UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII
Dipartimento di Ingegneria
dell'Informazione

La 'minaccia' del quantum computing e la crittografia Post-Quantum: stato dell'arte e impatto su 5G

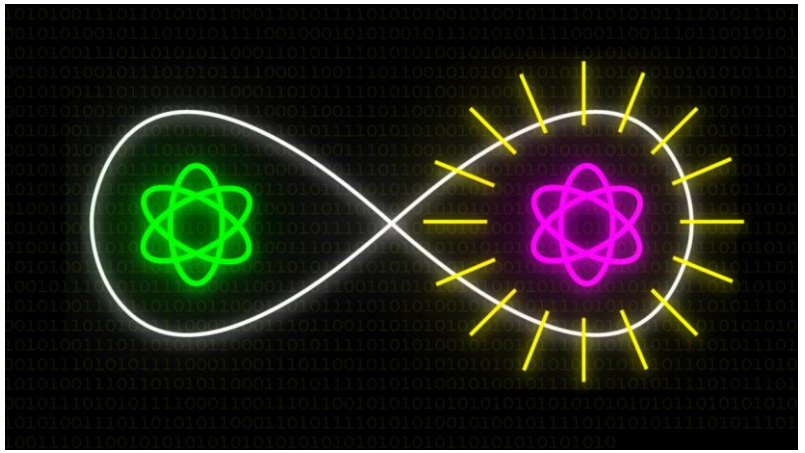
Marco Baldi

Università Politecnica delle Marche
Dipartimento di Ingegneria dell'Informazione
m.baldi@univpm.it

29 Marzo 2023


UNIVERSITÀ POLITECNICA DELLE MARCHE
CRiSPY
CENTRO DI RICERCA E SERVIZIO
PER LA PRIVACY E LA CYBERSECURITY
crispy.dii.univpm.it
cini
CYBERSECURITY
NATIONAL
LABORATORY
DE CIFRIS

Quantum Information Science



(scienza che usa gli stati quantici di particelle subatomiche per rappresentare l'informazione)

- **Quantum computing**

(computer che utilizza fenomeni di meccanica quantistica, come il principio di sovrapposizione e la correlazione quantistica per l'esecuzione di calcoli)

- **Quantum cryptography**

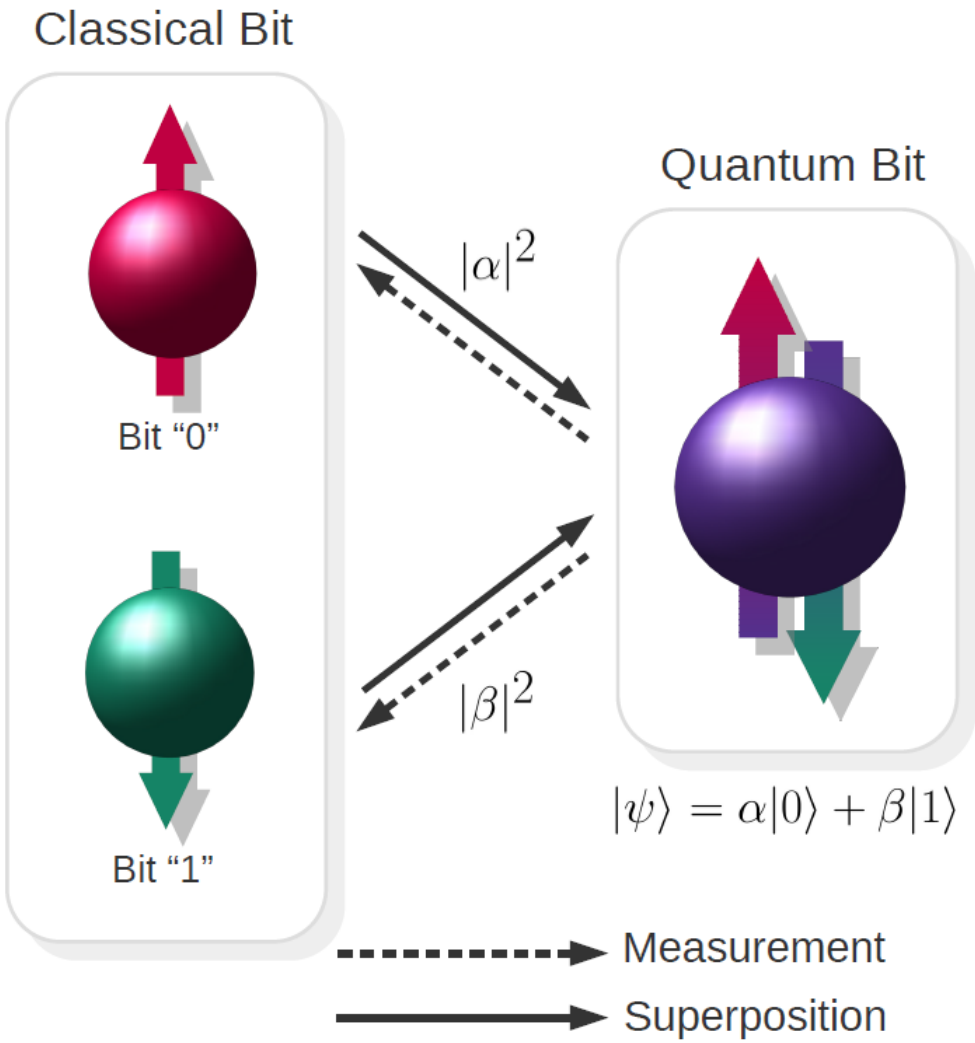
(scienza che sfrutta le proprietà della meccanica quantistica per scopi crittografici, come la quantum key distribution)

- **Quantum communication**

(scienza che sfrutta le proprietà della meccanica quantistica per trasmettere informazione)

Qubit

- a differenza dei bit classici, che possono assumere solo uno dei valori "0" o "1" in un dato intervallo di tempo, un **qubit** può contenere entrambi i valori contemporaneamente in una forma di sovrapposizione



Qubit (2)

- N qubit in uno stato di **sovrapposizione quantum** possono rappresentare contemporaneamente tutte le 2^N combinazioni di bit classici.
- **Teorema di non clonazione**: quando si prova ad osservare i qubit, essi collassano nel dominio classico.
- Quindi non si può eseguire una perfetta operazione di copia di un qubit trovato in uno stato di sovrapposizione.
- Ciò è alla base della sicurezza dei protocolli di **Quantum Key Distribution** (QKD).
- La prima implementazione di QKD fu il protocollo Bennett-Brassard (BB84) basato sull'approccio «prepara e misura».
- Invece il protocollo E91 usa gli stati quantistici entangled dell'esperimento Einstein-Podolsky-Rosen (EPR).

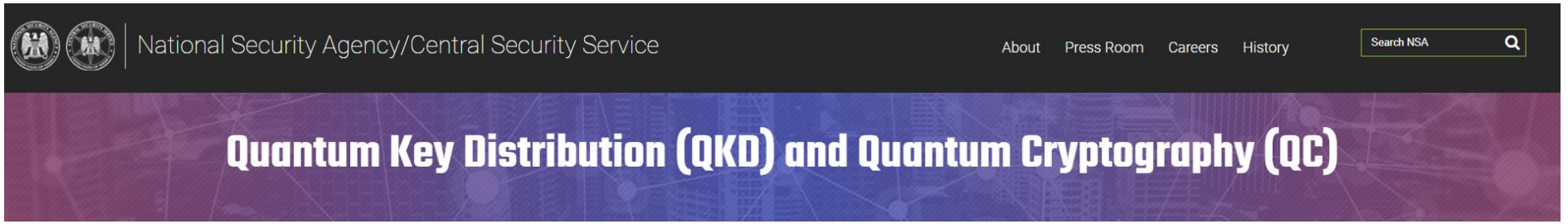
Quantum Key Distribution

- Esempio più noto di **crittografia quantistica**
- Consente a due interlocutori di condividere un segreto trasmettendolo su un collegamento ottico
- L'informazione è codificata in stati quantistici
- La comunicazione sfrutta fenomeni quantistici come **quantum superposition** o **quantum entanglement**
- È noto che l'effettuazione di una misura di un fenomeno quantistico perturba il fenomeno stesso
- Questo rende l'intercettazione **teoricamente impossibile**
- La sicurezza di QKD è dimostrabile teoricamente e non dipende dalle risorse di un attaccante

Esperimenti di QKD

- Nel **2010** in Giappone è stata inaugurata una rete denominata **Tokyo QKD Network** che coinvolge molti enti tra cui NICT, NEC, Mitsubishi Electric, NTT, Toshiba Research Europe, the Austrian Institute of Technology ed altri.
- Nel **2017** in Inghilterra sono stati eseguiti esperimenti sulla **Cambridge Quantum Network**, composta di tre nodi presso sedi universitarie e un quarto nodo presso Toshiba Research Europe labs (TREL).
- Dal **2017** il satellite cinese **Micius** consente di distribuire coppie di fotoni entangled su due downlink bidirezionali consentendo esperimenti di QKD in spazio libero su tratte di migliaia di chilometri.
- Nel **2019** nell'area metropolitana di **Firenze** ricercatori dell'Istituto nazionale di ottica del Cnr e del Lens di Firenze, in collaborazione con Inrim di Torino e Università Tecnica della Danimarca effettuato un trial.
- Nel **2019** è stato effettuato un esperimento su 96 km di cavo in fibra ottica sottomarina fra Malta e la Sicilia.
- Nel **2021** Italtel, Top-Ix, Inrim, Politecnico di Milano e Cohaerentia hanno sviluppato un prototipo della soluzione **Italtel Quantum Secure Network** collegando tre datacenter su una rete in esercizio: ITGates, Colt e Csi Piemonte.

Cosa ne pensa la NSA



Technical limitations:

1. Quantum key distribution is only a partial solution.
2. Quantum key distribution requires special purpose equipment.
3. Quantum key distribution increases infrastructure costs and insider threat risks.
4. Securing and validating quantum key distribution is a significant challenge.
5. Quantum key distribution increases the risk of denial of service.

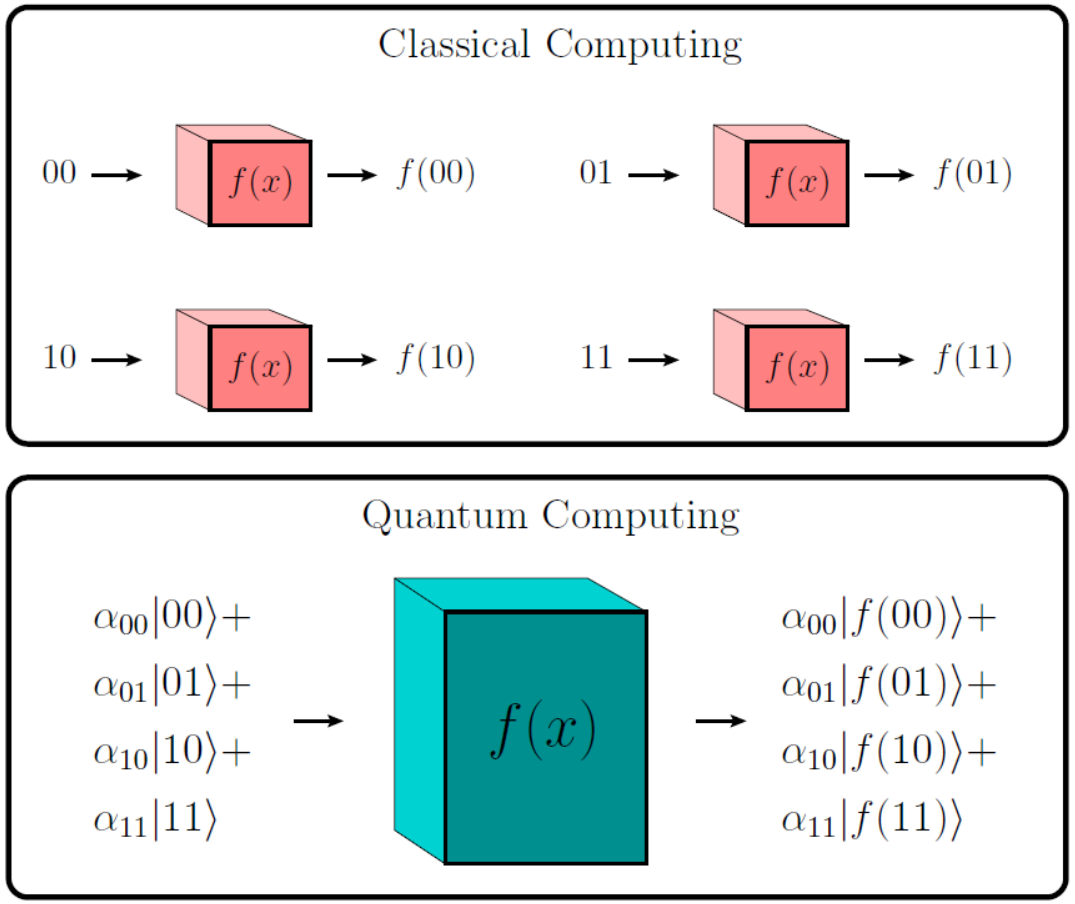
Conclusion:

In summary, NSA views quantum-resistant (or post-quantum) cryptography as a more cost effective and easily maintained solution than quantum key distribution. For all of these reasons, NSA does not support the usage of QKD or QC to protect communications in National Security Systems, and does not anticipate certifying or approving any QKD or QC security products for usage by NSS customers unless these limitations are overcome.

Il Quantum Computer

- Teorizzato da **Richard Feynman** e **Yuri Manin** all'inizio degli anni 80

- Il parallelismo intrinseco dell'informazione quantistica può accelerare significativamente la soluzione di alcune classi di problemi.



Algoritmi quantum

- Algoritmo di **Shor** (1994)
  - fattorizzazione di numeri interi su quantum computer
  - dato un intero N, lo fattorizza in un tempo polinomiale in log N
  - su un computer classico il tempo è esponenziale in log N

- Algoritmo di **Grover** (1996)
  - ricerca in una lista non ordinata su quantum computer
  - in una lista lunga N trova un elemento in un tempo proporzionale a $\sqrt{N}$
  - su un computer classico il tempo è proporzionale a N

Verso il Quantum Computer

- **Ottobre 2011**:

Primo centro accademico di quantum computing (Univ. South. California, Lockheed Martin e D-Wave Systems)

- **Gennaio 2012**:

D-Wave annuncia la realizzazione di un quantum computer a 84 qubit

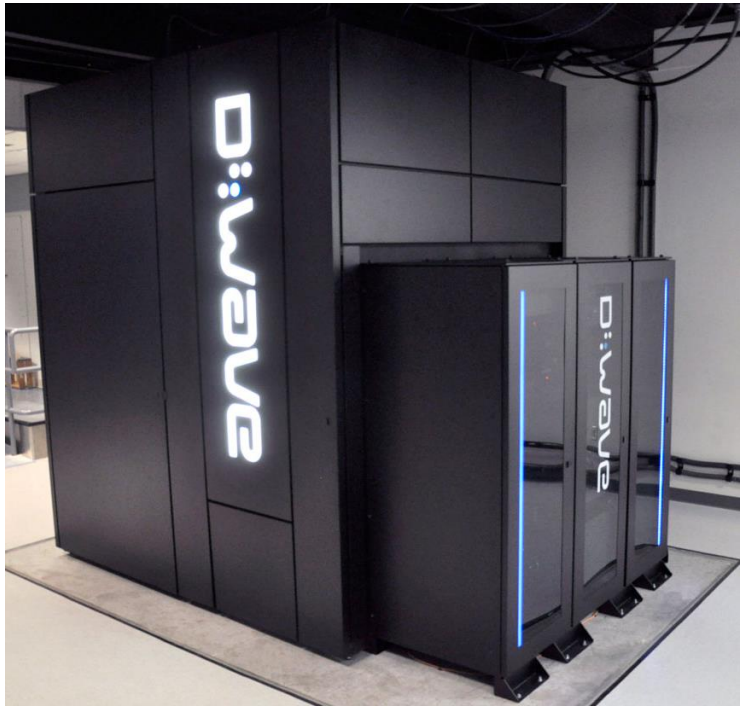
- **Primavera 2013**:

Quantum computer D-Wave Two™ installato presso il centro NASA Advanced Supercomputing (NAS) del Ames Research Center

- …

- **Gennaio 2017**:

Annunciato D-Wave 2000Q con 2000 qubit



Sistemi che si basano su ***quantum annealing***, meno versatili di quelli basati su ***quantum superposition***

Verso il Quantum Computer (2)

The Washington Post
2 Gennaio 2014

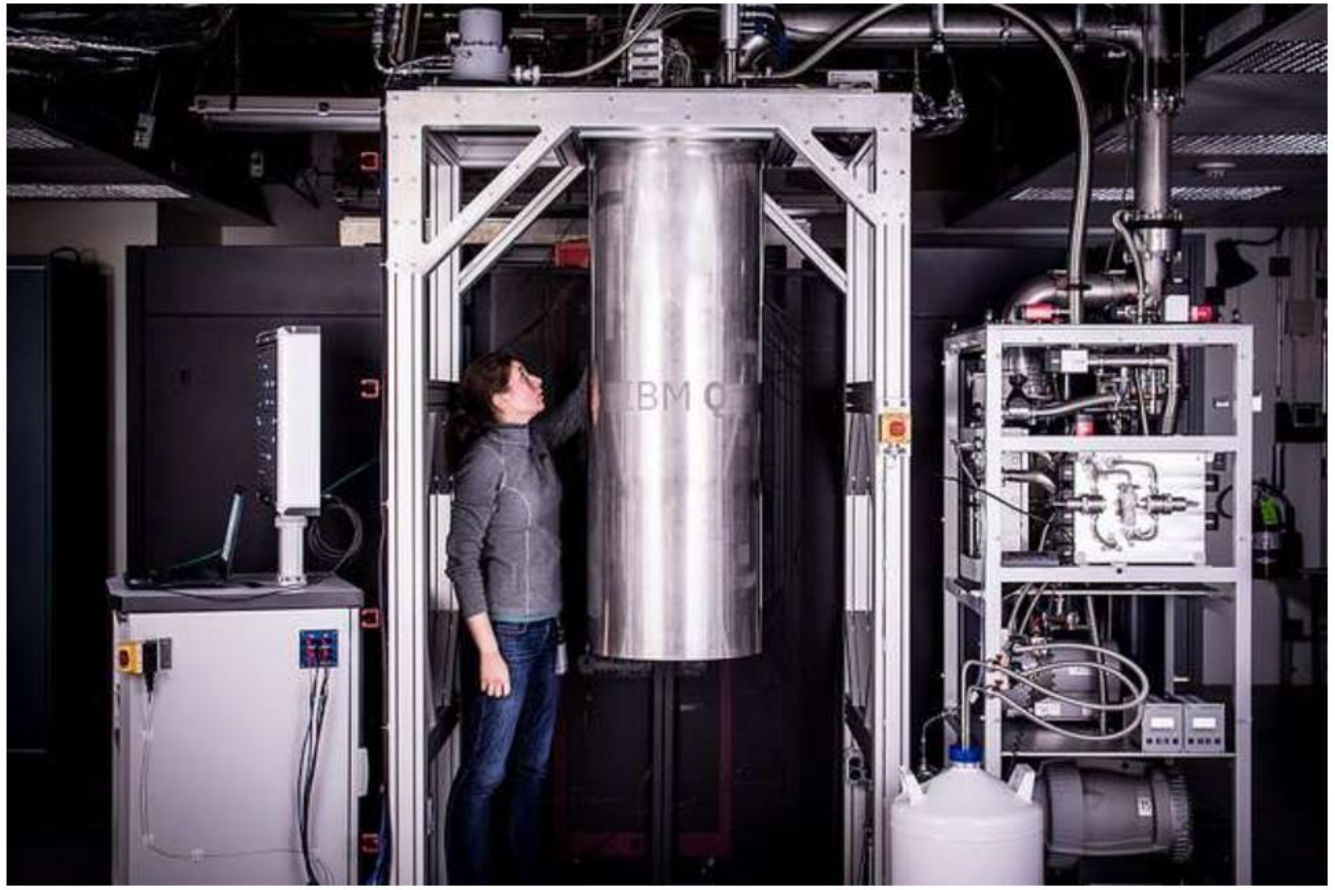
- The effort to build “a cryptologically useful quantum computer” — a machine exponentially faster than classical computers — is part of a $79.7 million research program titled “Penetrating Hard Targets.” Much of the work is hosted under classified contracts at a laboratory in College Park, Md.

- Seth Lloyd, an MIT professor of quantum mechanical engineering, said the NSA’s focus is not misplaced. “The E.U. and Switzerland have made significant advances over the last decade and have caught up to the U.S. in quantum computing technology,” he said.

Verso il Quantum Computer (3)

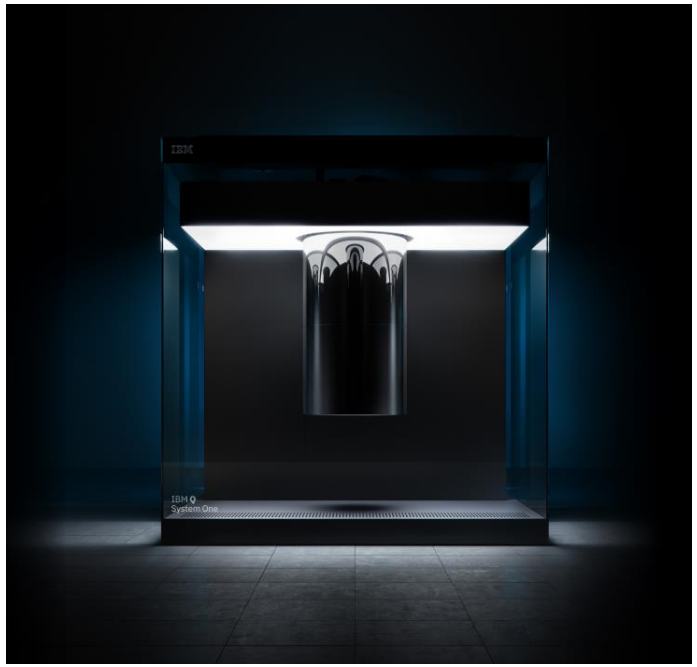
IBM builds its most powerful universal quantum computing

May 17, 2017



IBM Research Staff Member Katie Pooley, a Physics PhD from Harvard who recently joined IBM, pictured at the Thomas J Watson Research Center, working on a new prototype of a commercial quantum processor, which will be the core for the first ... more

IBM Q



- «**Q System One**» di IBM è stato il primo quantum computer per scopi commerciali
- Il sistema aveva **20 qubit** (50 qubit sono ritenuti necessari per competere con i computer classici, anche detta quantum supremacy)
- Basato su **quantum superposition**
- Per funzionare, va mantenuto ad una temperatura bassissima ed isolato da ogni forma di rumore elettromagnetico
- Equivalente quantum dei primi computer degli anni ’50 e ’60
- Disponibili simulatori e modelli software per la programmazione

Verso il Quantum Computer (4)

- **2017**:

Google lavora ad un quantum computer a 72 qubit che si rivela troppo difficile da controllare.

- **Gennaio 2019**:

IBM annuncia il suo Q System One con **20 qubit** basati su **quantum superposition**.

- **Ottobre 2019**:

Google annuncia che il suo sistema Sycamore con **53 qubit** è capace di eseguire in 200 secondi un calcolo che richiederebbe 10’000 anni se eseguito sul più potente supercomputer del mondo.

- **Ottobre 2020**:

La startup IonQ annuncia il lancio di un quantum computer a 32 qubit con bassi tassi d’errore, necessari affinché la tecnologia sia scalabile.

Verso il Quantum Computer (5)

- **2020**:

un team dell'Università della Scienza e Tecnologia della Cina (USTC) sviluppa Jiuzhang, un quantum computer basato su fotoni anziché superconduttori.

- **Giugno 2021**:

Ricercatori cinesi sperimentano Zuchongzi, dotato di **56 qubit** basati su superconduttori.

- **Ottobre 2021**:

Zuchongzi viene esteso a **66 qubit**.

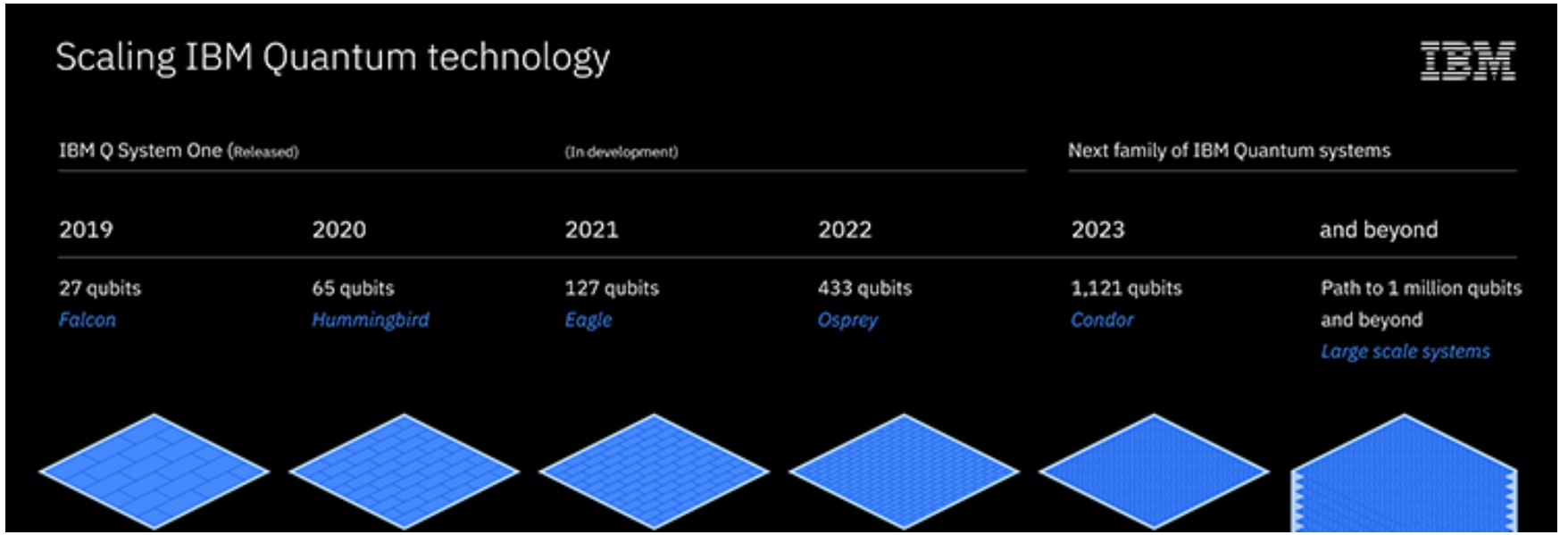
- **Novembre 2022**:

IBM annuncia il completamento dello sviluppo di una unità di elaborazione quantistica (QPU) da **433 qubit** prevista per il 2022, denominata Osprey.

Verso il Quantum Computer (6)

- **2023**:

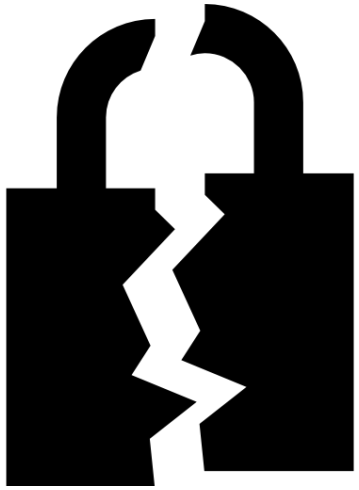
IBM prevede di sviluppare il sistema Quantum Condor con più di **1000 qubit**.



- **2030**:

Potrebbe esistere un quantum computer capace di rompere RSA a 2048 bit.

Crittografia quantum-vulnerable



I sistemi crittografici attualmente più diffusi si basano su problemi matematici risolvibili con l'algoritmo di **Shor**:

- **RSA**

(crittosistema a chiave pubblica basato su fattorizzazione di numeri interi, usato in SSL/TLS, online banking, ATM,…)

- **ElGamal**

(crittosistema a chiave pubblica basato su logaritmo discreto, usato in SSL/TLS,…)

- **Diffie-Hellman, ECDH**

(protocollo di scambio di chiave basato su logaritmo discreto, usato in SSL/TLS, NFC/contactless,…)

- **ECC**, **DSA**, **ECDSA**,…

Crittografia Post-Quantum

- **Sistemi asimmetrici**:
  - Basati su reticoli
  - Basati su codici
  - Basati su sistemi multivariati
  - Basati su funzioni hash
  - Altri (isogenie…)
- **Sistemi simmetrici**:
  - Sistemi di cifratura simmetrica (AES…)
  - Funzioni hash (SHA…)

Bisogna però tenere conto dell'accelerazione degli attacchi dovuta all'algoritmo di **Grover**

NIST PQcrypto Project

Nel 2016 il NIST ha avviato un processo per lo sviluppo e la standardizzazione di uno o più algoritmi crittografici a chiave pubblica per:

- **Public-key encryption (PKE)**
  - key generation, encryption and decryption
- **Key encapsulation mechanism (KEM)**
  - key generation, encapsulation and decapsulation
- **Digital signature**
  - key generation, signature generation and signature verification

NIST PQcrypto timeline

- **20 Dicembre 2016**: Pubblicazione ufficiale del bando
- **30 Novembre 2017**: Scadenza del termine per l'invio da parte dei candidati
- **30 Gennaio 2019**: Annuncio dei candidati ammessi al secondo round (17 per PKE+KEM e 9 per firma digitale)
- **22 Luglio 2020**: Annuncio dei candidati ammessi al terzo round (finalisti: 4 per PKE+KEM e 3 per firma digitale, alternativi: 5 per PKE+KEM e 3 per firma digitale)
- **5 Luglio 2022**: Annuncio dei candidati da standardizzare (1 per PKE+KEM e 3 per firma digitale) e ammessi al quarto round (4 per PKE+KEM)
- **6 Settembre 2022**: Pubblicazione di un nuovo bando per firme digitali post-quantum

Livelli di Sicurezza

Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for:

1. key search on a block cipher with a **128-bit** key (e.g. AES128)
2. collision search on a 256-bit hash function (e.g. SHA256/ SHA3-256)
3. key search on a block cipher with a **192-bit** key (e.g. AES192)
4. collision search on a 384-bit hash function (e.g. SHA384/ SHA3-384)
5. key search on a block cipher with a **256-bit** key (e.g. AES 256)

Candidati Primo Round

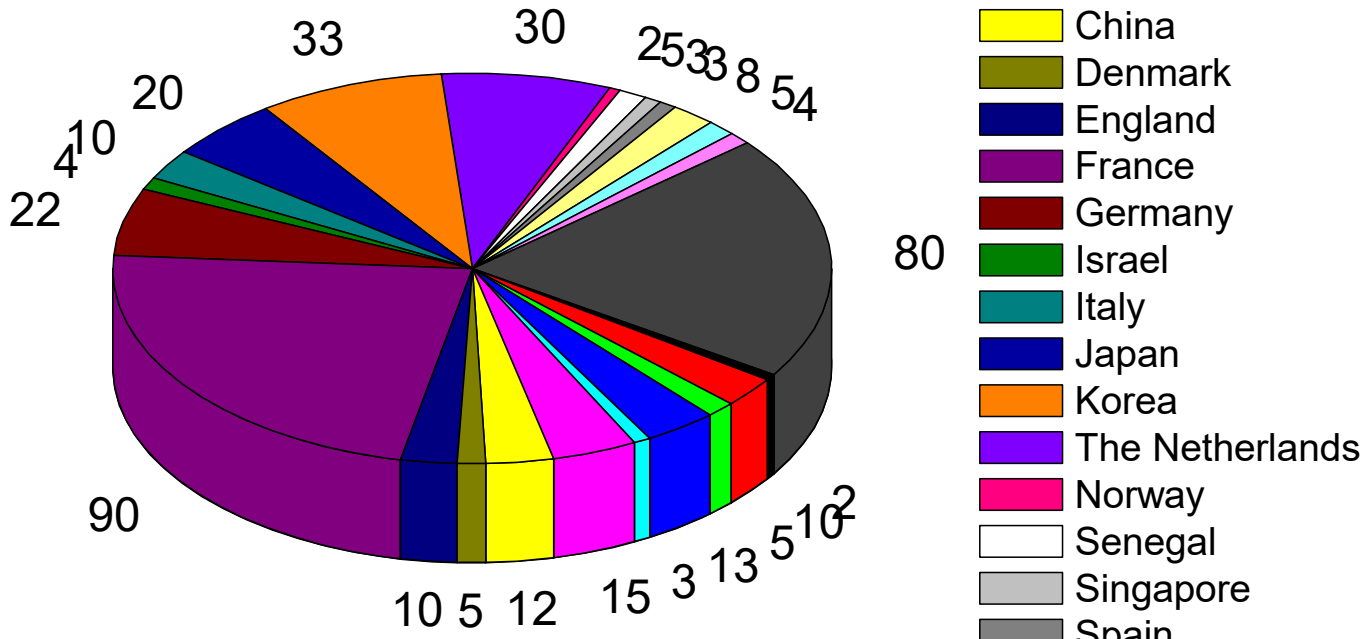
FINAL SUBMISSIONS RECEIVED

- The deadline is past – no more submissions
- 82 total submissions received
  - 23 signature schemes
  - 59 Encryption/KEM schemes

	Signatures	KEM/Encryption	Overall
Lattice-based	4	24	28
Code-based	5	19	24
Multi-variate	7	6	13
Hash-based	4		4
Other	3	10	13
Total	**23**	**59**	**82**

Candidati Primo Round (2)

263 ricercatori provenienti da
24 Paesi diversi



https://www.ledacrypt.org/

NIST – Esito terzo round

- Annunciato il **5 Luglio 2022**
- Selezionati per la standardizzazione:
  - **CRYSTALS-KYBER** (KEM) e **CRYSTALS-Dilithium** (firme digitali) sono entrambi basati su **reticoli** e selezionati per la loro forte sicurezza e le eccellenti prestazioni. Il NIST si aspetta che funzionino bene nella maggior parte delle applicazioni.
  - **FALCON** (firme digitali) è basato su **reticoli** e sarà standardizzato perché potrebbero esistere casi d'uso per i quali le firme CRYSTALS-Dilithium sono troppo grandi.
  - **SPHINCS+** (firme digitali) è basato su funzioni **hash** e sarà standardizzato per evitare di affidarsi solo alla sicurezza dei problemi basati su reticoli per le firme digitali.
- Ammessi al quarto round: **BIKE**, **Classic McEliece**, **HQC**, **SIKE**

NIST – Bersaglio centrato?

- Il percorso del NIST ha avuto diversi «**imprevisti**»
- **Rainbow**, sistema di firma digitale basato su equazioni multivariate ammesso al terzo round a Luglio 2020 come finalista è stato crittanalizzato da Ward Beullens a Febbraio 2022.
- **SIKE**, sistema di scambio di chiavi basato su isogenie ammesso al quarto round a Luglio 2022 è stato crittanalizzato da Castryck e Decru poche settimane dopo.
- Per le firme digitali non si è raggiunta sufficiente diversità (solo sistemi basati su **reticoli** e SPHINCS+ basato su **hash**, che è lento), perciò si è resa necessaria la riapertura di una nuova gara.

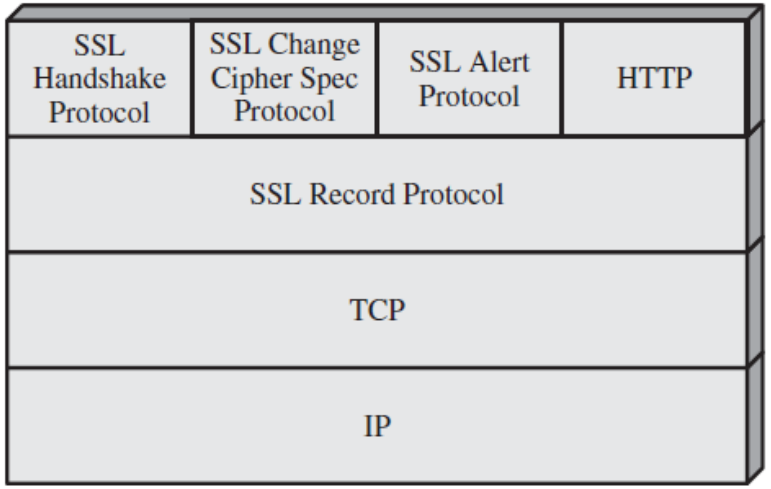
Dove la usiamo? … SSL/TLS

https://www.

- Secure Socket Layer (SSL): protocollo introdotto da Netscape nel 1994 per realizzare servizi sicuri basati su TCP

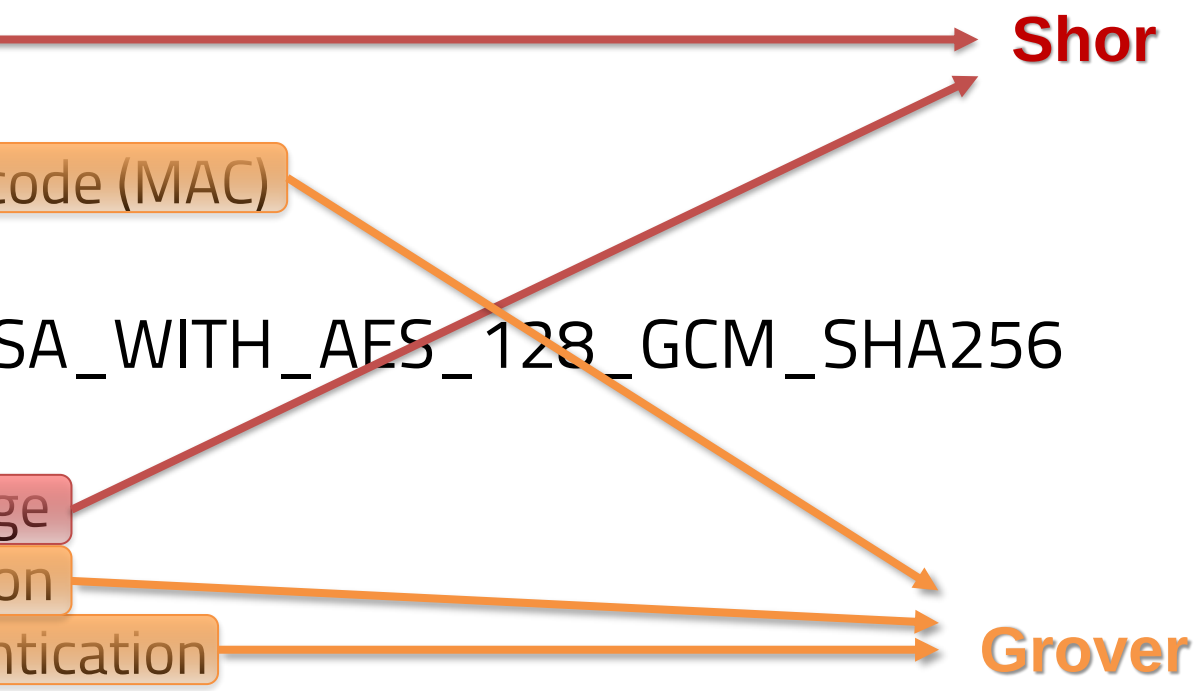
- Transport Layer Security (TLS) è un'iniziativa di standardizzazione IETF allo scopo di produrre una versione standard di SSL

- **Gennaio 1999**: TLS 1.0 (RFC 2246)
- **Aprile 2006**: TLS 1.1 (RFC 4346)
- **Agosto 2008**: TLS 1.2 (RFC 5246)
- **Agosto 2018**: TLS 1.3 (RFC 8446)



TLS cipher suite

- Gruppo di algoritmi crittografici per:
  - key exchange
  - bulk encryption
  - message authentication code (MAC)
- Esempio: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - ECDHE_RSA: key exchange
  - AES_128_GCM: encryption
  - SHA256: message authentication



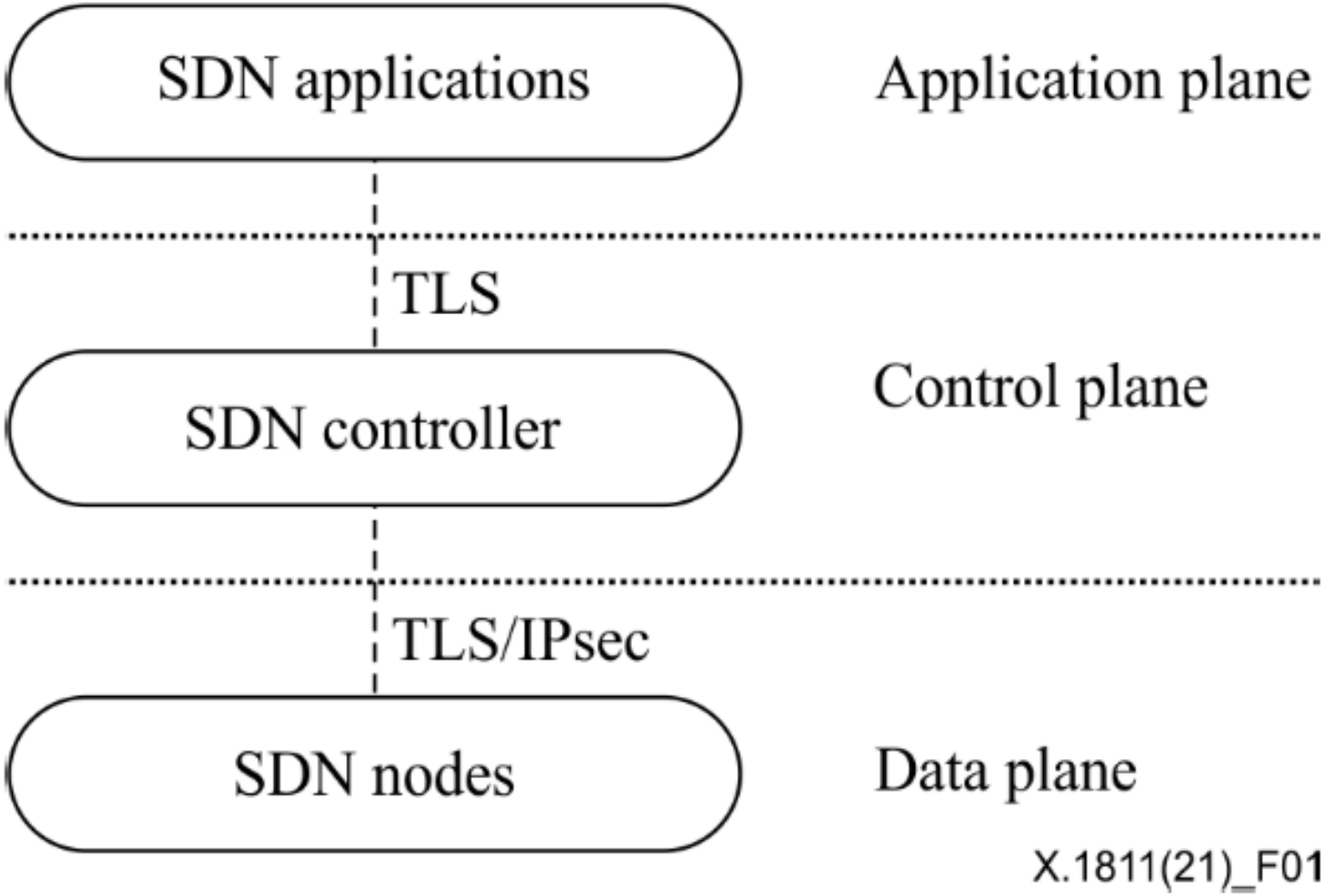
Dove la usiamo? … IKEv2/IPsec

- Internet Key Exchange versione 2 (IKEv2) è un protocollo di tunneling incluso in **IPsec**, usato per creare una **Virtual Private Network** (VPN).
- IKEv2 serve a generare e distribuire chiavi crittografiche per garantire comunicazione sicura tra l'utente e il server VPN.
- IKEv2 è più veloce e stabile di OpenVPN (basato su SSL) e offre una funzione di riconnessione automatica che migliora la sicurezza e la facilità d'uso.
- IKEv2/IPsec usa AES-256-GCM per la cifratura simmetrica e SHA2-384 per l'integrità.
- Per lo scambio di chiavi si usa Diffie-Hellmann a 3072 bit con perfect forward secrecy (PFS).

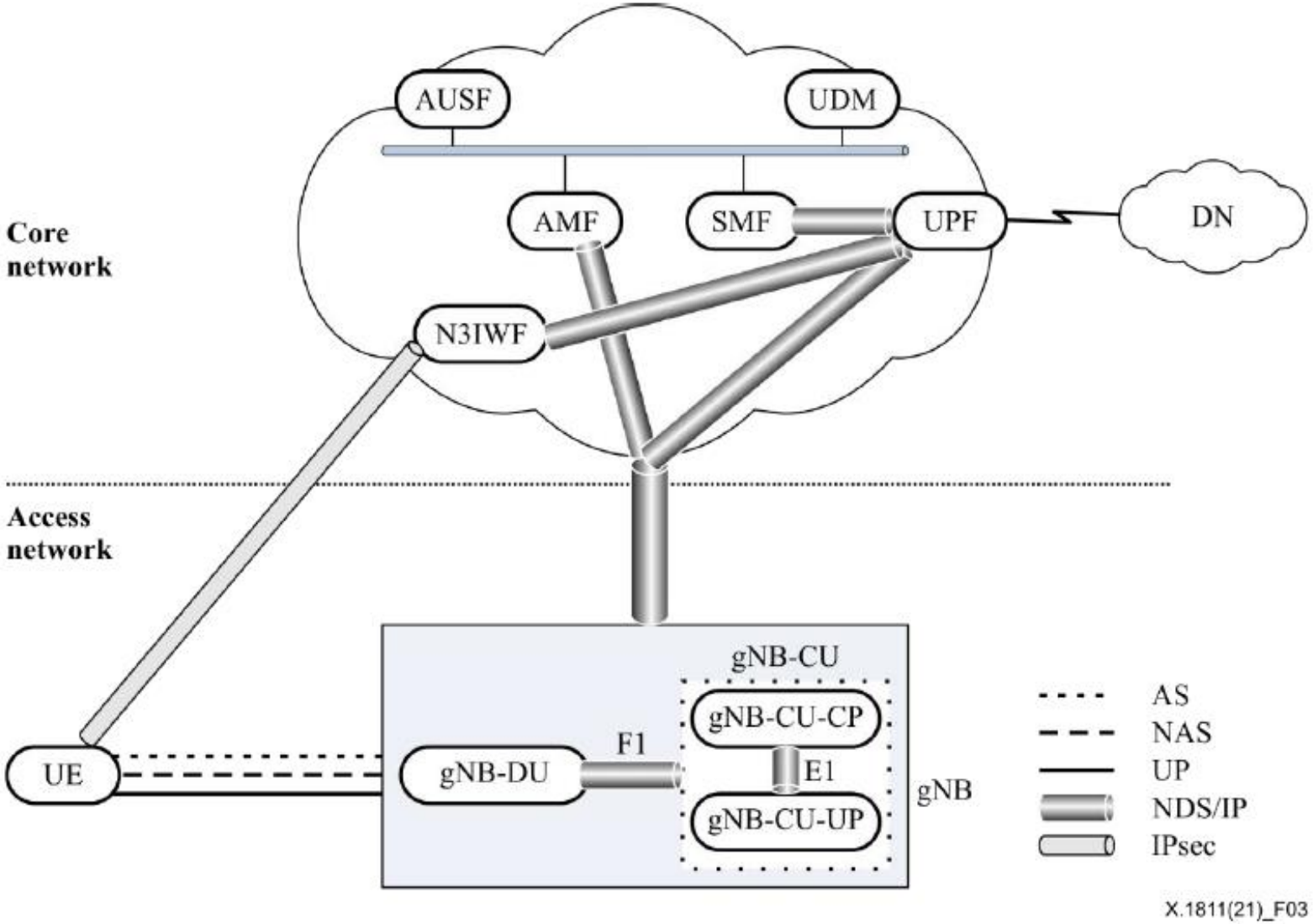
Shor

Grover

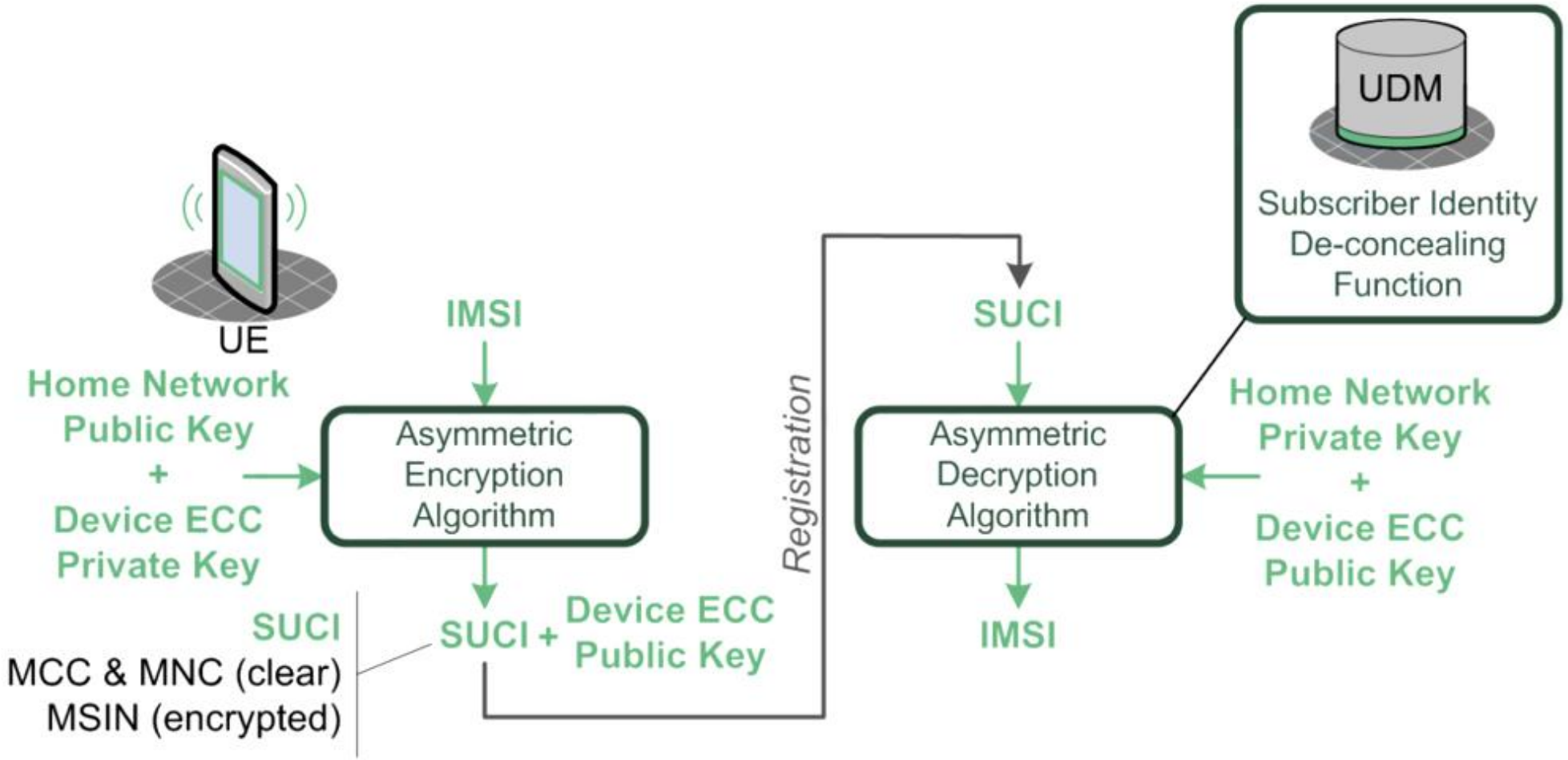
E nel 5G? (software-defined network)



E nel 5G? (access network)



E nel 5G? (subscriber privacy)



Siamo pronti? …Quantum-safe TLS

[Search] [txt|html|xml|pdfized|bibtex] [Tracker] [WG] [Email] [Nits]
Versions: (draft-stebila-tls-hybrid-design) 00
01 02 03 04 05

Network Working Group
Internet-Draft
Intended status: Informational
Expires: 17 October 2020

D. Stebila
University of Waterloo
S. Fluhrer
Cisco Systems
S. Gueron
U. Haifa, Amazon Web Services
15 April 2020

Hybrid key exchange in TLS 1.3
draft-ietf-tls-hybrid-design-00

Abstract

Hybrid key exchange refers to using multiple key exchange algorithms simultaneously and combining the result with the goal of providing security even if all but one of the component algorithms is broken. It is motivated by transition to post-quantum cryptography. This document provides a construction for hybrid key exchange in the Transport Layer Security (TLS) protocol version 1.3.

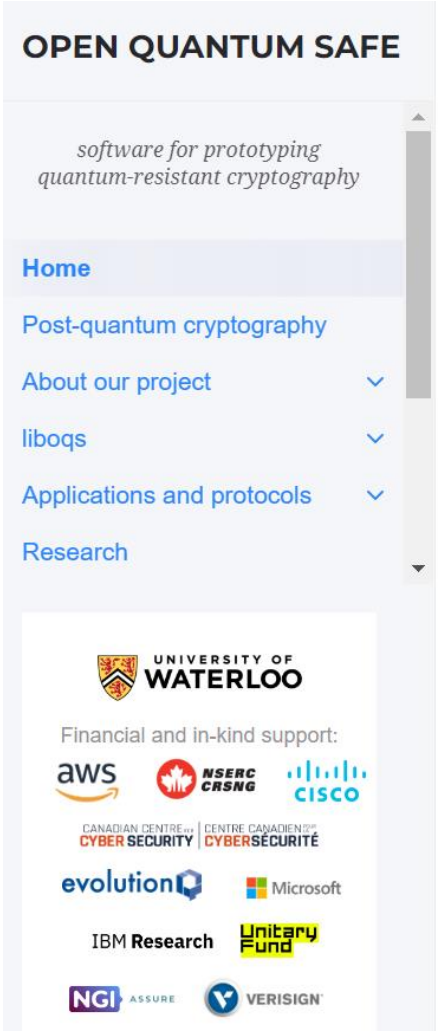
Discussion of this work is encouraged to happen on the TLS IETF mailing list tls@ietf.org or on the GitHub repository which contains the draft: https://github.com/dstebila/draft-ietf-tls-hybrid-design.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Siamo pronti? …Open Quantum Safe



The Open Quantum Safe (OQS) project is an open-source project that aims to support the development and prototyping of quantum-resistant cryptography.

OQS consists of two main lines of work: liboqs, an open source C library for quantum-resistant cryptographic algorithms, and prototype integrations into protocols and applications, including the widely used OpenSSL library. These tools support research by ourselves and others.

All of our development takes place on our Github repositories. We welcome new contributors interested in joining our team. We are grateful to our financial sponsors and the companies who contribute in-kind developer time.

Siamo pronti? …Quantum-safe IKEv2

From: draft-ietf-ipsecme-qr-ikev2-11 Proposed Standard

Internet Engineering Task Force (IETF)
Request for Comments: 8784
Category: Standards Track
ISSN: 2070-1721

S. Fluhrer
P. Kampanakis
D. McGrew
Cisco Systems
V. Smyslov
ELVIS-PLUS

June 2020

Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security

Abstract

The possibility of quantum computers poses a serious challenge to cryptographic algorithms deployed widely today. The Internet Key Exchange Protocol Version 2 (IKEv2) is one example of a cryptosystem that could be broken; someone storing VPN communications today could decrypt them at a later time when a quantum computer is available. It is anticipated that IKEv2 will be extended to support quantum-secure key exchange algorithms; however, that is not likely to happen in the near term. To address this problem before then, this document describes an extension of IKEv2 to allow it to be resistant to a quantum computer by using preshared keys.

Conclusioni

- Il **quantum computer** sta rapidamente diventando realtà.
- Esso mette a rischio la **sicurezza** degli attuali **sistemi crittografici**.
- I sistemi crittografici **simmetrici** possono essere **adattati**, quelli **asimmetrici** devono essere **sostituiti**.
- Il **5G** fa pesante uso della **crittografia** per proteggere la sicurezza della rete e la privacy degli utenti.
- **3GPP** ha già iniziato a studiare l'adozione di chiavi di 256 bit nei **cifrari simmetrici** usati in **5G** (3GPP TR 33.841 V16.1.0) per contrastare l'algoritmo di Grover.
- **3GPP** considera invece prematuro studiare l'inclusione di **cifrari asimmetrici post-quantum** in **5G**, in quanto non sono ancora disponibili i primi standard NIST (previsti entro il 2024).