REPLY è specializzata nella progettazione e nell'implementazione di soluzioni basate sui nuovi canali di comunicazione e media digitali. Costituita da un modello a rete di aziende altamente specializzate, Reply affianca i principali gruppi industriali europei appartenenti ai settori Telco & Media, Industria e Servizi, Banche e Assicurazioni e Pubblica Amministrazione nella definizione e nello sviluppo di modelli di business abilitati dai nuovi paradigmi del Big Data, Cloud Computing, Digital Media e Internet degli Oggetti. I servizi di Reply includono: Consulenza, System Integration e Digital Services.

SEI QUANTUM-SAFE?

CYBERSECURITY NELL'ERA DELLA QUANTUM SUPREMACY

I computer quantistici permettono di decriptare gli attuali sistemi di cifratura, mettendo in discussione i paradigmi e i principi su cui si fonda la cybersecurity tradizionale. Per garantire la protezione dei dati e potenziare i meccanismi di sicurezza, le organizzazioni devono imparare a proteggersi anche in una logica post-quantistica.

www.reply.com

QUANTUM COMPUTING: VELOCITÀ, SICUREZZA E AFFIDABILITÀ

La cybersecurity è ormai parte integrante di ogni organizzazione, processo e attività: proteggere reti, dati, transazioni, prodotti e persone da possibili attacchi informatici o accessi non autorizzati viene prima di tutto, anche del business "core", indipendentemente dal settore e dalle dimensioni di un'azienda.

La resilienza alle minacce informatiche è la resilienza di un'industria. Nell'era della Supremazia Quantistica, sempre più vicina, ci saranno computer in grado di risolvere problemi insormontabili per le attuali tecnologie mainstream: la capacità computazionale del Quantum Computing permette di risolvere in pochi minuti algoritmi che al supercomputer più potente al mondo richiederebbero un tempo stimato nell'età della Terra. Tra i settori più esposti alla Quantum Disruption c'è proprio quello della sicurezza informatica, la cui affidabilità dipende soprattutto dalla non risolvibilità degli algoritmi su cui è costruita.

Irrisolvibili? Un concetto che appartiene al passato. È il caso, per esempio, della fattorizzazione della chiave crittografica RSA che, sebbene non sia un calcolo teoricamente impossibile da risolvere ma solo altamente improbabile per la sua complessità, è attualmente considerato un algoritmo sicuro al 100%. Grazie a un quantum processor di 6000-qubit, si stima che l'RSA possa essere fattorizzato in sole 2 settimane, se non addirittura in 8 ore avvalendosi di 20 milioni-qubit noisy. Si tratta di hardware non ancora esistenti, ma la cui realizzazione è prevista nei prossimi anni.

FATTORIZZAZIONE RSA

6000 QUBIT - 2 WEEKS

Sei quantum-safe? Dalla crittografia ai meccanismi di autenticazione OTP, passando per la gestione delle transazioni bancarie, le connessioni VPN, lo scambio di e-mail, il gaming, il mondo delle scommesse on-line arrivando fino ai sistemi di votazione democratici. Il potere "dirompente" di questa tecnologia sarà enorme sia in ambito sicurezza, sia in ambito computistico, ma potrà essere gestito e valorizzato adottando soluzioni post-quantistiche o integrando le infrastrutture tecnologiche esistenti con soluzioni sufficientemente robuste, mature ed economicamente competitive.

Nei campi della Sicurezza e della Communication Encryption, si possono trarre grandi benefici dal Quantum Computing: sono già stati realizzati hardware capaci di rafforzare le reti di sicurezza (hardening), sfruttando, in questo caso non la parte computistica della meccanica quantistica, bensì i fotoni e l'entanglement.

In attesa della Rivoluzione Quantistica. Preparare le aziende Clienti alla Quantum Supremacy è l'obiettivo di Reply che, da oltre due anni, ha team multidisciplinari esclusivamente dedicati al Quantum Computing (QC), che lavorano anche su Practice realizzate in collaborazione con importanti player internazionali.

SPAVENTATI DALLA SUPREMAZIA QUANTISTICA?

Negli anni la tecnologia è migliorata notevolmente: l'algoritmo di crittografia di largo utilizzo "RSA", per esempio, si basa su un'asimmetria nella complessità di due calcoli complementari. Ciò si traduce in un calcolo relativamente facile - e quindi veloce - da risolvere, mentre il percorso inverso è relativamente complesso.

Se da un lato la moltiplicazione di due numeri (primi) non è un'operazione matematica particolarmente complessa, dall'altro la scomposizione di un grande numero nei fattori da cui è composto costituisce un traguardo decisamente maggiore. In questo caso, si parla di una "complessità non polinomiale", cioè di un calcolo praticamente impossibile da risolvere.

Nell'ambito della crittografia, c'è un grande vantaggio: una chiave lunga e complessa (per esempio 2048 bit) implica che la crittografia sia resa più difficile solo con uno sforzo polinomiale, il che significa che è, nella pratica, facilmente attuabile. Una decodifica non autorizzata, invece, diventa esponenzialmente più complicata. In fin dei conti, ciò significa che i computer possono diventare sì più veloci, ma è sufficiente aumentare la lunghezza della chiave per rimanere criptati in modo sicuro.

GOOGLE E IL CAMBIO DI PARADIGMA

L’anno scorso Google ha annunciato di aver raggiunto la "Quantum Supremacy"; con questa "supremazia" gli ingegneri di Mountain View sono stati in grado di risolvere - attraverso il proprio hardware quantistico - in poco più di tre minuti un problema che, hanno dichiarato, avrebbe richiesto 10.000 anni per essere risolto su un computer tradizionale. La motivazione: la complessità dell'algoritmo eseguito su un computer quantistico è polinomiale, ovvero un vantaggio significativo rispetto alla complessità esponenziale di un computer classico.

Il problema con cui Google ha dimostrato la supremazia quantistica era di scarsa rilevanza pratica, un "chiodo quantistico" per il quale era stato progettato appositamente un "martello quantistico". Quando si tratta di crittografia, però, la situazione diventa meno semplicistica. La complessità - sin qui elevata - nella decrittazione viene infatti meno se è disponibile un corrispondente computer quantistico. Il motivo: esiste un algoritmo in grado di fattorizzare efficientemente grandi numeri attraverso l'hardware quantistico, che prende il nome dal suo inventore (Peter Shor) e rende la cifratura vulnerabile agli attacchi.

Secondo le stime dell'US National Institute of Standards and Technology, è verosimile che nel 2027 la potenza dei computer quantistici potrebbe essere sufficiente per tentare un attacco alla cifratura RSA .

La crittografia è inoltre soggetta a un ulteriore problema, spesso sottovalutato. Per fare in modo che la cifratura non sia facilmente indovinabile, i numeri che compongono la chiave devono essere selezionati randomicamente tra un gran numero di possibilità. Non è così facile generare un numero casuale, soprattutto per un computer. In un gioco da tavolo, per esempio, l'elemento casuale risiede in uno o due dadi.

I numeri sono distribuiti nel corso della partita secondo regole statistiche. In questa circostanza, ciò che percepiamo come casualità è in realtà l'incapacità umana di controllare tutti i parametri fisici. Se si conoscessero il centro di gravità dei dadi e l'irregolarità del tavolo e si fosse in grado di controllare con precisione l'oscillazione della propria mano, sarebbe possibile ottenere qualsiasi risultato desiderato.

NESSUNA POSSIBILITÀ PER UN ATTACCO MAN-IN-THE-MIDDLE

Un fisico fa ricorso alla misurazione per determinare se un evento si sia verificato realmente. Fino al momento della misurazione, il sistema fisico è miracolosamente libero e aleggia in una sovrapposizione di tutti gli stati possibili.

Questa insolita “caratteristica” potrebbe essere sfruttata per criptare i dati, in quanto un messaggio inviato in codice quantico potrebbe essere letto solo "misurando" i caratteri da cui è composto: la sovrapposizione quantistica “tipica” andrebbe perduta e non sarebbe recuperabile. Per leggere tale messaggio, un eventuale “intercettatore” indesiderato dovrebbe esprimerlo in un nuovo stato quantistico, ma le due parti “originarie” della comunicazione potrebbero accordarsi sulle modalità di misurazione.

La potenziale creazione di singoli bit quantistici da parte di soggetti terzi non autorizzati verrebbe alla luce durante la misurazione, in quanto sempre più caratteri arriverebbero in modo errato. I due interlocutori “originari” potrebbero quindi accorgersi di eventuali incongruenze e, perdendo la fiducia nel canale di comunicazione, potrebbero ricominciare da capo neutralizzando così l’intercettatore impegnato nell’attacco “Man in the middle”.

Concretamente, un telefono quantistico di questo tipo sarebbe particolarmente difficile da realizzare. Gli stati quantistici sono relativamente volatili. La meccanica quantistica contraddice la nostra intuizione, perché nulla nel nostro contesto di vita familiare si comporta quanto-meccanicamente. Le proprietà si perdono a causa di influenze esterne. Questa suscettibilità agli errori ci limita ancora oggi nell’utilizzo dei computer quantistici e comporta costi elevati per gli sviluppatori di hardware dedicato.

LA CASUALITÀ AL SERVIZIO DELL'IOT

Da qualche tempo la società IDQuantique, spin-off dell'Università di Ginevra, ha sviluppato un sistema che offre al mercato "servizi di casualità". Fortinet, uno dei principali provider di software di sicurezza, ha recentemente annunciato una collaborazione con IDQuantique e doterà la prossima generazione del suo firewall di un'interfaccia a chiave quantistica.

Alcune aziende hanno già iniziato a utilizzare tecnologie post-quantistiche. Si tratta di organizzazioni molto grandi che hanno deciso di investire in ambito QC, ma queste soluzioni sono molto flessibili e possono essere impiegate in qualunque contesto dove occorra rafforzare i meccanismi di scambio chiavi e autenticazione.

NS&I - National Savings and Investments

L'Istituto bancario britannico che si occupa di risparmio e obbligazioni, ha adottato gli **Encryptor** per potenziare i meccanismi adibiti alla generazione di obbligazioni sulla propria piattaforma on-line. L'integrazione di **generatori di numeri casuali quantici** rende più difficile per un attaccante riuscire a rintracciare quelle che sono le chiavi utilizzate per la generazione di applicazioni all'interno dei sistemi National Savings and Investments.

Governo svizzero

Il Governo svizzero ha proposto una piattaforma di voto online, per rafforzare i meccanismi di indicazione degli elettori, assicurando maggiore protezione e confidenzialità, e per prevenire le frodi elettorali o i tentativi di sondaggi illegali inerenti ai sistemi di votazione, contrastando voti malevoli o falsi. La soluzione integra **Encryptor quantistici** e **distributore di chiavi quantistiche** per potenziare i meccanismi di autenticazione con password OTP e per impedire a potenziali MITM di intromettersi all'interno della comunicazione.

Banca Centrale Europea

Nell'ambito delle attività connesse all'emissione della Central Bank Digital Currency (CBDC), la BCE ha dovuto creare una piattaforma che permettesse agli utenti/investitori di gestire questa nuova moneta in sicurezza, a partire dai pagamenti. La soluzione implementata ha portato alla creazione di un nuovo meccanismo di autenticazione basato su tecnologia Gemalto, azienda leader nel settore Digital Security, con generazione di token per comunicazione OTP effettuati in maniera quantistica - integrazione con **Encryptor quantistici** - dimostrando concretamente quanto questo tipo di tecnologia sia flessibile ed integrabile alle soluzioni già presenti sul mercato.

British Telecom

La British Telecom ha avviato un piano di potenziamento delle proprie dorsali in ottica post-Quantum, in particolare per il rischio di attacchi MITM, diffusi in ambito telco e difficili da riconoscere a causa della grande mole di informazioni che passa all'interno di una dorsale. La soluzione proposta è l'integrazione di generatori di chiavi quantistiche. Si è ottenuta la creazione di nuove dorsali a 100 G che operano con meccanismi di scambio di chiavi quantistiche e hanno il vantaggio di riuscire a rilevare potenziali MITM all'interno della comunicazione, al fine di bloccare il tentativo di furto delle informazioni. Attualmente le dorsali attive sono due e sono ancora in fase sperimentale.

Loterie Romande

Sono stati integrati per la società di servizi pubblici di tutta la Svizzera francese, un **generatore di numeri quantistici** all'interno dei loro sistemi per un potenziamento complessivo della sicurezza di tutti i meccanismi connessi alla core activity, svincolando il Cliente dalla pseudocasualità dei meccanismi di generazione di numeri mediante algoritmi.

South Korea Telecom

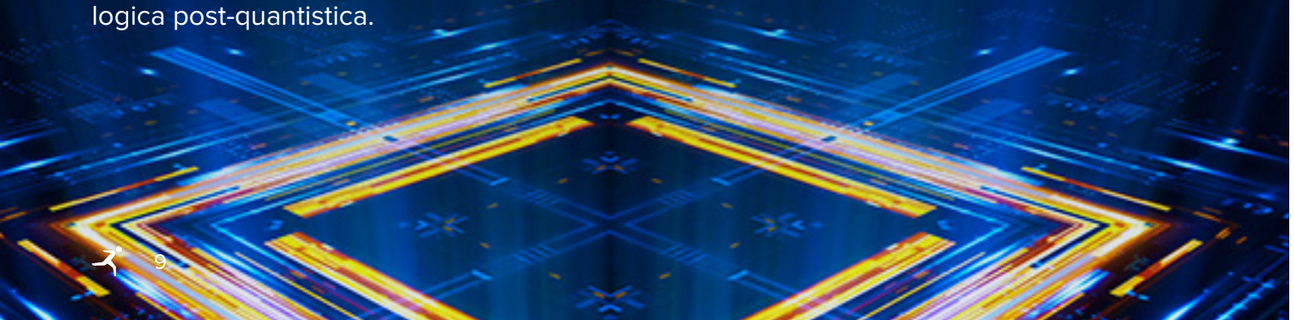
La South Korea Telecom ha avviato un progetto volto a rafforzare i principi di autenticazione, basati sulla generazione di chiavi, per dispositivi mobile e IoT su tecnologia 5G. Sono stati integrati degli **Encryptor quantistici** all'interno dei loro Data Center per offrire una connessione più sicura.

IL QUANTUM COMPUTING NON È FANTASCIENZA

La Quantum cybersecurity è sicuramente un mercato emergente in cui i player tecnologici specializzati, in grado di effettuare data integration in logica quantum-resilient, sono ancora pochi.

L’avvento dei computer quantistici permette di criptare gli attuali sistemi di cifratura, mettendo inesorabilmente in discussione i paradigmi e i principi su cui si fonda la cybersecurity tradizionale. Per garantire la protezione dei dati e potenziare i meccanismi di sicurezza, le organizzazioni devono imparare a proteggersi, in tempo utile, anche in una logica post-quantistica.

Le soluzioni a lungo termine come i distributori di chiavi quantistiche, che richiedono la sostituzione dell’infrastruttura tecnologica con un maggiore investimento iniziale e le soluzioni intermedie come gli encryptor quantistici o i generatori di numeri casuali quantistici non hanno costi molto diversi dalle soluzioni pre-quantistiche.



REPLY - IL BUSINESS NELL’ERA QUANTISTICA

In qualità di thought leader e consulente per i propri clienti, Reply è costantemente impegnata nell'identificazione e nella gestione delle opportunità emergenti e dei casi d'uso abilitati dal Quantum Computing.

Il Quantum Computing è una nuova tecnologia che offre molte opportunità in una vasta gamma di settori. Rappresenta la base per applicazioni avanzate nei settori dell'Intelligenza Artificiale, Quantum Machine Learning, cybersecurity, Finanza, Logistica e Trasporti, Telco, Medicina e molti altri ancora.

Reply è impegnata nello sviluppo di proof-of-concepts e progetti che applicano algoritmi quantistici a casi d’uso reali in molte aree di business e offre risposte concrete ed efficaci ai problemi dei propri clienti. Sulla rivista "Springer Journal Quantum Machine Intelligence" del 2020 è stato pubblicato uno studio di Reply sulle modalità in cui un Quantum Annealer può essere impiegato per risolvere problemi di ottimizzazione complessi.

Nel 2018, nell'ambito del Quantum Artificial Intelligence Research Programme al quale hanno partecipato anche la NASA e Google, Reply ha ottenuto una borsa di ricerca per utilizzare il Quantum Annealer D-Wave della Universities Space Research Association.