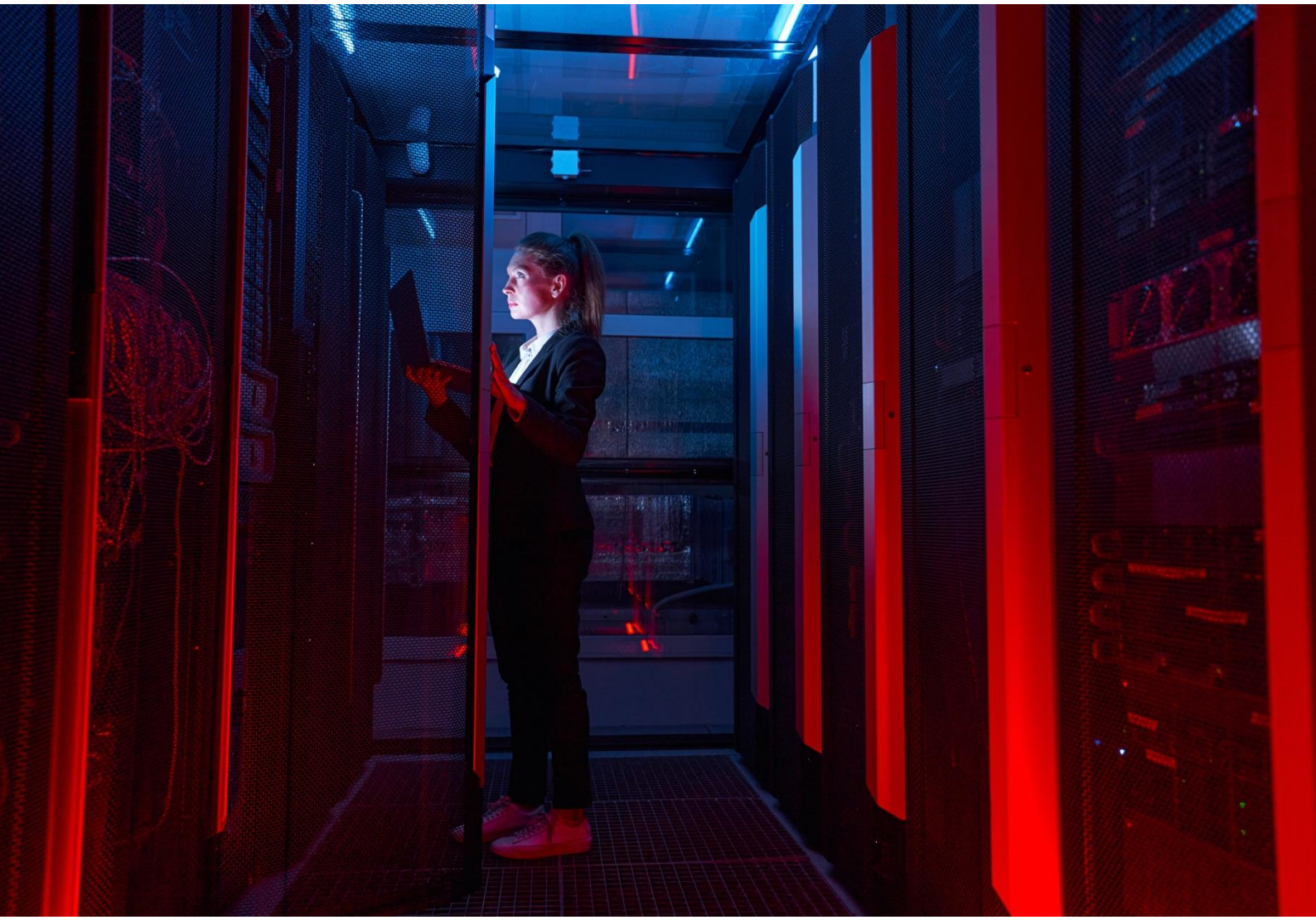


Namirial apre l'era della sicurezza post-quantum

La prima dimostrazione industriale su computer quantistico e le soluzioni che rendono firme e comunicazioni già "quantum-resistant"

Abstract

Questo documento presenta i rilevanti risultati ottenuti da Namirial nel settore della **sicurezza digitale** nell'era dei **computer quantistici**.

Namirial è la prima realtà industriale nel settore dei servizi fiduciari ad aver dimostrato concretamente l'impatto dei computer quantistici sui sistemi crittografici a chiave pubblica, nonché ad aver analizzato e proposto l'adozione di tecnologie in grado di contrastare tale minaccia attraverso un approccio comprensivo, integrato e multidimensionale.

Il documento illustra in particolare i seguenti risultati:

- l'utilizzo di un **vero computer quantistico per rompere una chiave crittografica RSA**;
- l'**analisi delle prestazioni degli algoritmi di crittografia post-quantum**, finalizzata a garantire un livello di sicurezza duraturo nel tempo, con risultati presentati nell'ambito della conferenza NIST dedicata alla standardizzazione di tali tecnologie;
- la **realizzazione di un portale formativo e sperimentale per i clienti Namirial**, che consente di comprendere l'ampiezza delle minaccia quantistica e di sperimentare direttamente l'applicabilità delle soluzioni proposte;
- lo **sviluppo di una modalità avanzata di integrazione tra crittografia post-quantum e reti quantistiche per la distribuzione delle chiavi**.

Questo lavoro posiziona Namirial come **abilitatore industriale della transizione post-quantum**, anticipando un **cambiamento** che non è più opzionale, ma anzi **necessario per garantire fiducia, validità legale e protezione dei dati nel lungo periodo**.

SOMMARIO

1. Introduzione

Una discontinuità storica nella sicurezza digitale

La sicurezza digitale globale ha superato un punto di non ritorno.
Namirial ha dimostrato in modo pratico, riproducibile e verificabile che un computer quantistico reale può essere programmato per attaccare i meccanismi crittografici alla base della fiducia digitale.
Questo risultato segna l'inizio concreto dell'era post-quantum.

Non teoria, non simulazione: hardware quantistico reale

Non si tratta di una simulazione teorica, né di una previsione futura. **È una sperimentazione reale, eseguita su hardware quantistico operativo AWS Braket**, che dimostra senza ambiguità che la minaccia quantistica **non è più un'ipotesi**, ma una realtà tecnologica misurabile.
Con questa iniziativa, **Namirial è la prima realtà industriale a portare il quantum computing fuori dall'ambito accademico e dentro il perimetro operativo della sicurezza digitale**.

Un primato industriale che cambia le regole del settore

Questo non è un risultato incrementale. È un **primato** che ridefinisce il modo in cui il settore deve affrontare il futuro della crittografia.
Per decenni, la sicurezza di documenti, identità digitali, comunicazioni e transazioni si è basata su algoritmi considerati "sicuri nel lungo periodo". **Questa certezza non esiste più.** L'algoritmo in grado di violare la crittografia a chiave pubblica **esiste già, funziona su hardware reale e non richiede nuove scoperte teoriche**. L'unico limite è la maturità dell'hardware quantistico, che sta avanzando rapidamente.

Perché questa sperimentazione è fondamentale per la sicurezza

La sperimentazione di Namirial è cruciale perché **trasforma un rischio astratto in una evidenza concreta**.
Dimostra che il problema non è *se* la crittografia classica verrà superata, ma **quando**. E dimostra che **chi non si prepara ora perderà la capacità di garantire fiducia nel tempo**.
La sicurezza digitale non riguarda solo la protezione immediata, ma la **durabilità della fiducia**: contratti firmati oggi, identità digitali, archivi documentali, registri sanitari, audit e infrastrutture critiche devono rimanere validi, verificabili e legalmente affidabili anche tra decenni.

Namirial sceglie di agire prima degli altri

Namirial ha scelto di assumersi questa responsabilità prima di chiunque altro.
Questa iniziativa non è un esercizio di ricerca fine a sé stesso, ma **un percorso strutturato di leadership tecnologica**, fondato su risultati concreti e immediatamente rilevanti per il mercato.

I primati di Namirial nella sicurezza post-quantum

Questo lavoro si basa su **quattro primati chiari e inequivocabili**:

- **Prima dimostrazione pratica industriale di un attacco quantistico alla crittografia a chiave pubblica eseguita su hardware reale**
- **Validazione diretta degli algoritmi post-quantum standardizzati dal NIST su infrastrutture industriali**
- **Implementazione concreta di firme digitali post-quantum su documenti PDF, pronte per test e adozione**
- **Partecipazione allo sviluppo della prima rete quantistica metropolitana multi-nodo che integra QKD e crittografia post-quantum**

Questi elementi posizionano Namirial come **abilitatore della sicurezza post-quantum**, non come osservatore.

Aprire oggi l'era della sicurezza di domani

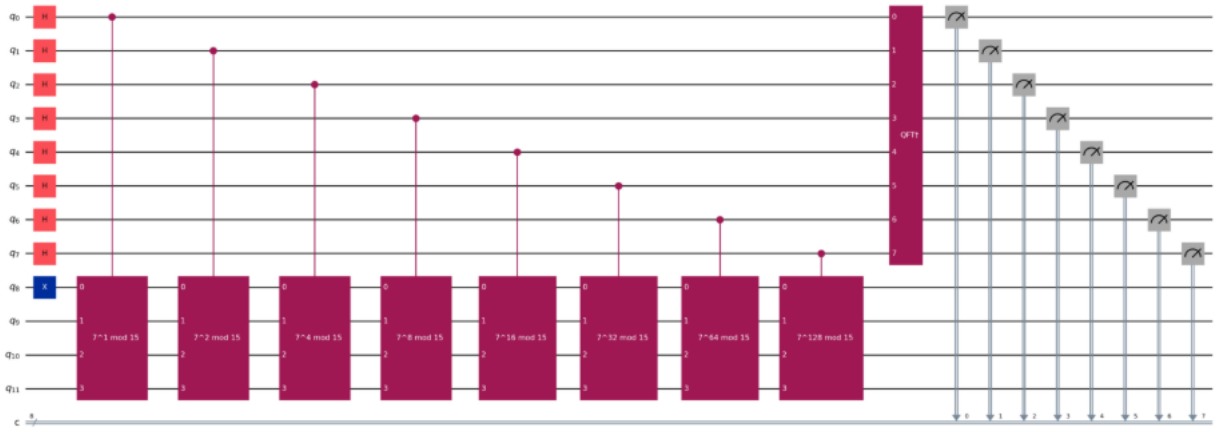
La transizione alla sicurezza post-quantum **non è opzionale**. È una necessità strategica per governi, imprese e infrastrutture critiche.
La sperimentazione descritta in questo documento è quindi **fondamentale per la sicurezza digitale**, perché fornisce evidenze reali, indica una direzione concreta e dimostra che esistono già oggi soluzioni praticabili.
Con questo lavoro, **Namirial apre ufficialmente l'era della sicurezza post-quantum** e pone le basi per una nuova generazione di servizi di fiducia, progettati per resistere non solo alle minacce di oggi, ma a quelle di domani.

Non un futuro ipotetico. Una realtà che è già iniziata.

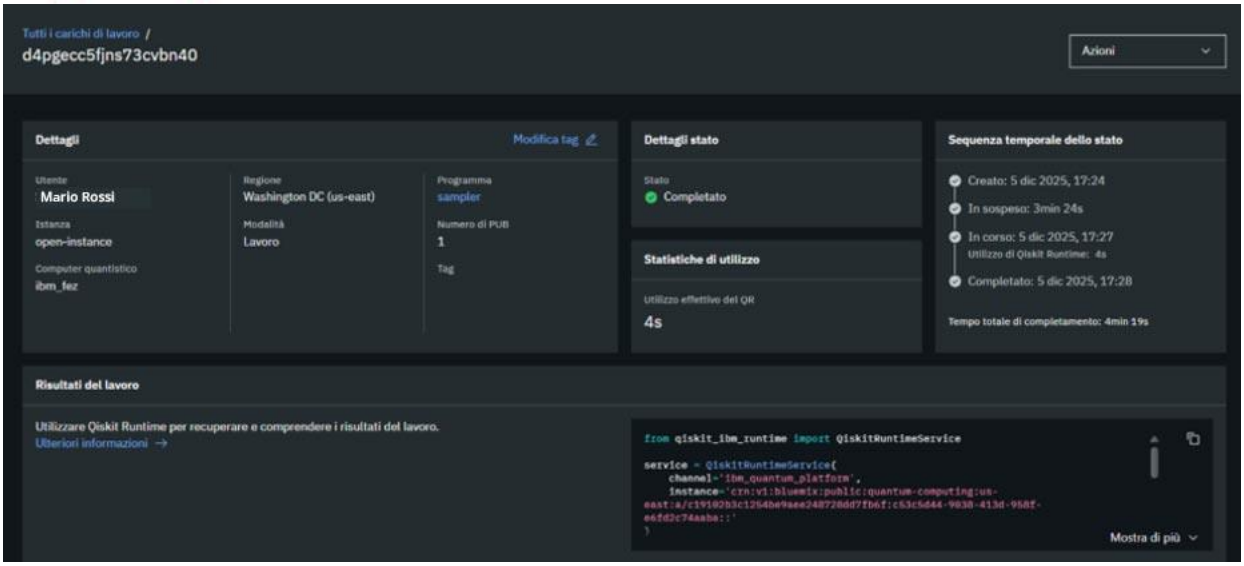
Questo white paper non descrive un futuro lontano. **Descrive ciò che è già iniziato — e chi lo sta guidando. Namirial.**

2. Sperimentazione Computer Quantistico IBM

Namirial ha condotto una **sperimentazione utilizzando hardware quantistico AWS Braket**, accessibile via cloud, per dimostrare la vulnerabilità delle chiavi crittografiche RSA rispetto ai computer quantistici. Poiché la crittografia RSA si basa sui numeri primi, l'esperimento ha utilizzato l'algoritmo di Shor per fattorizzare un modulo RSA e calcolare la chiave privata, dimostrando concretamente le potenzialità e le minacce del quantum computing applicato alla crittografia odierna.
Ai fini dell'esperimento, è stato realizzato un circuito quantistico basato sull'algoritmo di Shor per **fattorizzare il modulo RSA N = 15, composto dai fattori primi p = 3 e q = 5**. Questo valore è stato scelto come caso di studio poiché rappresenta il più piccolo numero semiprimo non banale richiedente **12 qubit**, una configurazione fattibile sull'hardware attualmente disponibile, permettendo di validare l'intero processo end-to-end su un computer quantistico reale.

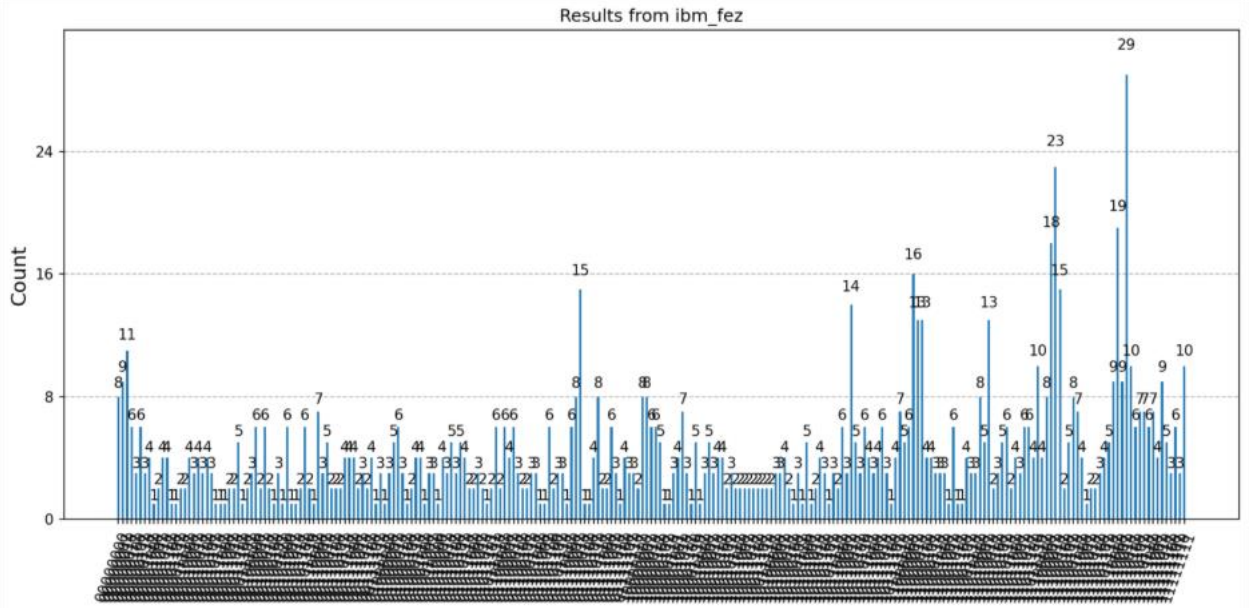


La figura mostra il circuito quantistico completo utilizzato per fattorizzare N=15. Si tratta di una sequenza di circa 75.000 operazioni quantistiche (gate) distribuite sui 12 qubit. Le linee orizzontali rappresentano i singoli qubit, mentre i simboli grafici lungo queste linee sono i gate quantistici che manipolano gli stati.
Una volta creato il circuito, esso è stato inviato al computer quantistico; Il circuito è stato quindi accettato ed **eseguito in circa 4 secondi** ed al termine è stato rilasciato un riassunto del risultato dell'esecuzione.



L'immagine mostra l'interfaccia della piattaforma **che conferma l'esecuzione del codice di Namirial su hardware quantistico reale**. Nella sezione "Dettagli" si visualizza l'utente, la regione del datacenter (Washington DC - us-east1), la modalità di lavoro e il numero di PUB (Primitive Unified Bloc) utilizzato.

I risultati delle misurazioni quantistiche sono stati quindi analizzati per estrarre la fase quantistica che codifica il periodo della funzione f(x) = 7^x mod 15. Da questo periodo sono stati calcolati i fattori primi, completando così la fattorizzazione. Con i fattori p e q ottenuti, si è potuto immediatamente recuperare la chiave privata RSA e poi successivamente la chiave pubblica.



Questo grafico mostra, con la sua variabilità, il rumore che si ha quando si effettua questo tipo di calcoli su un computer quantistico. La variabilità è dovuta alla cosiddetta *decoerenza quantistica*, che è dovuta al fatto che i computer quantistici hanno forti errori (che devono essere compensati) dovuti a varie condizioni tecnologiche ed ambientali. Questi errori sono quelli che impediscono di fattorizzare vere chiavi RSA. La ricerca tecnologica è oggi orientata a limitare questi errori.

Questo esperimento evidenzia sia la fattibilità pratica dell'algoritmo su hardware reale, sia le attuali limitazioni tecnologiche dei computer quantistici NISQ (Noisy Intermediate-Scale Quantum). **L'algoritmo di Shor funziona su hardware quantistico reale e non è solo teoria**.

Con più qubit disponibili, chiavi più grandi possono essere fattorizzate, non occorre sviluppare nuovi algoritmi, solo nuovi computer. In particolare, per violare con successo la crittografia RSA-2048 sono necessari circa 4000 qubit logici, che i computer quantistici potrebbero avere a disposizione dal 2030 in poi.

3. Studio e Sperimentazione degli Algoritmi Post-Quantistici

Al netto di questi risultati, che hanno dimostrato concretamente la vulnerabilità di RSA di fronte ai computer quantistici, Namirial ha **investito nello studio, analisi e validazione di algoritmi post-quantistici**, riconoscendo l'urgenza di prepararsi alla transizione crittografica che l'industria dovrà affrontare nei prossimi anni.

All'interno degli studi sviluppati, hanno ricevuto particolare approfondimento gli algoritmi standardizzati dal NIST (National Institute of Standards and Technology) nel 2024, che rappresentano il riferimento internazionale per la crittografia resistente ai computer quantistici. Essi sono stati analizzati e testati conducendo **benchmark approfonditi** sulle diverse soluzioni, valutando parametri critici quali prestazioni computazionali, dimensioni delle chiavi, overhead di banda e compatibilità con le infrastrutture esistenti.

Nello specifico, sono stati oggetto di indagine:

- **CRYSTALS-Kyber** per la **crittografia** (key encapsulation mechanism);
- **CRYSTALS-Dilithium** per la **firma digitale** (signature scheme basato su reticoli);
- **FALCON** per la **firma digitale** (signature scheme compatto e performante).

Questa selezione è particolarmente rilevante in quanto **sono e saranno gli algoritmi di riferimento per il settore del trust management nell'epoca post-quantum**.

Namirial ha partecipato e presentato i suoi risultati alla sesta NIST PQC Standardization Conference tenutasi in America a fine 2025, un evento di riferimento internazionale che riunisce i massimi esperti nel settore della crittografia. Durante la conferenza, la delegazione di Namirial ha avuto l'opportunità di discutere con i membri del NIST circa i passi da seguire per l'adozione degli standard e come la standardizzazione continuerà ad evolversi nei prossimi anni.

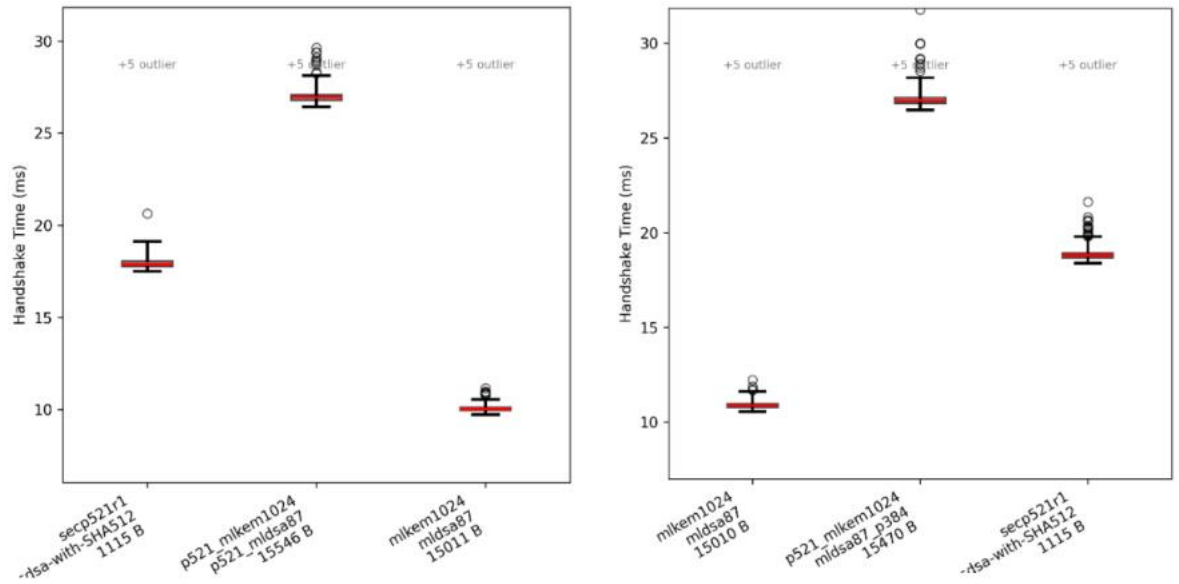
Questi incontri diretti con gli standardizzatori hanno fornito insight preziosi su:

- Le roadmap di implementazione raccomandate per le diverse industrie;
- Gli aggiornamenti futuri degli standard (round aggiuntivi di valutazione);
- Le best practices per la migrazione da algoritmi classici a post-quantistici;
- Le tempistiche realistiche per la deprecazione di RSA e ECDSA.

I benchmark condotti sui tre algoritmi selezionati hanno prodotto risultati cruciali che confermano la maturità e l'applicabilità concreta di queste soluzioni. È fondamentale precisare che i test di seguito descritti sono stati eseguiti su HSM (Hardware Security Module) industriali, dispositivi crittografici certificati utilizzati in ambienti produttivi per garantire la massima sicurezza nelle operazioni di firma e crittografia.

CRYSTALS-Kyber (Key Encapsulation Mechanism):

Kyber è stato testato nelle sue varianti di sicurezza (Kyber-512, Kyber-768, Kyber-1024) per valutare le prestazioni in scenari di key exchange. I risultati mostrano tempi di generazione chiavi e operazioni di encapsulation/decapsulation nell'ordine dei **millisecondi**, rendendolo estremamente efficiente per applicazioni ad alto throughput. **Kyber emerge come soluzione ottimale per sostituire RSA-2048 nel key exchange**, offrendo prestazioni superiori con garanzie di sicurezza post-quantistica. Il throughput misurato conferma la sua idoneità per connessioni HTTPS, VPN e protocolli di comunicazione sicura su larga scala.



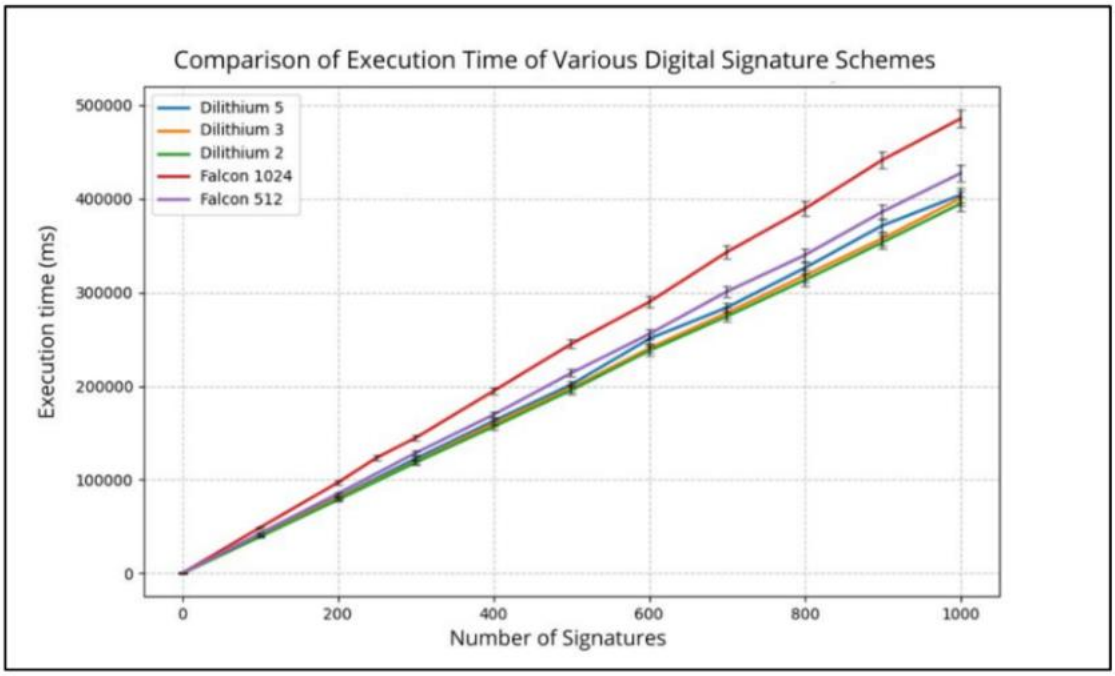
Questi grafici box-plot mostrano la consistenza delle performance con variabilità minima, confermando l'affidabilità delle implementazioni.

CRYSTALS-Dilithium (Digital Signature):

Dilithium è stato valutato nei suoi livelli di sicurezza (Dilithium2, Dilithium3, Dilithium5) con focus su operazioni di firma e verifica. I test dimostrano che **la generazione di firme digitali avviene in tempi** nettamente inferiori al secondo. La **verifica delle firme risulta particolarmente veloce**, caratteristica critica per sistemi che devono validare grandi volumi di documenti. Le **dimensioni delle firme sono accettabili per la maggior parte delle applicazioni**, specialmente considerando il beneficio della sicurezza quantistica. Dilithium si conferma come candidato robusto per sostituire RSA nelle firme digitali, particolarmente adatto per documenti legali e certificati digitali dove Namirial opera quotidianamente.

FALCON (Fast Fourier Lattice-based Compact Signatures):

FALCON è stato testato specificamente per valutare le sue caratteristiche di compattezza e velocità. I risultati evidenziano **firme significativamente più compatte** rispetto a Dilithium, rendendolo ideale per ambienti con vincoli di banda o storage. Le **prestazioni di firma e verifica sono eccellenti**, posizionandosi tra le più veloci della categoria lattice-based. FALCON risulta particolarmente efficiente per **applicazioni real-time** e scenari mobile, dove dimensioni contenute e bassa latenza sono critici. Il trade-off rispetto a Dilithium è una maggiore complessità implementativa, ma i benefici in termini di prestazioni lo rendono attraente per casi d'uso specifici , come la **firma massiva di documenti e applicazioni embedded**.



Come visibile nel grafico comparativo, Dilithium2 (verde) è il più veloce completando 1000 firme in circa 390 secondi, mentre FALCON1024 (rosso) richiede circa 490 secondi, risultando leggermente più lento delle varianti Dilithium a parità di numero di firme, in quanto più complesso.

I test sono stati condotti su HSM la cui architettura hardware è attualmente ottimizzata per RSA, con circuiteria dedicata progettata specificamente per eseguire esponenziali modulari ad alte prestazioni. Questo significa che i confronti diretti con RSA in termini di throughput assoluto non sono rappresentativi delle potenzialità reali degli algoritmi post-quantistici, in quanto sono eseguiti su hardware sicuro ma non ottimizzato.

Tuttavia, guardando al futuro, i produttori di HSM stanno già sviluppando nuove generazioni di dispositivi con firmware aggiornato che includerà nativamente il supporto agli algoritmi post-quantistici. Inoltre, sono in fase di progettazione supporti hardware ottimizzati come FPGA. Quando questi HSM di nuova generazione saranno disponibili, ci si aspetta che le performance degli algoritmi PQC si avvicinino significativamente o superino quelle attuali di RSA, eliminando ogni gap.

Per Namirial, questo significa che la transizione può iniziare subito, con approcci ibridi che garantiscano compatibilità retroattiva mentre si costruisce protezione contro la futura minaccia quantistica. L'adozione graduale permetterà di beneficiare della sicurezza post-quantistica mentre l'ecosistema hardware si evolve per offrire performance ottimali.

Questi risultati confermano che la transizione alla crittografia post-quantistica è tecnicamente fattibile oggi e che Namirial è pronta a guidare i propri clienti in questo percorso critico, garantendo continuità operativa e sicurezza a lungo termine per i servizi di firma digitale e crittografia che costituiscono il core business aziendale.

4. Implementazione Demo Firma Post-Quantum

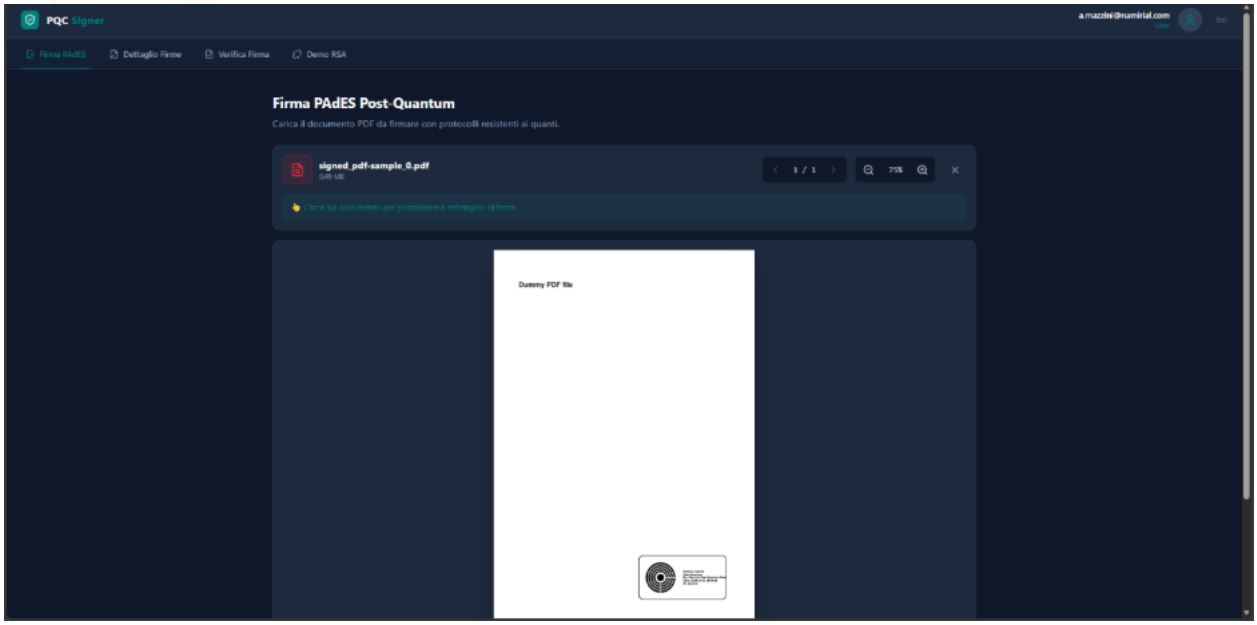
Come emerso nello studio dei diversi algoritmi di firma, è emerso che CRYSTALS-Dilithium3 è l'algoritmo ottimale per l'implementazione di firme digitali nei sistemi di produzione di Namirial. Questa scelta è motivata da una serie di fattori come:

- Bilanciamento prestazioni/sicurezza: offre il miglior compromesso tra velocità di firma (~100 firme/secondo su HSM) e livello di sicurezza adeguato (equivalente AES-128);
- Dimensioni firme ottimale: giusto bilanciamento tra la compattezza di Dilithium2 e l'estrema grandezza di Dilithium5, riducendo overhead di storage e banda;
- Standardizzazione NIST: algoritmo ufficialmente standardizzato come FIPS 204, garantendo interoperabilità e compliance normativa;
- Maturità implementativa: librerie robuste e testate disponibili per integrazione in ambienti enterprise.

Namirial ha sviluppato un applicativo web, accessibile ai propri clienti su richiesta, che implementa le seguenti funzionalità innovative di firma post-quantum.

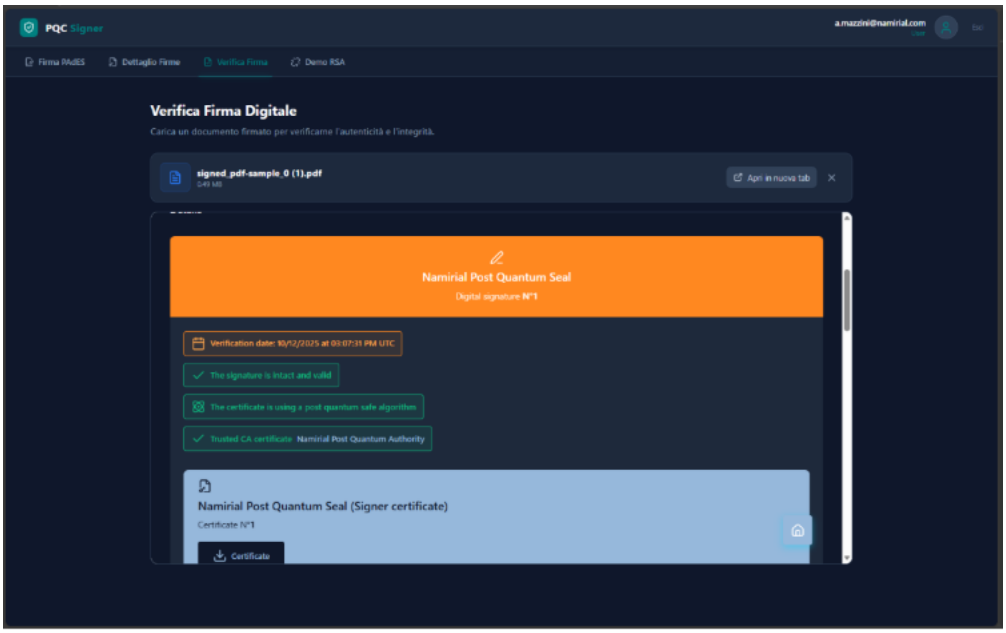
Processo di firma PAdES Post-Quantum

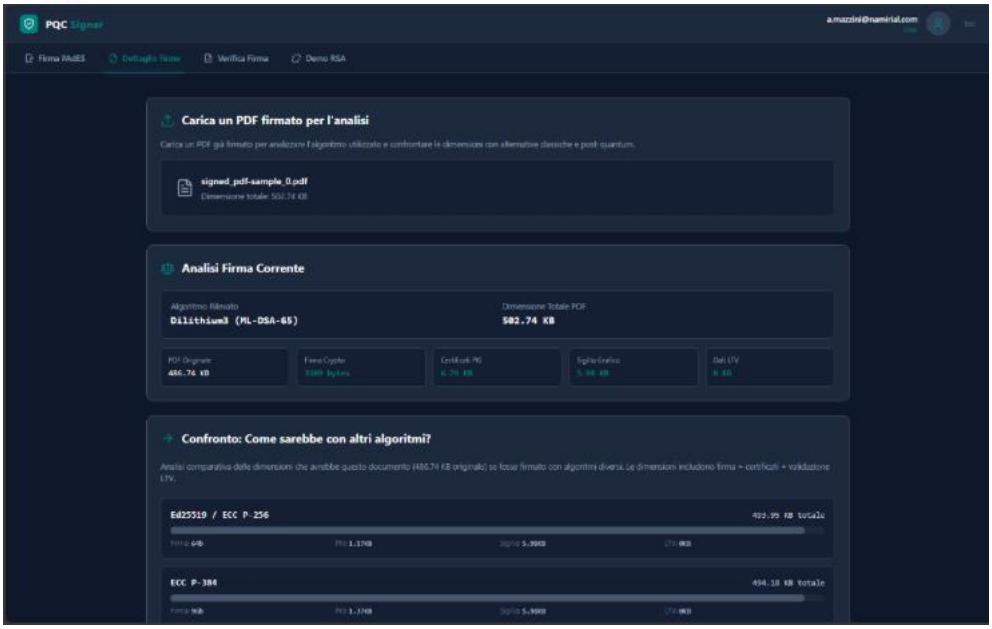
- Generazione firma PAdES, utilizzando certificato di firma basato su crittografia post-quantum;
- Inserimento di firma grafica visibile nel documento con posizionamento personalizzabile;
- Embedding della firma crittografica nel PDF secondo standard PAdES (PDF Advanced Electronic Signatures);
- Supporto ai metadati (timestamp, CRL).



Verifica Firma PAdES Post-Quantum

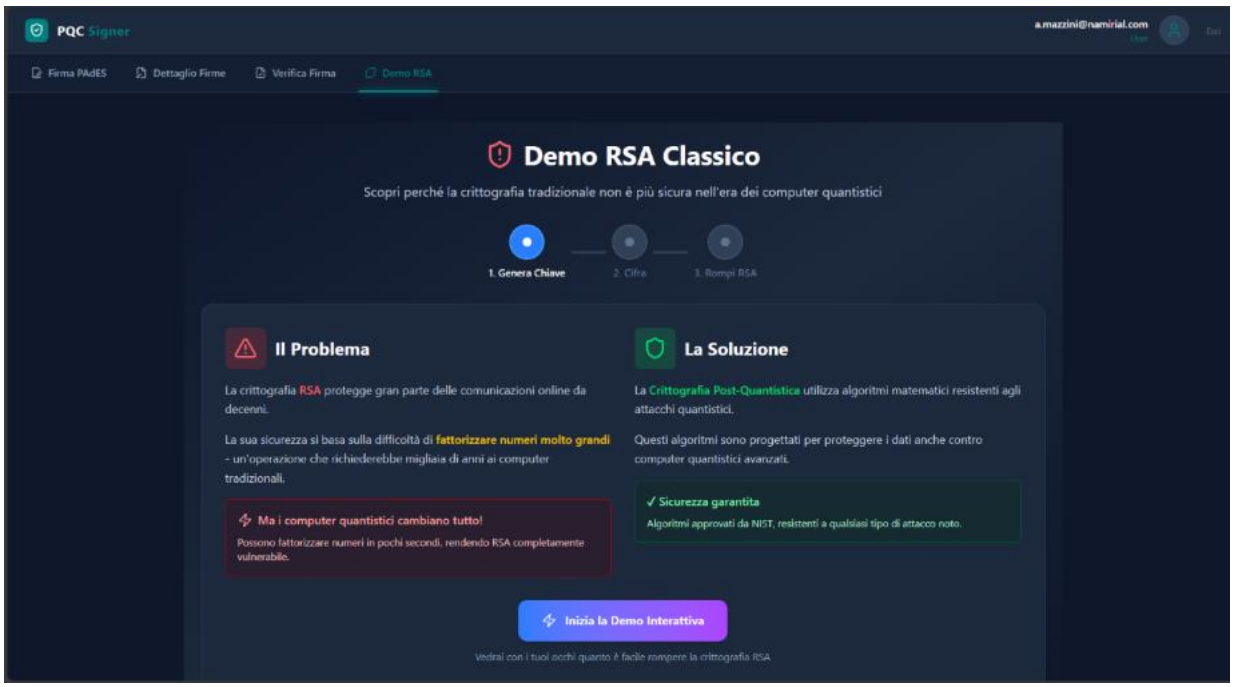
- Validazione crittografica della firma Dilithium3 rispetto al contenuto del documento;
- Controllo integrità e rilevamento di qualsiasi modifica post-firma;
- Visualizzazione dello stato di validità con interfaccia user-friendly;
- Report dettagliati per audit e compliance.

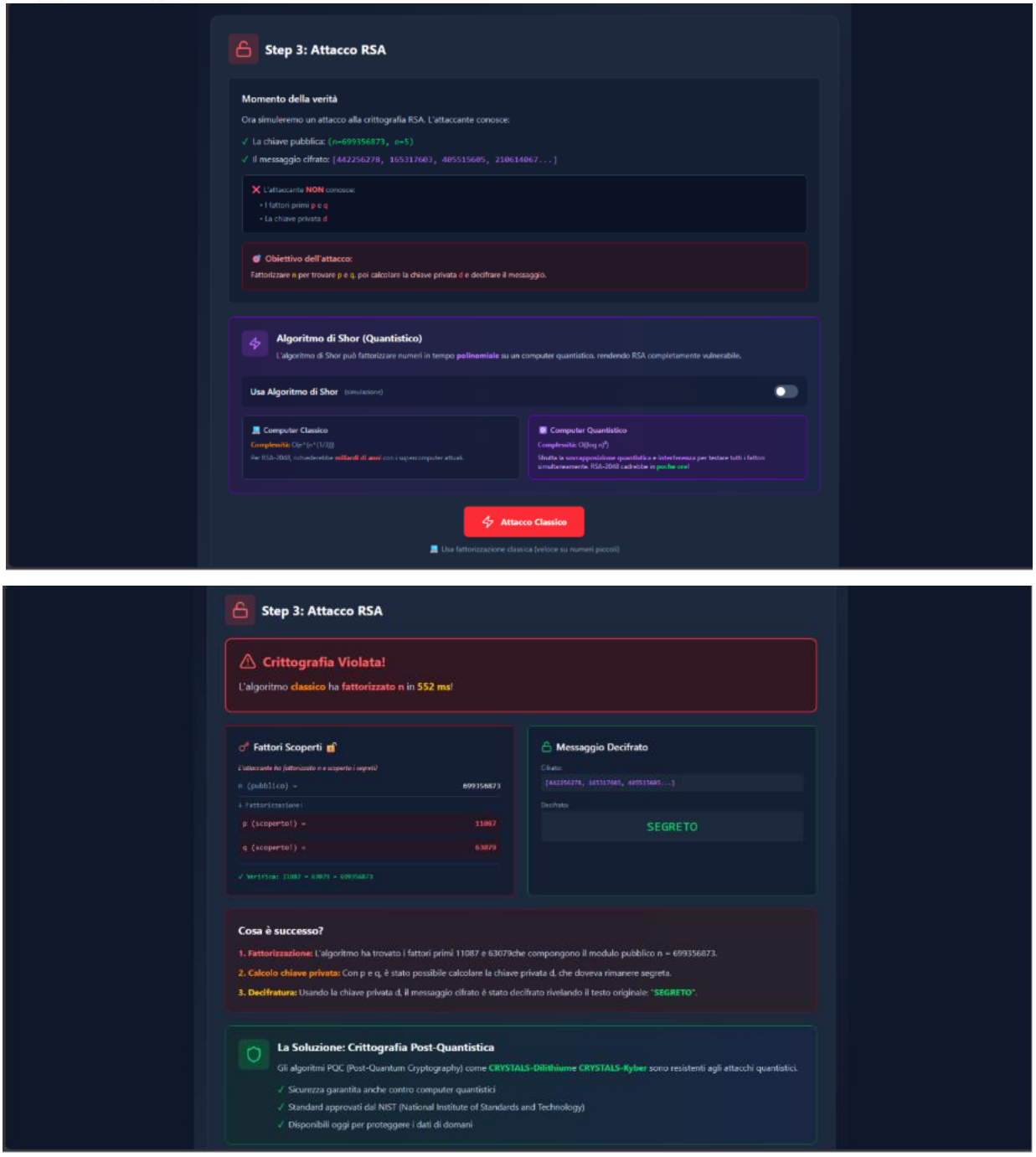




Test Interattivo violazione crittografia RSA, rappresenta da una demo che consente di creare una chiave RSA e tramite algoritmo di Shor violare la stessa:

- Creazione chiave RSA;
- Cifratura del messaggio scelto tramite interfaccia;
- Rottura chiave RSA e decifratura del messaggio crittografato.





Questo applicativo rappresenta più di una proof-of-concept: è una dimostrazione concreta che **Namirial può già oggi offrire ai propri clienti soluzioni di firma digitale resistenti alla minaccia quantistica**.

5. Combinazione QKD e Post-Quantum

Namirial ha esteso il proprio impegno nella sicurezza quantistica, collaborando con l'università di Napoli Federico II e il Centro di Competenza Meditech per lo **sviluppo di un sistema che integra sia crittografia quantistica (QKD - Quantum Key Distribution) che crittografia post-quantum (PQC)**. Questa sinergia rappresenta un approccio ibrido all'avanguardia, combinando la sicurezza fisica garantita dalle leggi della meccanica quantistica con la robustezza computazionale degli algoritmi post-quantistici.

La collaborazione con la Casa delle Tecnologie Emergenti di Napoli e il Centro di Competenza Meditech ha portato **all'inaugurazione della prima rete nazionale permanente di comunicazione quantistica multi-nodi metropolitana**. Il sistema sviluppato implementa un approccio ibrido dual-layer che combina:

Quantum Key Distribution (QKD):

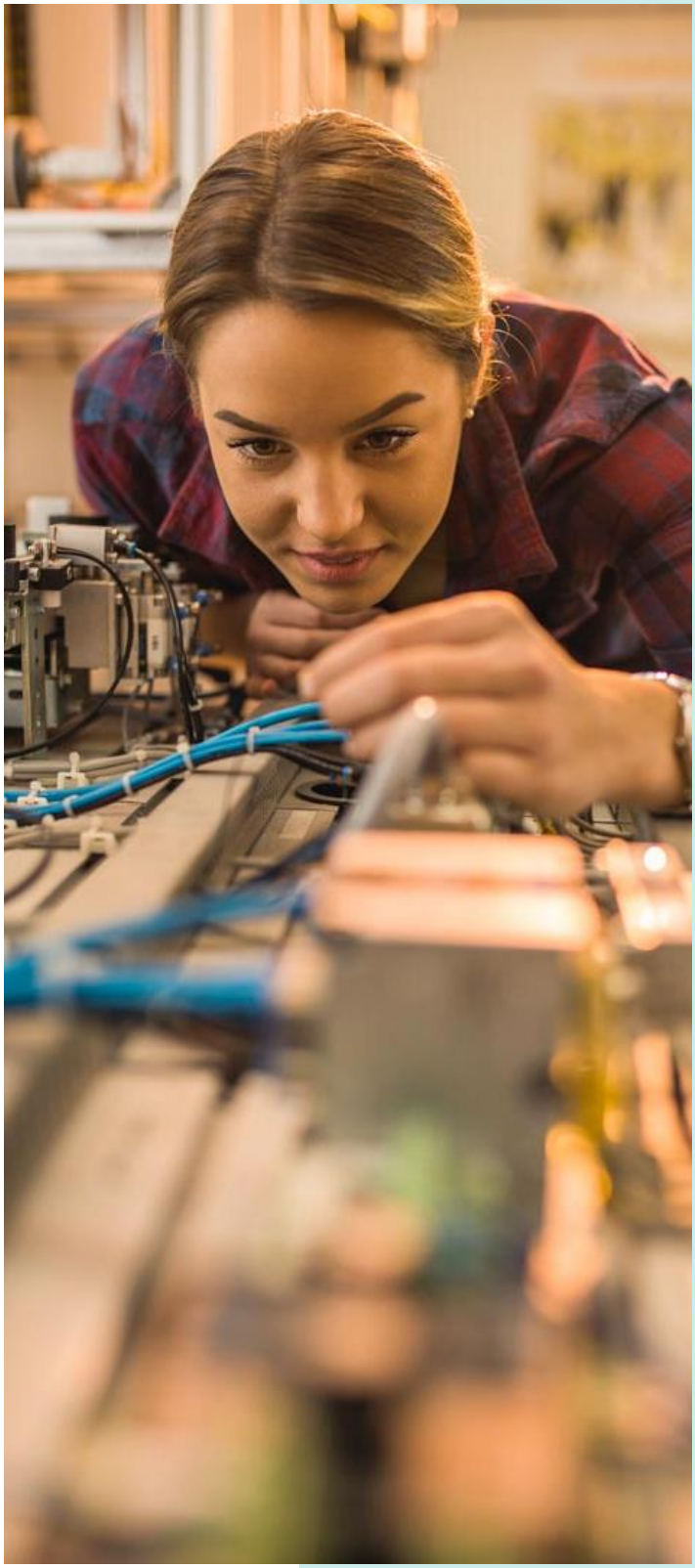
- Distribuzione di chiavi crittografiche tramite fotoni singoli su fibra ottica
- Sicurezza garantita dai principi fisici della meccanica quantistica (no-cloning theorem)
- Rilevamento automatico di tentativi di intercettazione (QBER - Quantum Bit Error Rate monitoring)
- Protocolli standard: BB84, E91 per generazione e distribuzione chiavi quantistiche

Post-Quantum Cryptography (PQC):

- Utilizzo di algoritmi Dilithium2/3/5 FALCON512/1024 per firma digitale dei messaggi trasmessi sulla rete quantistica
- Kyber per incapsulamento chiavi (KEM - Key Encapsulation Mechanism) nei layer applicativi
- Autenticazione end-to-end resistente a computer quantistici
- Compatibilità con standard NIST FIPS 203/204

La partecipazione a questo progetto di rilevanza nazionale conferma il ruolo di Namirial come attore chiave nell'ecosistema della sicurezza quantistica italiana.

L'esperienza acquisita nella progettazione e implementazione di sistemi ibridi QKD/PQC posiziona l'azienda per una certificazione avanzata ovvero una validazione su infrastrutture quantistiche reali, non solo simulatori e competenze uniche nel panorama italiano su integrazione QKD/PQC.



Per scoprire di più visita la pagina:

namirial.com/it/future/post-quantum-cryptography/

namirial.com