Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
NQSTI National Quantum Science and Technology Institute

UNIVERSITÀ DEGLI STUDI DI SALERNO
Dipartimento di Fisica E.R. Caianiello

Tecnologie quantistiche e sicurezza

- Cosa sono le tecnologie quantistiche e perché se ne parla tanto
- Il calcolo quantistico e la crittografia
- Le comunicazioni quantistiche
- Prospettive future

Sergio Pagano,

Dipartimento di Fisica, Università di Salerno
via Giovanni Paolo II 132, 84084 - Fisciano (SA), Italy

Cosa sono le tecnologie quantistiche e perché se ne parla tanto

UNIVERSITÀ DEGLI STUDI DI SALERNO
Dipartimento di Fisica E.R. Caianiello

- La **fisica quantistica** è una teoria che descrive il comportamento delle particelle più piccole della materia e dell'universo, come le molecole, gli atomi, le particelle subatomiche e le particelle di luce (i fotoni).

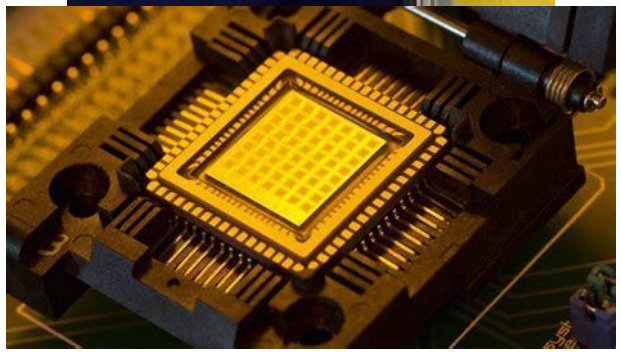
- **Tutta** la tecnologia moderna (computer, cellulari, telecomunicazioni, luce LED, LASER, energia fotovoltaica e nucleare) è basata sulle conoscenze sviluppate dalla fisica quantistica negli ultimi cento anni.

- Le **tecnologie quantistiche** sono un insieme di **nuove tecnologie,** basate sulla fisica quantistica, che promettono di rivoluzionare settori quali:
  - **Calcolo** risolvendo problemi **non affrontabili** dai calcolatori tradizionali in tempi umani
  - **Comunicazione** permettendo di trasferire l'informazione creando **canali di comunicazione estremamente sicuri**, dove **eventuali tentativi di intercettazione verrebbero immediatamente rilevati**.
  - **Sensori** permettendo la misurazione estremamente **precisa** e **sensibile** di svariati fenomeni per applicazioni scientifiche e mediche
  - **Simulazioni** simulando il funzionamento di **fenomeni naturali complessi**, come **le reazioni chimiche** o **i materiali innovativi**, accelerando **lo sviluppo di nuovi farmaci, materiali più resistenti o efficienti**.

Il calcolo quantistico e la crittografia

UNIVERSITÀ DEGLI STUDI DI SALERNO
Dipartimento di Fisica E.R. Caianiello

- Un computer **tradizionale** si basa su elementi logici chiamati **bit** che hanno solo due stati: **0** e **1** ma che combinati insieme possono rappresentare numeri arbitrari su cui si possono fare operazioni logiche e matematiche
- Un computer **quantistico** si basa su elementi logici chiamati **qubit** che, quando misurati hanno solo due stati: **0** e **1**, ma che nel frattempo assumono **tutti gli infiniti valori possibili tra 0 e 1**. La loro combinazione, attraverso opportune porte logiche, permettere di effettuare **operazioni in parallelo** con tutti gli infiniti valori che possono avere. In questo modo è possibile simulare sistemi fisici (quantistici e non) che hanno una complessità tale da renderli inattaccabili dai computer tradizionali
- Tradizionalmente la trasmissione sicura di informazione si è basata sulla **crittografia**: una tecnica per rendere un messaggio intellegibile solo al mittente e al destinatario.
- Esistono varie tecniche di crittografia usate in ambito civile e militare. In generale, il settore civile punta su velocità ed efficienza, mentre quello militare enfatizza resistenza agli attacchi, persino quelli quantistici.



Il calcolo quantistico e la crittografia

UNIVERSITÀ DEGLI STUDI DI SALERNO
Dipartimento di Fisica E.R. Caianiello

Crittografia in ambito civile è usata per proteggere comunicazioni, dati sensibili, transazioni finanziarie e autenticazione.

- Crittografia a chiave pubblica (asimmetrica)

RSA: Diffuso in protocolli come TLS/SSL (per HTTPS), firma digitale e scambio sicuro di chiavi.
ECC (Elliptic Curve Cryptography): Alternativa più efficiente a RSA, usata in crittografia mobile, Bitcoin e certificati digitali.
Diffie-Hellman: Usato per lo scambio sicuro di chiavi.

- Crittografia a chiave simmetrica

AES (Advanced Encryption Standard): Standard per crittografare dati in sistemi bancari, cloud storage e Wi-Fi (WPA2/WPA3).
ChaCha20: Alternativa ad AES, usata in VPN, WireGuard e crittografia mobile.

- Hashing e firme digitali

SHA-256 / SHA-3: Utilizzato per firme digitali, password hashing e blockchain.
HMAC (Hash-based Message Authentication Code): Usato per garantire l'integrità dei messaggi (ad esempio, in API e protocolli di autenticazione).

Il calcolo quantistico e la crittografia

UNIVERSITÀ DEGLI STUDI DI SALERNO
Dipartimento di Fisica E.R. Caianiello

Crittografia in ambito militare: richiede algoritmi con livelli di sicurezza estremi e spesso usa sistemi proprietari o classificati.

- Standard militari e governativi

Suite B (NSA): Include AES-256, ECC (Curve P-384), SHA-384 e il protocollo ECDH.
Type 1 Encryption (NSA): Algoritmi classificati per proteggere informazioni Top Secret (es. algoritmi come MAYFLY, SAVILLE).
Quantum-Resistant Cryptography: Algoritmi considerati resistenti ai computer quantistici, come Kyber, NTRUEncrypt, Dilithium, SPHINCS+ e McEliece. (in valutazione)

- Protocolli militari

TACLANE (DISA/NSA): Sistema di cifratura hardware per reti sicure.
OTAR (Over-the-Air Rekeying): Permette di aggiornare chiavi crittografiche a distanza senza intervento fisico.

Il calcolo quantistico e la crittografia

UNIVERSITÀ DEGLI STUDI DI SALERNO
Dipartimento di Fisica E.R. Caianiello

- Negli anni '90 sono stati pubblicati i lavori matematici di Peter Shor (1994) e di Lov Grover (1996) che **dimostrano** come un **computer quantistico abbastanza potente** può **rompere** la sicurezza associata ai protocolli **RSA**, **ECC**, **Diffie-Hellman**, **CDH**, **DSA/ECDSA** e rendere **parzialmente vulnerabili** i protocolli **AES-128**.

Allora non esistevano computer quantistici, ma ora si!

- La crittografia militare basata su questi protocolli (come reti sicure, comunicazioni governative e autenticazione) potrebbe essere compromessa. Le reti **NATO** e governi alleati, che usano spesso **ECC** e **RSA**, diventerebbero insicure. I **sistemi satellitari e militari (es. GPS crittografato)** potrebbero essere vulnerabili.

- Sono ancora sicuri (se con chiavi lunghe):
  AES-256 → Ancora resistente (l'attacco di Grover lo ridurrebbe a un equivalente di AES-128).
  ChaCha20 → Sicuro se con chiavi sufficientemente lunghe.
  One-Time Pad (OTP) → **Assolutamente sicuro** se usato correttamente, usato in **comunicazioni ultra-sicure**

- Le contromisure sono la **Quantum-Resistant Cryptography**: Algoritmi considerati resistenti ai computer quantistici, come Kyber, NTRUEncrypt, Dilithium, SPHINCS+ e McEliece.
  (tuttora in valutazione e non può essere escluso che in futuro non siano attaccabili)

Le comunicazioni quantistiche

UNIVERSITÀ DEGLI STUDI DI SALERNO
Dipartimento di Fisica E.R. Caianiello

- Molti governi stanno iniziando a implementare **reti quantisticamente sicure** e sperimentano con **quantum key distribution (QKD)** che usa **One-Time Pad (OTP)** per garantire comunicazioni **a prova di attacco**.

- **OTP** è basato sul fatto che mittente (A=Alice) e destinatario (B=Bob) hanno una chiave segreta comune. Se la chiave è abbastanza lunga (in bits) si può usare per codificare un messaggio mandato dal mittente al destinatario di pari lunghezza.

- È **impossibile** decifrare il messaggio codificato se intercettato durante il trasferimento .(Claude Shannon 1949)

- Il punto è fare in modo che Alice e Bob possano scambiarsi la chiave in modo sicuro.

- Qui si possono usare le leggi della **fisica quantistica** per avere una distribuzione sicura della chiave: **quantum key distribution (QKD)**

Le comunicazioni quantistiche

UNIVERSITÀ DEGLI STUDI DI SALERNO
Dipartimento di Fisica E.R. Caianiello

- Nel 1984, Charles Bennett e Gilles Brassard introdussero una delle pietre miliari della seconda rivoluzione quantistica: un protocollo per la **distribuzione delle chiavi quantistiche** ora noto come **BB84**. L'essenza del BB84 risiede nell'uso dei **qubit** per trasmettere una chiave segreta.
- Nella pratica i qubit sono realizzati con particelle di luce (i fotoni) che possono essere orientati (polarizzati) in direzioni prestabilite. In questo modo si codificalo stato 0 e 1 che si vuole trasmettere.

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

- Se si prova a leggere lo stato di polarizzazione di un fotone, lo si disturba in modo **inevitabile** e la misura **cambia** il suo stato. BB84 permette ad Alice e a Bob di accorgersi del tentativo di misura e di scartare il dato. I bit rimanenti formano la chiave segreta condivisa tra Alice e Bob. A questo punto la usano per codificare il messaggio da trasmettere. Le chiave viene rinnovata periodicamente per garantire la sicurezza della trasmissione.

Le comunicazioni quantistiche

UNIVERSITÀ DEGLI STUDI DI SALERNO
Dipartimento di Fisica E.R. Caianiello

- Dimostrazioni di QKD su **fibra ottica**

Toshiba – Tokyo QKD Network (2021) 600 km di fibra a Tokyo. Usata per la sicurezza bancaria e delle comunicazioni governative.
BT & Toshiba – Rete QKD nel Regno Unito (2022) Londra – Bristol con fibra da **100 km**. Usata per trasmissioni sicure tra aziende e istituzioni finanziarie
Governo Cinese – Rete QKD tra Pechino e Shanghai (2017) Copertura di **2.000 km**, combinando QKD in fibra e satellitare. Protegge le comunicazioni militari e governative cinesi.
ID Quantique – Reti bancarie in Svizzera Swiss Quantum Network, usato per proteggere transazioni finanziarie.
USA – DARPA Quantum Network (Boston, 2003-2007) Primo esperimento di rete QKD su fibra ottica negli Stati Uniti.

- Dimostrazioni di QKD via **satellite**

Micius (Cina, 2016), Primo satellite QKD al mondo. **Pechino e Vienna (7.600 km)** nel 2017.
SGDC (Brasile, 2017-2021) Esperimenti di QKD su satellite per protezione di comunicazioni governative.
QUARC (Regno Unito, 2022) Progetto per sviluppare comunicazioni quantistiche satellitari per la sicurezza nazionale.
SpeQtral-1 (Singapore, 2024) Satellite per testare QKD a livello commerciale.
NASA & JPL – Progetto QKD satellitare (USA, in sviluppo) Progetto per realizzare reti QKD spaziali con il Dipartimento della Difesa.

Prospettive future

UNIVERSITÀ DEGLI STUDI DI SALERNO
Dipartimento di Fisica E.R. Caianiello

- Oggi, i computer quantistici **non sono ancora abbastanza potenti** per rompere RSA-2048 o ECC-256. Ci vogliono computer con almeno 1.000.000 qubit. Quelli attuali ne hanno qualche centinaio e **non è facile** aumentarne il numero. Si prevede, tuttavia, che entro **10-20 anni** potrebbero essere sviluppati sistemi in grado di farlo.

- In molti Paesi si sta lavorando sulla **transizione alla crittografia post-quantistica** per garantire la sicurezza a lungo termine. I protocolli post quantum sviluppati sono efficaci rispetto agli attacchi degli algoritmi quantistici sviluppati finora, ma cosa si può dire del futuro?

- La QKD è una tecnologia che promette di effettuare trasmissioni criptate sicure, a prova di attacco da computer classici e quantistici. È comunque una tecnologia in fase di sviluppo, in cui vanno ancora risolti problemi di natura tecnica per ottenere il massimo delle prestazioni (velocità di comunicazione, lunghezza della chiave, distanza massima raggiungibile).
  La **Cina** sta già implementando reti **ibrida fibra-satellite** per QKD su scala nazionale.
  L'**Europa** sta sviluppando il progetto **EuroQCI** per la sicurezza quantistica nelle comunicazioni governative.
  Gli USA stanno sperimentando reti QKD per proteggere infrastrutture critiche