Allegato A

Titolo del progetto di ricerca	Architetture Hardware per la Post-Quantum Cryptography: progettazione e ottimizzazione per sistemi avanzati
Obiettivi del progetto	L'obiettivo di questo progetto è sviluppare e ottimizzare **soluzioni di accelerazione hardware** per primitive crittografiche di **Post-Quantum Cryptography (PQC)**, con un focus specifico sulle **applicazioni spaziali** e sulle **infrastrutture critiche**. In un contesto in cui l'avvento dei computer quantistici mette a rischio i sistemi di sicurezza tradizionali, la ricerca di **soluzioni crittografiche resistenti e implementabili in hardware** diventa essenziale per garantire la protezione delle comunicazioni e dei dati, soprattutto in ambienti operativi complessi come quelli spaziali. Il progetto affronta le sfide legate all'**efficienza computazionale**, alla **sicurezza** e alla **scalabilità** delle primitive PQC, progettando **architetture dedicate basate su acceleratori specializzati** e supportando l'integrazione con sistemi open-source come **RISC-V**. L'attività di ricerca esplorerà due approcci principali per migliorare le prestazioni delle primitive PQC: 1. **Acceleratori tightly coupled**: estensioni dell'**instruction set RISC-V** per l'esecuzione efficiente di operazioni crittografiche, riducendo il tempo di elaborazione e ottimizzando l'uso delle risorse hardware. 2. **Acceleratori loosely coupled**: unità hardware **memory-mapped** dedicate, progettate per garantire performance e scalabilità, adattandosi a diversi algoritmi post-quantum. **<u>Applicazioni per i sistemi spaziali</u>** Il progetto si distingue per il suo focus sulle **applicazioni spaziali**, un settore in cui la **sicurezza delle comunicazioni e dei dati** è fondamentale per il successo delle missioni e la protezione delle infrastrutture orbitali. Le sfide critiche includono: • **Ambienti ostili e vincoli hardware**: i sistemi spaziali devono operare in condizioni di radiazione elevata, con risorse computazionali limitate e requisiti di affidabilità stringenti. • **Protezione delle comunicazioni satellitari**: la necessità di garantire **autenticità, integrità e riservatezza** nei protocolli di comunicazione tra satelliti, stazioni di terra e assetti orbitanti.

	• **Resilienza agli attacchi fisici e cyber**: mitigazione di minacce come gli **attacchi side-channel**, il **fault injection** e le interferenze elettromagnetiche. L'integrazione di **acceleratori PQC nei sistemi spaziali** è quindi un passo essenziale per garantire una **cybersicurezza quantistica-ready** in conformità con le direttive **ESA** e con la normativa italiana sulla **space economy**. **<u>Obiettivi specifici</u>** Il progetto si propone di: • **Definire estensioni ISA per RISC-V**, ottimizzate per le operazioni di algebra lineare e trasformazioni matematiche richieste dagli algoritmi PQC. • **Progettare e implementare acceleratori hardware** dedicati a primitive PQC, con un focus su prestazioni, consumo energetico e **resistenza agli attacchi fisici**. • **Sviluppare una piattaforma di benchmarking** per valutare le prestazioni e la sicurezza degli acceleratori rispetto alle implementazioni software ottimizzate. • **Validare le soluzioni su FPGA**, con test su scenari reali, inclusa l'integrazione in **sistemi embedded, cloud e piattaforme spaziali**. **<u>Impatto del progetto</u>** L'impatto del progetto è duplice: 1. **Rafforzare la sicurezza informatica nazionale e spaziale**, fornendo soluzioni hardware in grado di proteggere le comunicazioni e i dati delle infrastrutture critiche, incluse quelle orbitali. 2. **Supportare l'adozione di architetture open-source** come **RISC-V**, promuovendo un ecosistema tecnologico **sicuro**, **indipendente e trasparente**, riducendo la dipendenza da tecnologie proprietarie. Grazie a questo progetto, sarà possibile colmare il divario tra le attuali capacità crittografiche e le esigenze future imposte dalla **transizione verso l'era post-quantistica**, garantendo che i sistemi spaziali e terrestri siano dotati di soluzioni crittografiche avanzate, efficienti e sicure, in linea con le direttive internazionali e nazionali.

Pertinenza del progetto agli argomenti dell'Agenda di Ricerca e Innovazione per la Cybersicurezza 2023 - 2026	Il progetto si allinea alle priorità dell'**Agenda di Ricerca e Innovazione per la Cybersicurezza 2023-2026**, con un focus sulle **applicazioni spaziali della Post-Quantum Cryptography (PQC)**. In particolare, risponde all'**argomento 1.2.1 – Primitive, algoritmi e protocolli per PQC**, sviluppando **acceleratori hardware** per migliorare l'efficienza e la sicurezza degli algoritmi crittografici post-quantum. Questa ricerca è fondamentale per garantire la protezione di comunicazioni e dati sensibili, soprattutto in ambienti ad alta criticità come lo spazio. Il progetto contribuisce inoltre all'**area 2.3.1 – Resilienza dei sistemi cyber-fisici**, poiché i **sistemi spaziali**, dai satelliti alle stazioni di terra, devono essere protetti da attacchi informatici e fisici. L'implementazione hardware della PQC aumenta la robustezza delle infrastrutture critiche, mitigando minacce come attacchi **side-channel e fault injection**. Un altro aspetto chiave riguarda l'**argomento 4.2.2 – Approcci per la sicurezza dei sistemi IoT**, considerando che i dispositivi spaziali condividono molte caratteristiche dei sistemi IoT, tra cui **vincoli energetici e computazionali**. Il progetto sviluppa soluzioni di **accelerazione hardware** per consentire l'adozione della PQC in questi scenari senza comprometterne le prestazioni. Infine, il progetto supporta l'**argomento 5.3.2 – Modelli e regole per favorire l'autonomia strategica**, sviluppando soluzioni crittografiche **open-source e scalabili**, riducendo la dipendenza da tecnologie proprietarie. Questo rafforza la capacità dell'Italia e dell'Europa di proteggere le proprie infrastrutture strategiche, in linea con le direttive **ESA** e con la normativa nazionale sulla **space economy**. Il progetto rappresenta quindi un passo avanti nella protezione delle infrastrutture critiche, garantendo **soluzioni hardware avanzate per la cybersicurezza nell'era post-quantistica**.
Modalità di realizzazione del progetto, anche in termini di fattori abilitanti a disposizione	Il progetto seguirà un approccio **iterativo e modulare**, articolato in più fasi per garantire **efficienza, sicurezza e scalabilità** delle soluzioni hardware per **Post-Quantum Cryptography (PQC)**, con particolare attenzione alle **applicazioni spaziali**. Le principali fasi di sviluppo saranno: 1. **Analisi e selezione degli algoritmi**: individuazione delle primitive PQC più adatte per implementazioni hardware, valutando prestazioni, sicurezza e idoneità per ambienti critici come lo spazio.

	2. **Definizione dell'architettura**: progettazione di estensioni **ISA per RISC-V** (tightly coupled) e di **acceleratori hardware memory-mapped** (loosely coupled), ottimizzando il bilanciamento tra potenza computazionale, consumo energetico e area occupata. 3. **Implementazione hardware**: sviluppo e test su **FPGA**, con successiva ottimizzazione per garantire robustezza e affidabilità in ambienti ostili. 4. **Benchmarking e sicurezza**: confronto con implementazioni software, analisi delle prestazioni e valutazione della **resistenza agli attacchi fisici**, inclusi **side-channel e fault injection**. 5. **Validazione e integrazione**: testing su scenari reali, con particolare attenzione all'integrazione in **sistemi embedded, cloud e piattaforme spaziali**. Il progetto sfrutterà diversi **fattori abilitanti** già disponibili: • **L'adozione di architetture open-source come RISC-V**, che consente l'integrazione di estensioni dedicate e riduce la dipendenza da tecnologie proprietarie. • **Piattaforme FPGA**, fondamentali per la prototipazione e il testing in scenari operativi. • **Competenze avanzate in progettazione hardware e sicurezza informatica**, con esperienza nell'ottimizzazione di acceleratori crittografici. • **Collaborazioni con enti di ricerca e aziende del settore spaziale**, per garantire l'applicabilità delle soluzioni in contesti reali. Questa strategia permetterà di sviluppare **soluzioni sicure ed efficienti**, rispondendo alle esigenze della **cybersicurezza post-quantum** e delle **infrastrutture critiche spaziali**.	
ELEMENTI DEL PROGETTO RELATIVI ALLE TEMATICHE PRIORITARIE del Bando per il finanziamento di borse di dottorato di ricerca nel settore della cybersicurezza - XLI Ciclo di dottorato ***(art. 4 comma 3 e art. 6 comma 3 del Bando)***		
Contributo distintivo del progetto in relazione agli argomenti prioritari	**Argomento/i prioritario/i**	**1.2.1 – Primitive, algoritmi e protocolli per PQC** **2.3.1 – Resilienza dei sistemi cyber-fisici** **4.2.2 – Approcci per la sicurezza dei sistemi IoT** **5.3.2 – Modelli e regole per favorire l'autonomia strategica**

	Il progetto introduce un contributo innovativo alla **Post-Quantum Cryptography (PQC)**, con un focus particolare sulle **applicazioni spaziali e sui sistemi critici**. Per l'**argomento 1.2.1 – Primitive, algoritmi e protocolli per PQC**, il progetto sviluppa **architetture hardware dedicate** per migliorare l'efficienza computazionale delle primitive crittografiche post-quantum. L'adozione di acceleratori specializzati consente di ridurre il consumo energetico e ottimizzare l'esecuzione di questi algoritmi in **contesti ad alte prestazioni e con risorse limitate**, come i sistemi embedded spaziali. In riferimento all'**argomento 2.3.1 – Resilienza dei sistemi cyber-fisici**, il progetto affronta la protezione delle **infrastrutture critiche, terrestri e spaziali**, contro attacchi cyber e fisici. Le implementazioni hardware PQC progettate saranno **resistenti a fault injection, attacchi side-channel e disturbi ambientali**, garantendo la sicurezza delle comunicazioni satellitari e delle reti spaziali. Per quanto riguarda l'**argomento 4.2.2 – Approcci per la sicurezza dei sistemi IoT**, il progetto si concentra sull'integrazione della PQC in dispositivi a **basso consumo e alta efficienza**, tipici di applicazioni IoT e spaziali. Gli acceleratori hardware sviluppati permetteranno di eseguire primitive crittografiche avanzate **senza compromettere le prestazioni** e rispettando i vincoli energetici dei dispositivi embedded utilizzati nelle infrastrutture orbitanti. Infine, il progetto supporta l'**argomento 5.3.2 – Modelli e regole per favorire l'autonomia strategica**, contribuendo alla creazione di **soluzioni hardware open-source e scalabili** per la sicurezza post-quantum. L'uso di **architetture aperte come RISC-V** riduce la dipendenza da tecnologie proprietarie, rafforzando la **capacità nazionale ed europea** di sviluppare e implementare tecnologie crittografiche avanzate per la protezione delle infrastrutture strategiche, incluse quelle spaziali.
Motivazione ed evidenze del coinvolgimento nel progetto di ricerca di imprese, enti e laboratori di ricerca pubblici o privati riconducibili a realtà italiane e/o europee, organismi internazionali	Il progetto prevede il coinvolgimento di **IngeniArs** (https://www.ingeniars.com/), spin-off dell'Università di Pisa specializzato in **acceleratori hardware per applicazioni spaziali**. L'azienda ha esperienza consolidata nel settore dell'**elaborazione a bordo di sistemi satellitari**, con un focus sulla sicurezza e l'efficienza computazionale. La collaborazione con IngeniArs permetterà di trasferire le soluzioni di **accelerazione hardware per la Post-Quantum Cryptography (PQC)** verso applicazioni reali nel settore aerospaziale. A livello europeo, il progetto si inserisce nel contesto della collaborazione con l'**Agenzia Spaziale Europea (ESA)**, con la quale è attivo un **Memorandum of Understanding (MoU)** che facilita lo **scambio di competenze, strumenti e il coinvolgimento di studenti in attività di ricerca e sviluppo**. In particolare, il progetto beneficerà delle sinergie con il **Centro di ricerca ESTEC** nei Paesi

	Bassi, nodo chiave per l'innovazione nella cybersecurity spaziale e la protezione delle infrastrutture critiche di **telecomunicazioni, navigazione e osservazione della Terra**. Infine, il gruppo di ricerca proponente ha partecipato al progetto **European Processor Initiative (EPI)**, contribuendo alla progettazione di **IP core per la crittografia** nei programmi **SGA1 e SGA2**. Questa esperienza fornirà competenze chiave per lo sviluppo di **acceleratori hardware per la PQC**, assicurando un forte legame con le strategie europee di autonomia tecnologica e sicurezza.
Svolgimento di un periodo di studio all'estero nei Paesi dell'Unione Europea contestualizzato al progetto di ricerca	Le attività di ricerca prevedono un periodo di studio presso il **Centro di ricerca ESTEC (European Space Research and Technology Centre)** dell'**Agenzia Spaziale Europea (ESA)** nei Paesi Bassi. Grazie al **Memorandum of Understanding (MoU) tra il laboratorio proponente ed ESA**, è già attiva una collaborazione per lo sviluppo congiunto di ricerche nel settore della **cybersicurezza per applicazioni spaziali**, facilitando lo **scambio di conoscenze, strumenti e risorse di laboratorio**. Durante il periodo all'ESTEC, il dottorando avrà accesso ai laboratori di ricerca ESA, dove potrà testare le **soluzioni hardware per la Post-Quantum Cryptography (PQC)** in scenari reali, valutandone **l'integrazione in infrastrutture critiche spaziali**. L'esperienza permetterà di confrontare le **implementazioni hardware sviluppate nel progetto con i requisiti di sicurezza e affidabilità** richiesti dai sistemi satellitari. Questa mobilità internazionale consentirà inoltre al dottorando di entrare in contatto con esperti di **cybersecurity spaziale**e partecipare a **programmi di ricerca ESA**, rafforzando le competenze necessarie per la transizione della PQC nel settore aerospaziale.
Durata del periodo all'estero *(Max 6 mesi finanziabili)*	6 mesi