finestra ottica sulla faccia frontale della

scatola. Infine, la finestra ottica è installata nell'alloggiamento fissando il supporto in alluminio precedentemente descritto mediante l'utilizzo di viti passanti.

Per proteggere la finestra ottica dalle intemperie come pioggia o grandine, è necessaria la progettazione di uno shutter meccanico (Figura 9.b, Figura 10.b) che copra la finestra quando l'apparato non è in funzione e di una tettoia (Figura 9.c, Figura 10.c) che protegga superiormente e lateralmente la faccia frontale del contenitore. Quest'ultima è necessaria per evitare che la finestra ottica, lo shutter e i relativi meccanismi siano esposti alle intemperie.

Lo shutter è ottenuto da taglio e piegatura di una lamiera di alluminio di spessore 2.0 mm. Il suo design ne massimizza la capacità di proteggere la finestra anche da schizzi provenienti da direzioni parallele al piano della finestra ottica stessa. La lamiera è fissata a due carrelli a guide lineari, posti sul lato superiore e inferiore che ne garantiscono la traslazione per l'apertura e la chiusura. Al fine di agevolarne la sua movimentazione, si è cercato di limitarne l'ingombro e la sua massa.

Un sistema meccanico formato da un motore stepper brushless, due pulegge e una cinghia sincroni è installato lungo la guida superiore per automatizzare l'apertura e chiusura dello shutter (Figura 9.d, Figura 10.d). Il motore trasmette il moto ad una puleggia che a sua volta aziona la cinghia. Quest'ultima è fissata al carrello superiore. La massa limitata e le dimensioni ridotte dello shutter, e la tecnologia a sfere dei carrelli permettono uno scorrimento fluido dell'assemblato senza necessità di applicare il moto anche al carrello inferiore. Per limitare l'azione del motore, due finecorsa sono installati agli estremi della guida inferiore (Figura 9.e, Figura 10.e). Essi consistono in due semplici switch azionati dal carrello non appena raggiunge il fine della sua corsa. Per proteggere pulegge e switch sono stati disegnate delle coperture ad-hoc stampabili in 3D. Non è da trascurare la necessità di effettuare dei fori sulla scatola per poter fissare nella corretta posizione guide, pulegge, motore e switch.

La tettoia è realizzata a partire da una lastra di alluminio di spessore 4.4 mm utilizzando tagli e piegature. Essa è fissata mediante bulloni passanti sulla parte frontale della faccia superiore del coperchio della scatola. In questo modo si garantisce la corretta apertura di quest'ultimo.

Ulteriori minime lavorazioni consistono nell'installazione di maniglie, di un foro passacavi posteriore e dei fori necessari per fissare in posizione l'apparato. Le prime sono installate sulle facce laterali della scatola per permetterne la movimentazione in modo agevole, impegnando non più di due persone. Il foro passacavi è posizionato sulla faccia posteriore ed è necessario per i cavi di alimentazione dei componenti all'interno del contenitore e della SMF che veicola il fascio dal dispositivo per QKD al trasmettitore/ricevitore. Infine, i fori per il fissaggio sono stati effettuati sulla base della scatola per garantirne un corretto fissaggio.

Di seguito sono riportati i render degli apparati trasmittente e ricevente completi di telescopi e strumentazione necessaria.



Figura 11: Render dell'apparato trasmittente con vista all'interno del contenitore. a) Telescopio ricevitore, b) Mount alt-azimut motorizzata, c) Supporto finestra ottica, d) Motore stepper per automazione shutter.

Da questa prospettiva è possibile notare l'installazione della mount giroscopica *altitude-azimuth* utilizzata per l'allineamento *coarse* dei due telescopi (Figura 11.b, Figura 12.b), il design e l'assemblaggio del supporto per la finestra ottica, e la finestra ottica stessa (Figura 11.c, Figura 12.c), il motore DC stepper utilizzato per automatizzare l'apertura e la chiusura dello shutter meccanico (Figura 11.d, Figura 12.d) e infine il passacavi sul retro delle scatole (Figura 12.e).

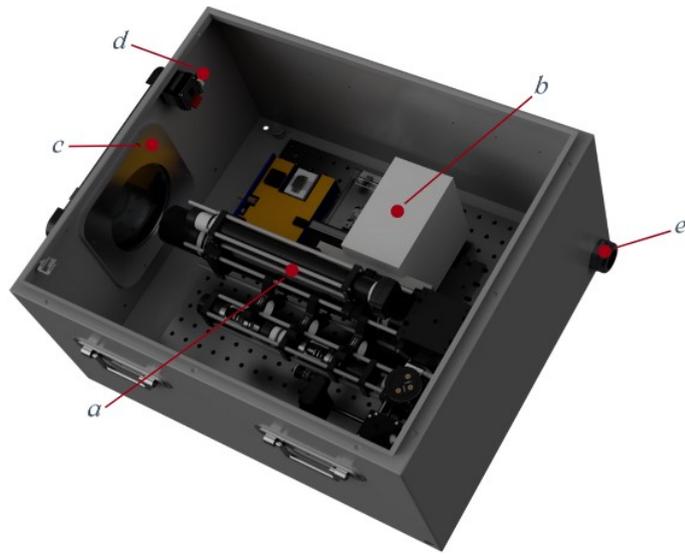


Figura 12: Render dell'apparato ricevitore con vista all'interno del contenitore. a) Telescopio ricevitore, b) Mount alt-azimut motorizzata, c) Supporto finestra ottica, d) Motore stepper per automazione shutter, e) Passacavi posteriore.

5 Automazione tip-tilt di uno specchio a 45°

La seconda attività relativa al sistema per IM-QKD svoltasi in questa tesi è la progettazione e il test di un apparato optomeccanico per l'automazione della correzione tip-tilt di un componente ottico. La realizzazione di questa attività è stata spinta dalla necessità e comodità di un controllo a distanza e potenzialmente automatizzato per effettuare correzioni e setup, tuttora svolti manualmente, sui telescopi utilizzati per le trasmissioni di QKD in free-space.

Nel caso trattato di seguito, il componente ottico montato sul supporto di correzione tip-tilt è uno specchio angolare a 45° che ha lo scopo di ridirezionare il fascio al ricevitore verso l'apparato per l'accoppiamento SMF. È infatti facile notare che un'alta precisione e risoluzione nel direzionare il fascio laser al centro dell'adattatore FC/PC garantisce una migliore efficienza di accoppiamento in fibra. Un'altra possibile applicazione del suddetto sistema, in questo caso al trasmettitore, potrebbe migliorare la risoluzione di puntamento del telescopio. Difatti, la mount *alt-azimut* utilizzata per l'allineamento *coarse* ha una risoluzione angolare dell'ordine dei 30 μrad che per link di lunghezza superiore all'ordine dei 20 km, come il link tra il Montegrande e il DEI che si sta sviluppando, risulta essere di circa 60 cm, maggiore dell'apertura del telescopio di 40 cm installato sul tetto del DEI.

5.1 Design optomeccanico per l'automazione dello stage

Il design meccanico del sistema di accoppiamento in fibra automatizzato è pensato per fornire al trasmettitore le funzionalità aggiuntive di controllo a distanza sempre mantenendo un ingombro limitato. Questo risulta necessario per preservare la sua compattezza e compatibilità con il design del contenitore creato in precedenza per il ricevitore.

Il componente principale utilizzato per la regolazione tip-tilt è una mount cinematica da 1" compatibile con sistemi caged, modello *KC1T/M* (Figura 13.a). Ad essa è assemblato un supporto a 45° per uno specchio dielettrico di geometria circolare da 1", modello *H45* (Figura 13.b). Va osservato che per assemblare mount cinematica e specchio è necessario un adattatore da foro filettato a foro liscio, modello *SM1P2*

(Figura 13.c). Questo adattatore è necessario, inoltre, per posizionare lo specchio centralmente rispetto al “gomito” formato dal sistema caged, in modo tale da coprire completamente l’area di propagazione del fascio. Un altro componente utile all’assemblaggio di questo sistema è un supporto a 90° per sistemi caged da 1”, modello CP30 (Figura 13.d). Infine, sono stati scelti due attuatori lineari stepper per l’automazione della mount cinematica, modello ZFS13 (Figura 13.e).

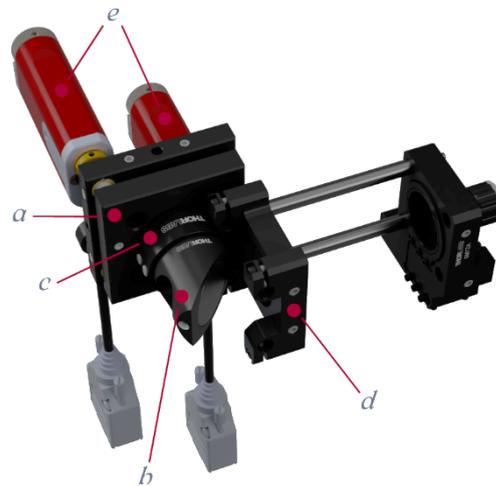


Figura 13: Render del sistema automatizzato per l'accoppiamento in fibra. a) Mount cinematica tip-tilt, b) Supporto a 45° per specchio circolare, c) Adattatore, d) Supporto caged a 90°, e) Componenti per l'accoppiamento in fibra, f) Attuatori stepper.

La progettazione del sistema descritto in questo capitolo ne assicura un comodo e relativamente immediato assemblaggio al sistema caged da 1” del telescopio ricevente.



Figura 14: Render del telescopio ricevitore con stage per l'automazione dell'accoppiamento in fibra.

Difatti non risulta necessario rimuovere alcun componente al di fuori di quelli direttamente interessati, ovvero il supporto cinematico a 45° con regolazione manuale e lo stage per l'accoppiamento in fibra. In Figura 14 è riportato il render del sistema optomeccanico del telescopio ricevente completo dell'apparato di automatizzazione.

5.2 Test e caratterizzazione del sistema automatizzato

Al fine di valutare le performance e quindi l'effettiva utilità del sistema progettato, sono stati eseguiti dei test al banco ottico in laboratorio. In particolare, risulta utile determinare il minimo incremento angolare che è possibile effettuare in modo ripetibile con una buona precisione, e la caratterizzazione del rapporto tra inclinazione angolare della mount e spostamento lineare degli attuatori.

Come sorgente si è utilizzato un diodo laser da circa 4 mW che produce un fascio a 800 nm collimato. Per attenuarne l'intensità, è stato montato un filtro da 30 dB davanti alla sorgente. Utilizzando uno specchio, il fascio viene poi direzionato verso lo specchio a 45° assemblato alla mount automatizzata. Il fascio quindi si propaga attraverso una lente di focale $f = 2.2\text{ m}$, incide su uno specchio e infine viene catturato da una camera CMOS posizionata nel fuoco della lente, modello *ASI-183MM* prodotta da *ZWO*.

In Figura 15 è riportato uno schema con i principali componenti utilizzati in questo test.

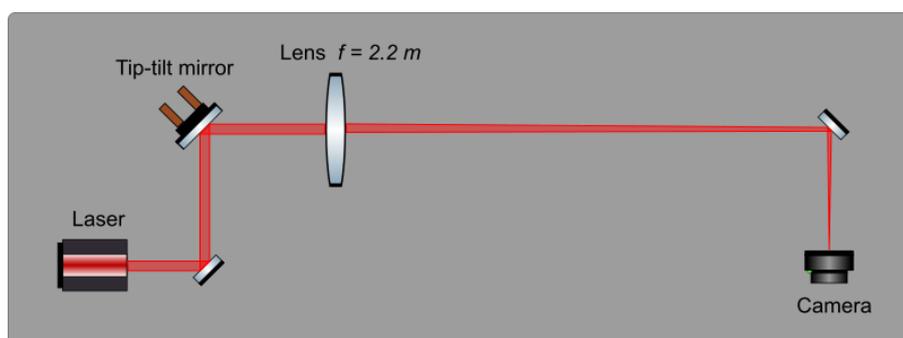


Figura 15: Design del sistema ottico utilizzato per il test.

Al fine di calcolare il centroide dello spot a partire dai fotogrammi catturati e di collezionarne le variazioni di posizione, si è utilizzato un software di controllo sviluppato dal gruppo Quantum Future che permette di loggare la posizione del centroide dello spot ad una data frequenza di campionamento.

È stato poi sviluppato uno script in linguaggio Python per automatizzare il controllo degli attuatori in modo da effettuare serie di misurazioni al variare dell'incremento lineare degli attuatori. Sono state effettuate 80 misurazioni per ogni diverso valore di incremento lineare e facendo variare quest'ultimo nell'intervallo da 5 nm a $5\text{ }\mu\text{m}$ con 11 valori intermedi.

Per una corretta interpretazione dei risultati esposti di seguito è necessario ricordare alcune specifiche degli attuatori lineari stepper, tra cui il minimo incremento dichiarato dal costruttore pari a 0.46 nm mentre la ripetibilità dello spostamento che può avere un errore massimo dichiarato di $5\text{ }\mu\text{m}$. Inoltre, la camera utilizzata per l'esperimento è caratterizzata da una *pixel-size* di $2.4\text{ }\mu\text{m}$ e da un frame rate massimo di 19 Hz .

Di seguito si utilizza l'incremento da $1\text{ }\mu\text{m}$ a titolo esemplificativo. In Figura 16 è rappresentato il grafico di un segmento di circa 2 minuti e 30 secondi delle serie temporali relative allo spostamento degli attuatori e alla posizione dello spot sul piano focale della camera. Per il secondo caso sono rappresentati prima i dati grezzi e successivamente i dati puliti e mediati all'interno degli intervalli di campionamento, identificati in azzurro. Questi ultimi sono selezionati in modo da non considerare le acquisizioni della posizione dello spot compromesse dal movimento degli attuatori, come identificabile nel secondo grafico in Figura 16 dove si verificano delle dispersioni verticali dei punti durante l'attivazione degli attuatori.

Infine, nel terzo grafico in Figura 16, grazie alla mediazione sugli intervalli e alla pulizia dei valori, si nota in modo evidente lo spostamento dello spot sul piano focale della camera lungo entrambi gli assi. L'utilizzo di valori mediati su periodi di 4 secondi assicura la cattura di circa 76 campioni per ogni incremento, riducendo così l'errore di misura. Questo errore è attribuibile al rumore elettronico dei pixel della camera, che influisce sul relativo calcolo del centroide. In questo passaggio risulta quindi utile calcolare, per ogni intervallo, anche l'errore standard della media (SEM) calcolato come la deviazione standard dei valori misurati diviso per la radice quadrata del numero di valori misurati.

Serie temporali della posizione di attuatori e centroide dello spot, step=0.001 mm

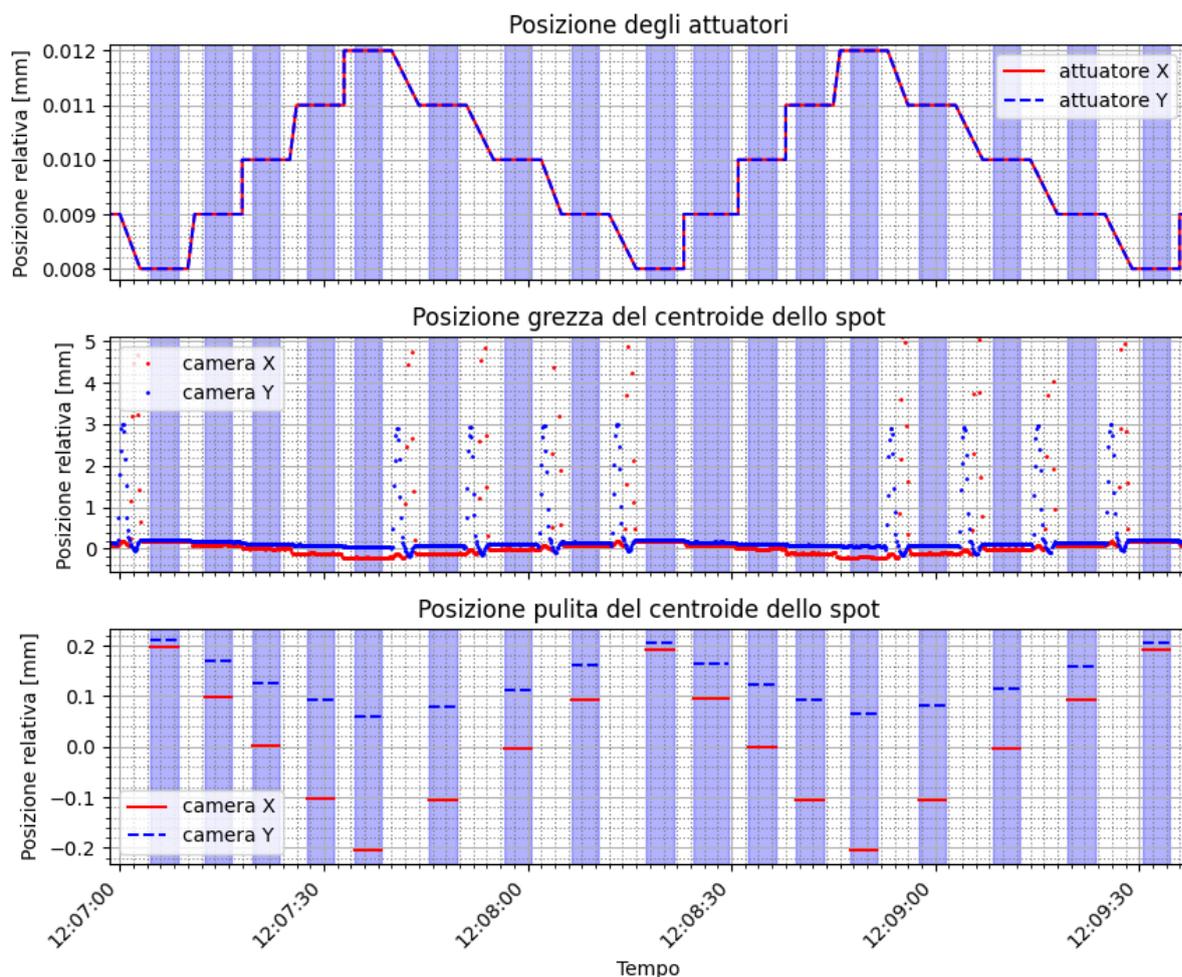


Figura 16: Serie temporali relative a: spostamento degli attuatori, dati grezzi della posizione dello spot sul sensore della camera e dati puliti e mediati sugli intervalli di campionamento della posizione dello spot.

Considerando inoltre che l'incremento è effettuato su entrambi gli attuatori in modo contemporaneo e uguale in valore, è già possibile notare dal terzo grafico in Figura 16 una sensibile differenza tra gli effetti sullo spostamento dello spot lungo i due diversi assi, dati da un uguale movimento dello specchio.

Successivamente, dai valori puliti della serie temporale è possibile ricavare lo spostamento relativo del centroide dello spot, associato ad ogni incremento degli attuatori. In Figura 17 sono riportati gli istogrammi prima e dopo l'eliminazione dei valori caratterizzati da un errore sopra al 95 percentile, rispettivamente nella prima e seconda riga. Questa operazione è utile a rimuovere gli spostamenti più disturbati e ottenere risultati sensibilmente più precisi. Si può inoltre notare che, la rimozione degli *outliers* effettuata come descritto in precedenza, interessa circa 6 valori su 80 totali.

Istogrammi dello spostamento del centroide per l'incremento 0.001 mm con rimozione degli outliers

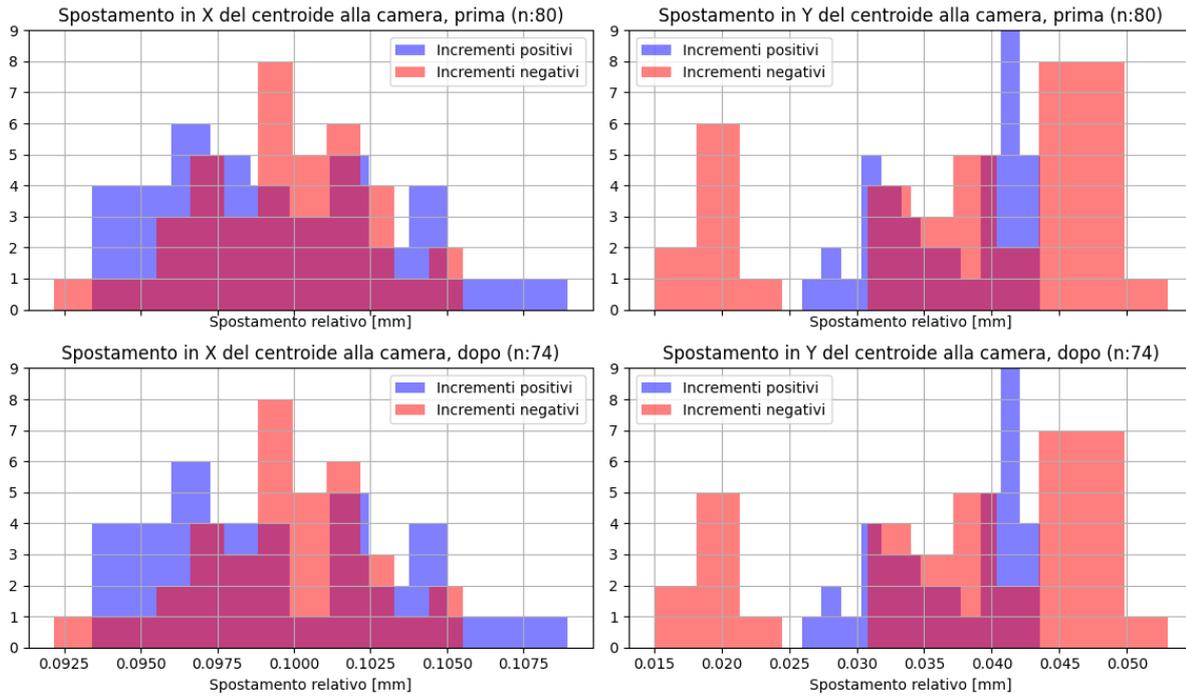


Figura 17: Istogrammi dello spostamento relativo del centroide dello spot prima e dopo la rimozione dei valori affetti in modo maggiore da errore, separando tra i due assi e tra incrementi positivi e negativi.

Si ricorda che uno spostamento è dato dal valore assoluto della differenza tra due valori consecutivi della posizione del centroide, che a loro volta sono stati calcolati come la media delle misurazioni in un intervallo temporale e caratterizzati dall'errore standard della media. È quindi possibile ottenere l'errore di uno spostamento come la somma degli errori dei due valori sottratti, propagando così facendo l'errore di misura.

Dati tutti gli spostamenti calcolati per un determinato incremento degli attuatori e i relativi errori, è possibile quindi calcolare una media pesata dello spostamento per una data azione degli attuatori

$$\bar{x} = \frac{1}{K} \sum_{i=1}^N \frac{x_i}{\sigma_i^2} \quad (26)$$

Dove x_i è l' i -esimo spostamento, σ_i il relativo errore standard, N il numero di campioni utilizzati e K dato dalla seguente

$$K = \frac{1}{\sum_{i=1}^N \frac{1}{\sigma_i^2}} \quad (27)$$

In questo modo viene quindi assegnato, ad ogni misura, un peso inversamente proporzionale al quadrato dell'errore ad essa associato. L'errore standard della media pesata determinata dall'Equazione (26) è pari alla radice quadrata di K [11].

Infine, partendo dalla seguente relazione, sotto l'approssimazione per piccoli angoli, è possibile ricavare lo spostamento angolare relativo α dello specchio associato ad ogni spostamento medio relativo del centroide dello spot sul piano focale della camera x

$$x = f \cdot \alpha \quad (28)$$

Con $f = 2.2 \text{ m}$ la lunghezza focale della lente utilizzata, che risulta inoltre pari alla distanza di propagazione del fascio dalla lente alla camera. Essendo poi f una costante priva di errore è possibile determinare l'errore standard dello spostamento angolare dalla medesima relazione.

Effettuando i passaggi sopra citati per tutti i diversi valori di incremento degli attuatori, determinando così tutti gli spostamenti angolari relativi medi, è possibile ottenere la relazione tra incremento lineare degli attuatori e spostamento angolare dello specchio interpolando i punti ottenuti per entrambi gli assi.

Data la natura dell'esperimento, risulta logico utilizzare un'interpolazione dei dati con una retta passante per l'origine [11]. Per determinare quindi il coefficiente si applica ad entrambi gli assi la seguente formula

$$m = \frac{\sum_{i=N-3}^N \delta_i \cdot \alpha_i}{\sum_{i=N-3}^N \delta_i} \quad (29)$$

Con δ_i l' i -esimo tra gli incrementi lineari dell'attuatore ordinati in modo crescente, in millimetri. Il coefficiente m ha valore pari allo spostamento angolare associato ad un incremento lineare unitaria dell'attuatore e ha unità di misura $m = [\text{rad}/\text{mm}]$. Si noti che l'Equazione (29) considera solo i 4 incrementi maggiori per i quali si ha alta precisione e ripetibilità nello spostamento dell'attuatore.

In Figura 18 sono raffigurati gli spostamenti angolari medi, con i relativi errori standard, per tutti i valori di incremento lineare testati e la retta interpolata passante per l'origine.

Dai grafici si nota in modo più preciso la sostanziale differenza tra i due assi precedentemente accennata. Per l'asse delle ascisse uno spostamento lineare

dell'attuatore di 1 mm comporta uno spostamento angolare di circa 45.5 mrad mentre per l'asse delle ordinate il medesimo spostamento dell'attuatore è invece associato ad un angolo di 19.0 mrad. Questa differenza può trovare spiegazione nella geometria asimmetrica della mount cinematica responsabile del movimento dello specchio.

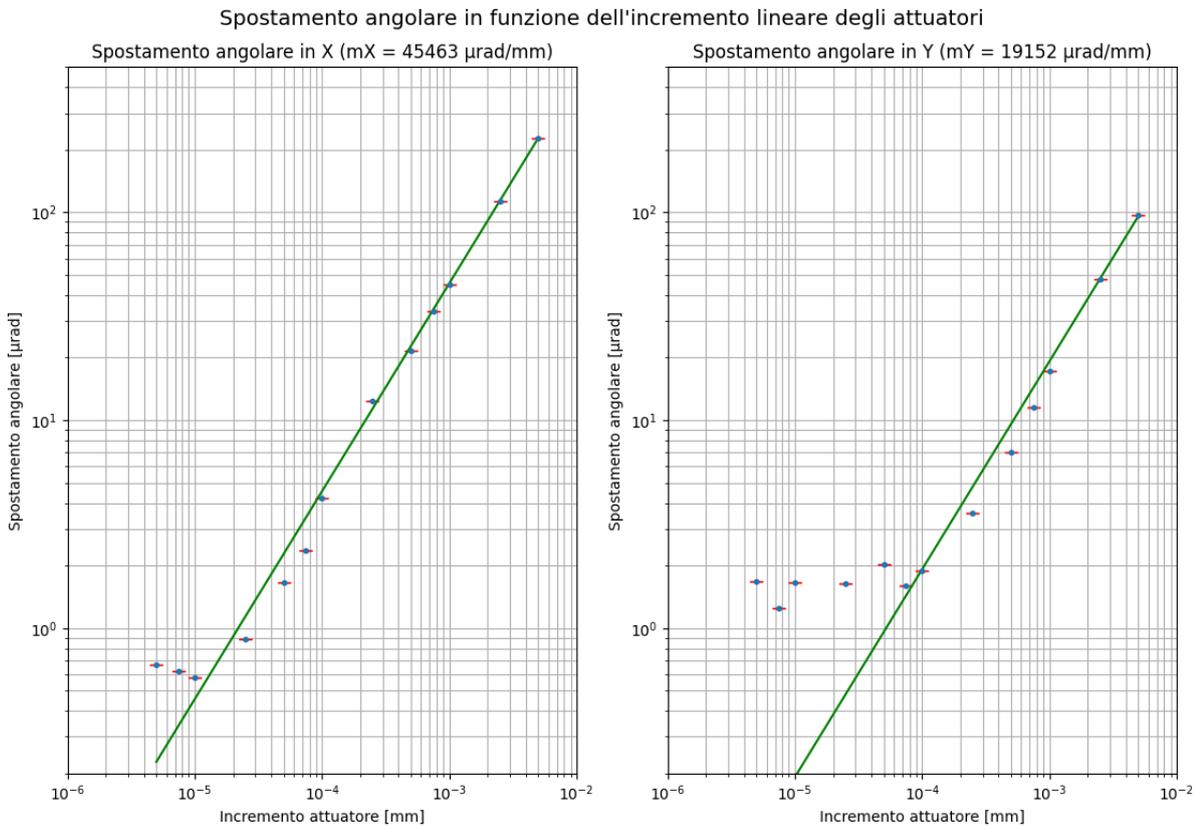


Figura 18: Relazione tra spostamento lineare degli attuatori e spostamento angolare dello specchio con interpolazione lineare per entrambi gli assi, in scala logaritmica. I punti rappresentano il valore mediato dello spostamento angolare con il relativo errore standard.

Il minimo spostamento angolare osservato, che soddisfa l'Equazione (28) entro un errore di circa 100 nm, è dell'ordine di 0.9 μrad per l'asse delle ascisse e di 1.5 μrad per le ordinate. L'incremento lineare necessario per raggiungere questi spostamenti angolari minimi è dato da circa 25 nm per il primo caso e 75 nm per il secondo.

Si osserva inoltre che la retta interpolata rappresentante la relazione teorica sovrastima sensibilmente 3 punti per l'asse delle ascisse e 4 per le ordinate adiacenti al minimo incremento. Ovvero, relativamente a questi specifici punti, lo spostamento angolare misurato è inferiore rispetto a quello atteso. Per il fine di questa analisi e dell'applicazione dello specchio nelle modalità descritte a inizio Capitolo 5, questo comportamento non limita le performance dell'apparato automatizzato. Risulta

comunque necessario considerare questa caratterizzazione durante l'interazione con l'apparato stesso, manualmente o via software.

Sotto l'ipotesi di correttezza di questi risultati e di assenza di ulteriori fattori non considerati in questo test che ne peggiorino le performance, nel caso di un link con estensione circa pari a 20 km , ad esempio nel caso del link Montegrande-DEI, l'applicazione dello specchio automatizzato al trasmettitore porterebbe notevoli vantaggi. Nello specifico, la risoluzione di puntamento scenderebbe da circa 60 cm a circa 1.8 cm per uno spostamento orizzontale, mentre a 3.0 cm per uno spostamento verticale.

Infine, gli errori standard associati ai punti risultano molto bassi grazie all'alto numero di campioni utilizzati per determinare i valori mediati per ogni intervallo e all'alto numero di intervalli stessi. Si evidenzia un lieve aumento dell'errore al diminuire della dimensione dell'incremento lineare degli attuatori.

Conclusione

In questa tesi si è svolto uno studio preliminare dei protocolli per QKD, di ottica Gaussiana e propagazione di fasci in atmosfera al fine di comprendere al meglio il funzionamento dei dispositivi opto-meccanici progettati e utilizzati dal gruppo Quantum Future nel campo di IM-QKD. Successivamente sono state svolte alcune attività a supporto dei progetti in atto, nello specifico riguardanti la realizzazione di un link per IM-QKD stabile e automatizzato.

La prima attività è stata finalizzata al design meccanico CAD dei terminali trasmettitore e ricevitore utilizzati per il link di QKD in free-space. I contenitori realizzati soddisfano i requisiti di resistenza ad agenti atmosferici e protezione della strumentazione da essi, di compattezza e trasportabilità, e infine di funzionamento con controllo da remoto di alcuni componenti mobili.

Nella seconda attività invece è stata portata a termine la progettazione di uno specchio a 45° automatizzato utile per diverse applicazioni sui telescopi trasmettitore e ricevitore. Il componente progettato rispetta i requisiti di compattezza e di compatibilità con i sistemi opto-meccanici precedentemente progettati e utilizzati per le trasmissioni per QKD. In questo modo la sua integrazione risulta comoda e relativamente veloce.

In questa attività è stato inoltre svolto il test in laboratorio dell'apparato progettato, al fine di determinare la sua caratterizzazione e i relativi limiti. Dai risultati ottenuti è possibile concludere che il suo impiego nelle operazioni di QKD potrebbe portare vantaggi relativamente a precisione e risoluzione di puntamento, se applicato al trasmettitore, oppure all'efficienza di accoppiamento in fibra e automazione delle fasi di setup, se applicato al ricevitore.

Tuttavia, ulteriori studi in laboratorio e sul campo sono necessari per accertare e affinare queste conclusioni.

Bibliografia

- [1] P. Shor, «Algorithms for quantum computation: discrete logarithms and factoring,» *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124-134, 1994.
- [2] C. H. Bennett e G. Brassard, «Quantum cryptography: Public key distribution and coin tossing,» *Theoretical Computer Science*, vol. 560, pp. 7-11, 2014.
- [3] M. A. Nielsen e I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, Cambridge: Cambridge University Press, 2010.
- [4] C.-Y. Lu, Y. Cao, C.-Z. Peng e J.-W. Pan, «Micius quantum experiments in space,» *Rev. Mod. Phys.*, vol. 94, n. 3, p. 46, 2022.
- [5] R. Wolf, *Quantum Key Distribution: An Introduction with Exercises*, Springer Cham, 2021.
- [6] L. C. Andrews, *Field Guide to Atmospheric Optics*, Bellingham, Washington USA: SPIE, 2004.
- [7] B. E. Saleh e M. C. Teich, *Fundamentals of Photonics*, Wiley, 2019.
- [8] A. Scriminich, G. Foletto, F. Picciariello, A. Stanco, F. Vedovato, G. Vallone e P. Vedovato, «Optimal design and performance evaluation of free-space quantum key distribution systems,» *Quantum Science and Technology*, vol. 7, n. 4, 2022.
- [9] R. K. Tyson e B. W. Frazier, *Field Guide to Adaptive Optics*, Washington: Spie Press, 2012.
- [10] F. Vedovato, F. Picciariello, I. Karakosta-Amarantidou, D. Scalcon, M. Avesani, E. Rossi, A. Scriminich, G. Foletto, M. Padovan, A. Lorenzetto, F. Berra, L. Calderaro, F. Kutschera, M. Achleitner, H. Huber, G. Vallone e P. Villoresi, «Realization of intermodal fiber/free-space quantum key distribution networks,» *SPIE 12446, Quantum Computing, Communication, and Simulation*, vol. III, n. 124460Q, 2023.
- [11] M. Loreti, *Teoria degli Errori e Fondamenti di Statistica: Introduzione alla Fisica Sperimentale*, Padova, 2006.