La Crittografia Post Quantum nell'Industria

Guglielmo Morgari – Telsy Research Manager

PQCifris 2019

Roma, 9 maggio 2019

Telsy

Telsy - profilo dell’azienda

Telsy

- Fondata nel 1971
- Oggi 100% gruppo TIM
- Specializzata in cybersecurity e crittografia
- Applicazioni in ambito governativo e civile
- Sotto Golden Power
- Fortemente attiva nella ricerca

Quantum Computer

- Teorizzato negli anni ’80
- A lungo considerato praticamente irrealizzabile
- Non più bit (0/1) ma qubit (sovrapposizione di stati 0 e 1, secondo il modello quantistico)

- Se realizzato, sarà (molto) più efficiente di un computer classico per risolvere **alcune** famiglie di problemi
- Impatto sulla crittografia?

- Ingenti investimenti governativi US / Cina
- Negli ultimi anni rapidi progressi e primi prototipi (scarso interesse pratico)
- IBM, D-Wave, Google, Microsoft
- NSA?
- Cina?

- Prodotti sul mercato: 2030? 2040? Mai?

Telsy

Sistema crittografico

« hallo »

Cifratura

«@#!Kx4+»

Decifratura

« hallo »

Telsy

Sistema crittografico

« hallo »

Cifratura

«@#!Kx4+»

algoritmo a chiave simmetrica
(cifratura dati)

Decifratura

« hallo »

Telsy

Sistema crittografico

« hallo »

« hallo »

Cifratura

«@#!Kx4+»

algoritmo a chiave simmetrica
(cifratura dati)

Decifratura

algoritmo a chiave asimmetrica
(scambio chiavi)

Telsy

Crittografia e Quantum Computer

Algoritmi a chiave simmetrica

- richiedono condivisione di una chiave segreta tra gli interlocutori
- DES, AES, …
- **Algoritmo di Grover (1996) (quantum computer)**

- Dimezza la lunghezza effettiva della chiave
- E' sufficiente raddoppiarla per avere lo stesso livello di sicurezza

Algoritmi a chiave asimmetrica

- basati su problemi matematici (oggi) considerati inattaccabili tramite computer classici
- RSA (fattorizzazione)
  (EC)Diffie Hellman (logaritmo discreto)
- **Algoritmo di Schor (1994) (quantum computer)**

- Rompe completamente i sistemi attuali
- Non esistono rimedi semplici

Telsy

Quantum Computer

Agosto 2015, NSA web site

> Our ultimate goal is to provide cost effective security against a potential quantum computer.
>
> [...]
>
> We recommend [...] **to prepare for the upcoming quantum resistant algorithm transition**.

Telsy

E’ davvero un problema?

- Non sappiamo se il computer quantistico arriverà davvero…
  … ma non possiamo rischiare!

- Lo sviluppo di nuove tecnologie richiede molto tempo
- Il loro deployment richiede molto tempo
- La vita utile di un messaggio può essere molto lunga

- Quindi…. **sì, è un problema**… da affrontare subito!

- Necessario definire **alternative agli attuali sistemi a chiave pubblica**
- Due strade
  - Post Quantum Cryptography (PQC)
  - Quantum Key Distribution (QKD)

Telsy

Post Quantum Cryptography

Intensa attività di ricerca nella comunità crittografica
Nuovi algoritmi a chiave pubblica basati su problemi matematici «quantum resistant»

NIST lancia una *call* nel 2016 e ***spera*** di chiuderla nel 2024

- 21 dicembre 2017: 69 algoritmi proposti
- 30 gennaio 2019: 26 algoritmi superstiti

5 famiglie principali
- Code-based
- Lattice-based
- Multi-variate-based
- Hash-based
- Supersingular e.c. isogenies-based

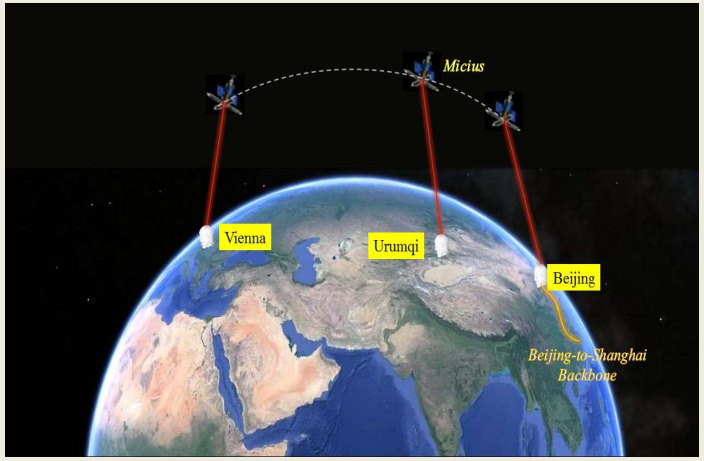
NIST
National Institute of Standards and Technology

Telsy

Quantum Key Distribution

- Chiave codificata tramite fotoni inviati su canale ottico (fibra o open space)
- Non intercettabilità della chiave garantita da principi quantistici indeterminazione di Heisenberg
- In associazione a canale classico non sicuro, su cui la chiave prodotta viene usata in modo tradizionale

Source: INRiM



Source: Chinese Academy of Sciences

Telsy

Telsy - attività in corso

Post Quantum Cryptography

POLITECNICO DI TORINO

UNIVERSITÀ DEGLI STUDI DI TRENTO

Studio e sviluppo famiglie di algoritmi PQC

Quantum Key Distribution

INRiM

CNR

Installazione link in fibra ottica Telsy – INRiM

- Dimostratore QKD
- Test-bed per sistemi QKD nazionali/europei
- Sviluppo soluzione QKD a filiera italiana

Telsy

Conclusioni

- Il Quantum Computer rappresenta una minaccia reale

- E’ necessario individuare fin da subito delle contromisure
  potrebbe essere tardi?

- PQC e QKD sono due strade percorribili
  soluzioni non alternative ma complementari
  possono coesistere in un singolo sistema

- Fondamentale collaborazione a livello nazionale
  istituti di ricerca
  industria
  enti istituzionali

Telsy


Grazie per l’attenzione
guglielmo.morgari@telsy.it
Telsy