Le sfide del Quantum Computing

Banche e Sicurezza

Milano, 14 maggio 2024

Lo sviluppo del computer quantistico mina gli algoritmi di crittografia asimmetrica

L'utilizzo di tecniche quantistiche risolve in tempi brevi (secondi o minuti) alcuni algoritmi di cifratura per cui l'aritmetica impiega troppo per rappresentare una minaccia (mesi o anni).

Questi algoritmi sono impiegati durante lo scambio iniziale della chiave della chiave crittografica.

Dunque il quantum computer rende vulnerabili i protocolli asimmetrici, mentre rimangono sicuri i protocolli simmetrici (es. AES, blowfish, …)

Esempi di use case a rischio

Applicazioni ✗

HTTPS
Navigazione sicura da browser web

VPN
Utilizzo della VPN per accedere alla rete aziendale

EMAIL
Invio e ricezione di email cifrate

APP BANCA
Accesso all'applicazione della Banca

Traffico WAN
Protezione del traffico fra Datacenter o verso le filiali

FIRMA DIGITALE
Validità della chiave di firma

Protocolli ✗

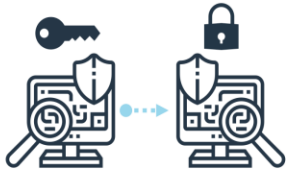
HTTPS *(Secure HTTP)* **PGP** *(Pretty good privacy)* **ECDSA** *(Elliptic Curve Digital Signature Algorithm)*

Algoritmi di cifratura Asimmetrica ✗

RSA *(Rivest, Shamir, Adleman)* **ECC** *(elliptic curve cryptography)*

INTESA SANPAOLO

Test *quantum proof solution*



CRITTOGRAFIA POST-QUANTUM

Sostituzione degli attuali algoritmi di crittografia con algoritmi post-quantum in protocolli preesistenti

È una soluzione software +

È più facilmente integrabile nei sistemi attuali +

Funziona su qualsiasi distanza +

L'inviolabilità è teorica e non può essere dimostrata –

Nel 2022/23 abbiamo dimostrato l'integrabilità della crittografia post-quantum in architetture standard, grazie al progetto **Quantum Safe Sandbox in collaborazione con IBM**

IBM

INTESA SANPAOLO

2023: la crittografia post-quantum è già qui

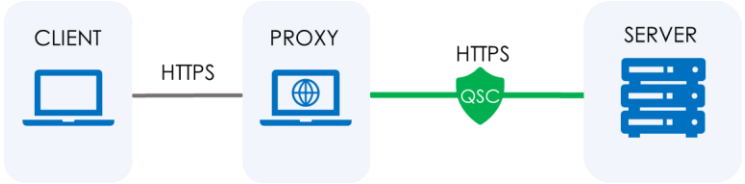
La crittografia post-quantum

Il National Institute of Standards and Technology (**NIST**) ha lanciato un bando per la creazione di algoritmi crittografici teoricamente non attaccabili dal quantum computer. Nel 2022 ne ha selezionati 4, fra cui 2 contenuti nella suite Crystals di IBM:

- **KYBER** per la **condivisione della chiave di cifratura dei dati**
- **DILITHIUM** come **schema di firma digitale**

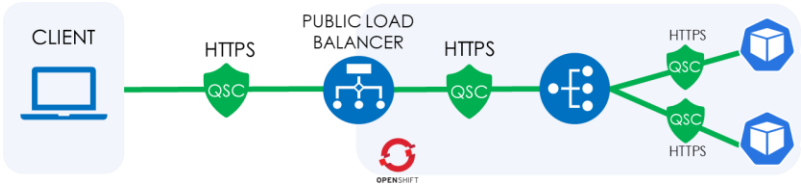
Questi algoritmi sono stati integrati nei protocolli di crittografia in una **Quantum Safe Sandbox**. Nelle tre architetture standard illustrate accanto vengono evidenziate connessioni protette da «quantum safe cryptography»

CONNESSIONE CLIENT – PROXY (QSC) – SERVER (QSC)



CONNESSIONE VPN CLIENT (QSC) E VPN SERVER (QSC)

CONNESSIONE CLIENT (QSC) E CLUSTER OPENSHIFT (QSC)



INTESA SANPAOLO

2023: un Quantum Risk Assessment e le prime linee guida di sviluppo *quantum safe*

KPMG evolution

QUANTUM RISK ASSESSMENT

Valutazione dell'esposizione al rischio derivante dal possibile sviluppo di nuove tecnologie quantistiche sulle infrastrutture di ISP

- Il perimetro di analisi è stato circoscritto all'applicazione del **mobile banking di ISP seguendo un modello standard** proposto dal NIST. Sono state identificate potenziali azioni da intraprendere per implementare la **Cryptographic agility.**

IBM

QUANTUM GUIDELINES

Stesura di Best Practices di sviluppo sicuro del SW in relazione ai rischi presenti in ambito Q-Safe

- L'analisi ha affrontato il rischio introdotto dai nuovi HW e ha portato alla redazione di un documento che traccia le principali raccomandazioni per mitigare il rischio quantistico: **Cryptographic agility**, utilizzo di modelli di threat modeling, Cryptographic Bill of Material

2024: la *crypto agility* e uno sguardo altrove

CRYPTO AGILITY

Capacità di un sistema informatico di introdurre nuovi algoritmi crittografici e protocolli di sicurezza (in questo caso quantum-proof) senza la necessità di sostituire componenti hardware o software.

QUANTUM INSPIRATION

Vogliamo sperimentare Quantum Hybrid Computing

Stiamo guardando dalla parte giusta?