COMANDO PER LE OPERAZIONI IN RETE

*Reparto Operazioni Cibernetiche*

# REQUISITO

# TECNICO OPERATIVO

**RELATIVO A**

***Acquisizione di studi e di un sistema prototipale relativi a un Device-Independent Quantum Key Distribution (DI-QKD) per applicazioni Difesa. Fase unica***

---

***Edizione***

***Dicembre 2024***

# COMANDO PER LE OPERAZIONI IN RETE
## *Reparto Operazioni Cibernetiche*

### PREDISPOSIZIONE DEL DOCUMENTO

| Redatto da | Data |
|---|---|
| Ufficio Tecnico Operativo | 14/12/2024 |
| | |
| | |
| | |

### LISTA REVISORI

| Ufficio/Sezione/Nominativo |
|---|
| |
| |
| |
| |

## REGISTRO DELLE REVISIONI

| Revisione | Data | Capitoli/paragrafi modificati | Osservazioni |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**QUESTO DOCUMENTO È COSTITUITO DA _____ PAGINE TOTALI**

## Sommario

## 1. OBIETTIVO

Lo Stato Maggiore delle Difesa, attraverso il Dipartimento Cyber Operations (ROC) del COR vuole prepararsi all'avvento sempre più invasivo di nuove soluzioni tecnologiche che risolvono il problema delle future esigenze dei sistemi crittografici. Mentre il mondo anticipa i prossimi standard di crittografia post-quantistica del NIST, è in essere lo sviluppo simultaneo di sistemi di distribuzione di chiavi quantistiche (QKD), con attori importanti come India, Cina, UE e Stati Uniti che ricercano e valutano attivamente gli standard per questo approccio crittografico emergente; la domanda cruciale rimane come la QKD potrebbe integrarsi in uno standard globale a prova di futuro per le comunicazioni digitali sicure oltre il 2030, anche se attualmente varie organizzazioni stanno perseguendo diverse implementazioni tecnologiche poiché non è emerso un chiaro leader in questo campo nascente.

La sicurezza delle informazioni digitali si basa sulla crittografia, utilizzata per la cifratura dei dati memorizzati su dischi e trasmessi in *streaming* su fibre ottiche o collegamenti "*free-space*" (spettro elettromagnetico). La base dei moderni sistemi di crittografia è data dai cifrari simmetrici, come Rijndael/AES, RC5 o SNOW, che garantiscono la riservatezza e l'integrità delle informazioni nelle reti Internet e 5G/6G distribuite. Questi algoritmi, in particolare Rijndael/AES, sono raccomandati da organizzazioni quali NATO, NIST, NSA negli Stati Uniti e dalle direttive eIDAS2/NIS2 dell'UE per la sicurezza delle informazioni fino al livello top-secret [NIST Federal Inf. Process. Stds. 197 (2001)]; nello specifico questi algoritmi utilizzano operazioni a bassa latenza e ad alte prestazioni per codificare e decodificare i *byte* in modo tale da rendere impossibili gli attacchi. Tuttavia, questi metodi richiedono l'utilizzo della stessa chiave segreta da parte di entrambi gli interlocutori.

Un'opzione, ampiamente utilizzata nelle infrastrutture critiche come le stazioni base 5G o i sistemi di controllo satellitare, è quella di salvare manualmente la chiave nel dispositivo *endpoint* (*pre-shared key*, PSK), ma questo comporta dei rischi quando il dispositivo viene catturato da un nemico o violato da un *hacker*. Attualmente, il problema della condivisione delle chiavi è risolto dall'infrastruttura a chiave pubblica (PKI) utilizzata per la generazione e la distribuzione di chiavi crittografiche con algoritmi asimmetrici. Tale soluzione è adeguata perché consente alle parti comunicanti di scambiare i dati senza una precedente interazione, basandosi solo sulla fiducia in un'autorità di certificazione (CA), solitamente fornita da un ente governativo o da un fornitore autorizzato. Tuttavia, le comuni PKI basate su Rivest-Shamir-Adleman (RSA) o sulla crittografia a curva ellittica (ECC) sono notoriamente violabili non solo da computer quantistici, ma anche da potenti computer convenzionali, e rappresentano il punto più debole del processo di scambio sicuro dei dati. Anche gli algoritmi asimmetrici di nuova generazione, ad esempio CRYSTALS-Kyber, che appartengono alla classe della crittografia post-quantistica (PQC) e che ora sono in fase di standardizzazione da parte del NIST, non offrono prove di sicurezza concrete e alcuni di essi hanno già dimostrato di poter essere violati nonostante anni di sviluppo. Pertanto, è urgente trovare nuove soluzioni per lo scambio di chiavi segrete che rispondano alle esigenze del moderno scenario sia in ambito

*warfare*, delle infrastrutture critiche e delle applicazioni commerciali ad alto valore economico e sociale.

Si intende sostituire la crittografia asimmetrica e l'infrastruttura a chiave pubblica con una tecnologia di distribuzione di chiavi quantistiche (QKD) che utilizzi l'*entanglement*, fornisca un'elevata sicurezza di creazione e distribuzione delle chiavi nonché un monitoraggio in tempo reale. La soluzione sarà dimostrata matematicamente e implementata sulla rete di test del COR-ROC e sarà sottoposta a collaudo al fine di verificarne la resistenza sia agli attacchi convenzionali che quantistici attraverso un protocollo che dovrà essere proposto dalla Ditta e validato da A.D.

## 2. SCENARIO ED ARTICOLAZIONE DEL PROGETTO

L'obiettivo di questo requisito tecnico operativo (RTO), redatto nell'ambito del PNRM di cui al titolo in copertina, è quello di definire i requisiti per una soluzione alternativa di crittografia quantistica indipendente dal dispositivo (DI) / distribuzione di chiavi quantistiche (QKD) che fornirà uno scambio sicuro di chiavi utilizzando la tecnologia fotonica quantistica più avanzata.

Lo scenario che si vuole realizzare si basa sull'ipotesi di un *entanglement* quantistico fotonico distribuito tra due terminali elettronico-ottici collegati mediante fibre ottiche in un modo che consenta loro di eseguire un *test* di Bell, e quindi estrarre i *bit* casuali correlati della chiave segreta senza inviarla fisicamente in alcuna forma tra gli *endpoint*. I terminali, che realizzeranno un protocollo ibrido quantistico-classico, eseguiranno un'ulteriore post-elaborazione crittografica dei *bit* estratti per garantirne l'utilità per le attività crittografiche, migliorare la loro *privacy* e fornirne l'utilizzo per le operazioni di rete. Inoltre, la velocità prevista con cui vengono generati i *bit* segreti sarà in rapporto con la radice quadrata della lunghezza della fibra ottica, consentendo lo scambio di informazioni a distanze molto lunghe, in modo simile al noto protocollo di distribuzione della chiave quantistica a doppio campo (TF), ma utilizzerà l' *entanglement* quantistico e un approccio completamente indipendente dal dispositivo, in cui il *test* di *entanglement* con risultato positivo informerà ulteriormente gli operatori di rete sull'assoluta sicurezza della chiave.

Quale *baseline* storica si tenga in considerazione che un sistema crittografico QKD è stato teoricamente descritto nel 1998, quindi le prove di sicurezza sono state sviluppate nel 2009 [https://iopscience.iop.org/article/10.1088/1367-2630/11/4/045021/meta], mentre le prime realizzazioni sperimentali sono state effettuate nel 2022 [https://www.nature.com/articles/s41534-023-00684-x].

Il progetto dovrà concretizzarsi con la realizzazione di un dimostratore per una soluzione DI-QKD da convalidare nell'infrastruttura di test del COR. Il sistema, composto da due terminali quantistici che utilizzano l'*entanglemen*t del numero di fotoni e da un nodo centrale, tutti ottimizzati per le operazioni nella lunghezza d'onda delle telecomunicazioni (1550 nm), potrà/dovrà prevedere eventuali personalizzazioni per le esigenze del settore della Difesa,

aggiungendo le opzioni di connettività necessarie e valutato per potenziali casi d'uso in diversi scenari.

Il progetto dovrà articolarsi nei seguenti *step*:

S1. Definire i casi di *test* e i criteri di successo;

S2. Realizzare un'installazione pilota DI-QKD basata su *entanglement*, collegando due terminali a una linea di test in fibra spenta ed eseguendo *test* delle prestazioni del sistema in scenari realistici, raggiungendo una velocità di trasmissione di almeno 10^4 *bit*/s su 15 km di fibra e allo stesso tempo soddisfacendo i criteri del *test* di Bell.

S3. Integrare e personalizzare il sistema per le esigenze del COR e del settore della Difesa, secondo le specifiche delle interfacce e degli standard utilizzati nella NATO e nelle Forze Armate italiane (queste ultime definite in S1).

S4. Eseguire *test* approfonditi di accettazione da parte dell'utente del funzionamento QKD in un collegamento tra due *data center* COR (da identificare nel corso di S1).

Il progetto si concluderà con un rapporto dettagliato sulla tecnologia QKD, le sue prestazioni, l'utilità per la Difesa e la robustezza nei diversi scenari definiti in S1.

## 3. OGGETTO DELLA DI FORNITURA

L'obiettivo è quello di acquisire un nuovo livello di conoscenza nel campo delle più avanzate soluzioni di crittografia quantistica che utilizzano l'*entanglement* quantistico e forniscono un livello di sicurezza delle informazioni indipendente dal dispositivo.

[R1] Per risolvere il problema dello scambio sicuro di chiavi, si propone di testare la sostituzione della crittografia asimmetrica *software-defined* e delle soluzioni PKI attualmente utilizzate con una nuova tecnologia di distribuzione di chiavi quantistiche (QKD) basata sull'*entanglement* quantistico multi-fotonico a lunga distanza, certificata da un test di Bell.

Il test di Bell è un concetto importante nell'ambito dell'informazione quantistica: è una misurazione congiunta di due stati quantistici che ne misura la correlazione. Questa tecnologia fornirà inoltre alla Difesa la possibilità di scambiare chiavi crittografiche realmente casuali, in modo incondizionatamente sicuro, superando il limite di distanza di circa 100 km [R2] imposto dalle precedenti soluzioni QKD.

[R3] Nella soluzione QKD ipotizzata, due parti comunicanti, "A" e "B", utilizzano cristalli SPDC (*Spontaneous Parametric Down-Conversion*) per produrre una coppia di impulsi quantistici multi-fotonici ciascuno, 10^5 - 10^8 volte al secondo. Quindi, uno degli impulsi di "A" e uno di "B" vengono inviati ad un nodo centrale, "C", che esegue lo scambio di *entanglement* per mezzo di una misura di Bell con "*heralding*" e crea di fatto un "*entanglement*" a lungo raggio tra i fotoni di "A" e "B". Questi fotoni *entangled* vengono

interferiti con impulsi coerenti sincronizzati su divisori di fascio variabili e misurati con rivelatori di nanofili superconduttori ad alta efficienza. L'*entanglement* è una fonte di casualità correlata: le letture di "A" e "B" sono davvero casuali, ma sono correlate nonostante la distanza, il che fornisce una base per produrre a distanza due chiavi segrete identiche, senza inviarle fisicamente attraverso il collegamento. L'esecuzione del *test* di Bell certifica la sicurezza e la casualità delle chiavi segrete prodotte in modo inconfutabile: permette alle parti di monitorare in tempo reale la sicurezza della connessione e di evidenziare immediatamente qualsiasi tentativo di intercettazione o manomissione delle informazioni scambiate, certificandone così l'integrità. Una volta che il *test* è positivo, le chiavi vengono post-elaborate e fornite agli utenti finali. Questa soluzione fornisce quindi un livello di sicurezza indipendente dal dispositivo (DI), che non dipende dalla sicurezza interna di alcun nodo o supporto fisico.

[R5] La soluzione QKD proposta sarà arricchita da un livello *software* che fornirà un'efficiente gestione delle chiavi segrete per ambienti multiutente, interfacce di programmazione delle applicazioni (API), connettori e *plug-in* per una perfetta integrazione con l'infrastruttura IT, un'interfaccia *user-friendly* per il controllo e l'amministrazione, il monitoraggio in tempo reale (osservabilità) e il funzionamento *cloud-native*.

## 4. PIANO DI ATTUAZIONE

L'implementazione del sistema complessivo, costituito da due terminali e da un nodo centrale, sarà realizzata nelle seguenti fasi:

1. Due terminali QKD saranno assemblati e consegnati da un fornitore di tecnologia a livello industriale, scelto dopo una selezione competitiva per le competenze nello specifico campo scientifico, così come i dispositivi *stand-alone* contenuti in *rack standard* 19''. [R6] Ognuno di essi sarà costituito da un sistema laser pulsato da 1550 nm, un cristallo SPDC, modulatori di luce, un rivelatore di nanofili superconduttori in un criostato, un computer e componenti fotonici passivi. I terminali saranno testati, caratterizzati per le loro prestazioni e convalidati dal personale del Comando per le Operazioni in Rete (COR) e dai ricercatori della parte fornitrice.
2. I terminali saranno installati in *data center* di proprietà del COR, separati e collegati con una coppia di fibre a bassissima perdita (a cura fornitore), dove una fibra sarà utilizzata esclusivamente per le comunicazioni quantistiche e l'altra per il trasferimento convenzionale dei dati. Il fornitore caratterizzerà i canali e testerà l'interferenza quantistica misurandone la visibilità. Se necessario, migliorerà l'installazione.
3. Verrà implementato il protocollo di distribuzione dell'*entanglement* a lungo raggio e i risultati saranno poi confrontati con il modello numerico definito in S1. Successivamente, verrà eseguito un *test* di Bell mediante interferenza locale di fotoni con impulsi coerenti di intensità variabile. Il sistema DI-QKD sarà collegato a una piattaforma di osservabilità, come Observium o Grafana (a cura fornitore).
4. IL COR, insieme al fornitore, concorrerà alla definizione del piano *test* e dei criteri di successo di S1. Al termine del progetto, verrà prodotta una documentazione che illustrerà i metodi di caratterizzazione e i risultati di robustezza del PoC.

## 5. NECESSITÀ FINANZIARIA

Nella tabella seguente sono riportate le forniture e le relative stime economiche di massima.

| **Elementi di alimentazione di base** | **Costo stimato (IVA esclusa)** |
|---|---|
| Fornitura di S1 + S2 + S3 + S4 (Fase Unica) | |
| COSTO TOTALE STIMATO | |

*Tabella 1 – Requisiti Tecnico-Funzionali*

## 6. TABELLA DEL CRONOPROGRAMMA

| **ITEM** | **DATA DI CONSEGNA** |
|---|---|
| S1 | T1 = T0 + 2 MESI |
| S2 | T2 = T1 + 3 MESI |
| S3 | T3 = T2 + 3 MESI |
| S4 | T4 = T3 + 1 MESE |

*Tabella 2 – Piano Attuativo*

Note:

- la fornitura di ogni articolo previsto dal presente requisito dovrà essere completata **entro il 30 settembre 2025** al fine di permettere all'Amministrazione Difesa di effettuare i pagamenti dovuti entro il medesimo esercizio finanziario a seguito di ricezione di regolare fattura.