Crittografia quantica e post-quantica

Giovanni Cancellieri
AEIT - Università Politecnica delle Marche
g.cancellieri@staff.univpm.it

Giornata di studio sulla Cyber Security
Milano, 23 gennaio 2020, FAST

Argomenti

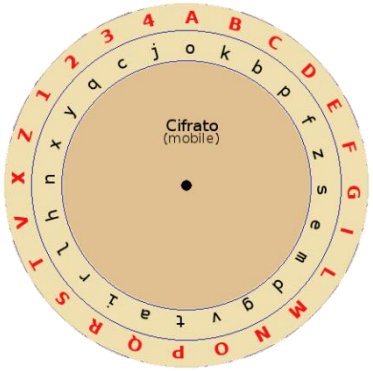
- Breve storia della cifratura
- Cifratura a doppia chiave
- Potenza e criticità di una blockchain
- Stato dell’arte dei computer quantistici
- Un computer quantistico potrebbe forzare un sistema crittografico tradizionale a doppia chiave
- Crittografia quantistica (per pochi privilegiati)
- Crittografia post-quantistica: cioè un algoritmo di crittografia tradizionale (per tutti) potrebbe resistere all’attacco di un calcolatore quantistico

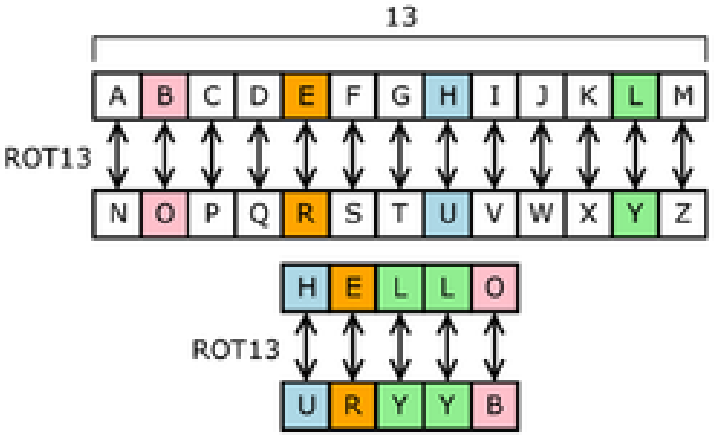
Principali tappe della storia della cifratura

- Il cifrario di Giulio Cesare

Testo in chiaro	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifratura	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Il disco di Leon Battista Alberti





Principali tappe della storia della cifratura

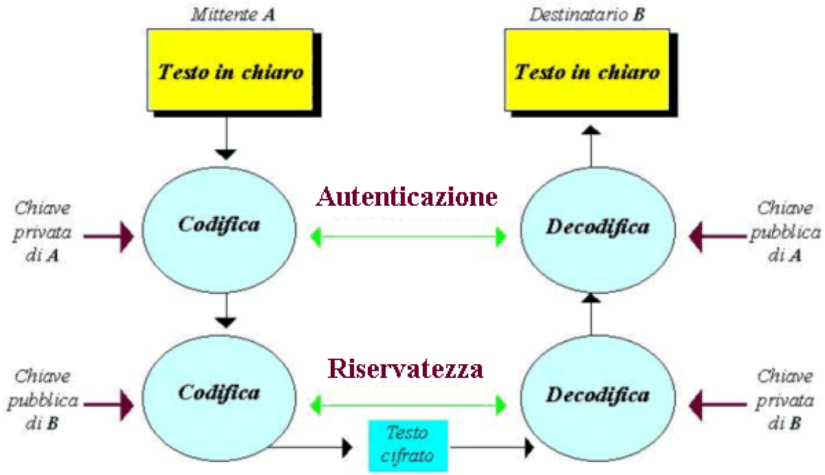
- La macchina cifrante Enigma

- Sistemi di steganografia

Tutti sistemi uno-a-uno (crittografia simmetrica)
a chiave singola

Crittografia moderna basata su una doppia chiave (1/4)

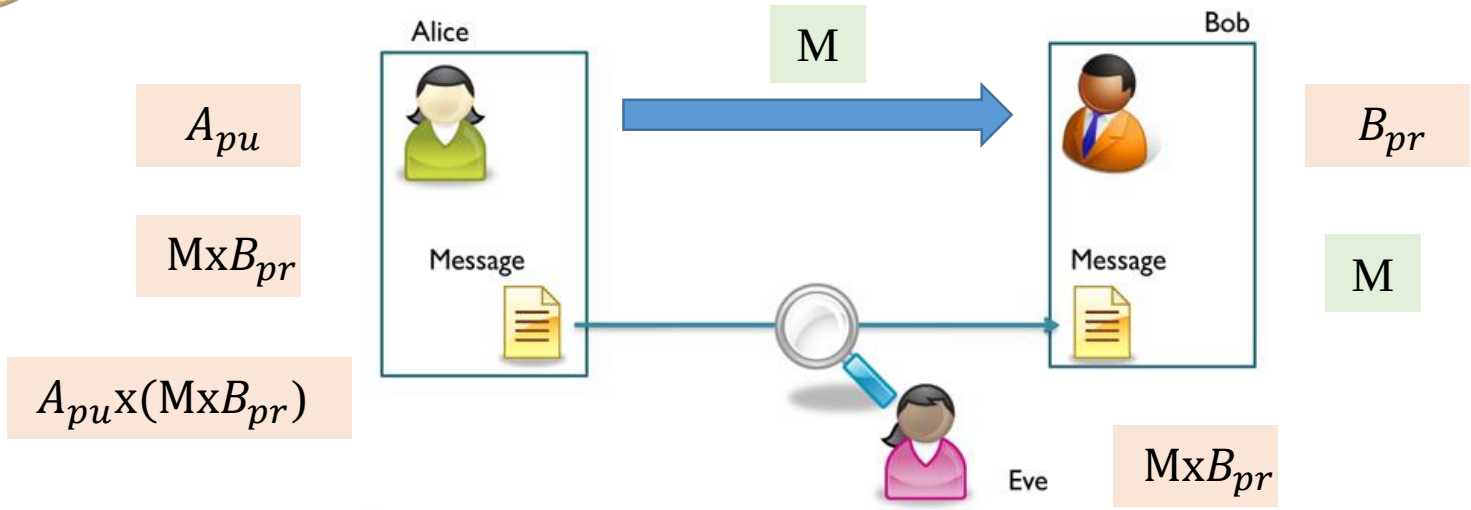
Ogni utente di una rete ha **due chiavi**:
- una chiave pubblica (nota a tutti);
- una chiave privata (nota solo a coloro con cui vuole corrispondere).



In totale ci sono 4 chiavi tra A e B.
Per garantire la riservatezza si usa prima l'una poi l'altra.
Per garantire l'autenticazione si fa in modo inverso.

Esempio: firma certificata

Crittografia moderna basata su una doppia chiave (semplificato) (2/4)

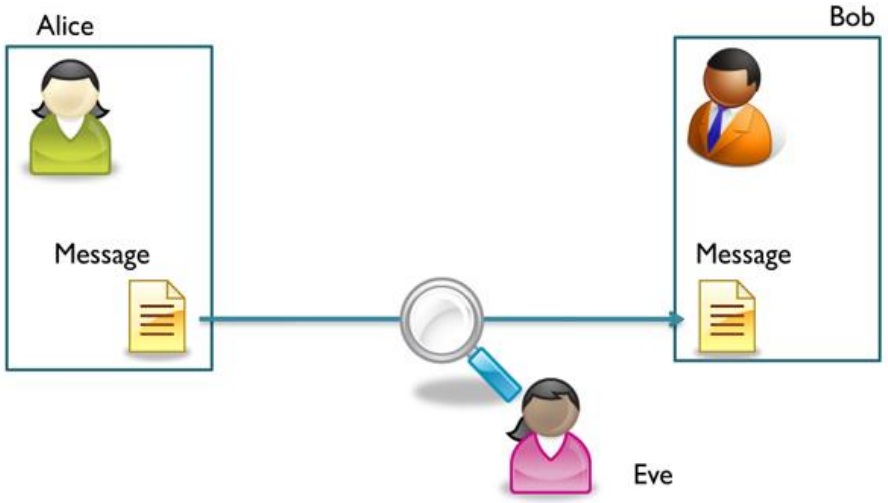


- Alice vuole trasmettere a Bob il messaggio M
- Alice ha una chiave pubblica A_{pu}. Bob ha una chiave privata B_{pr}
- Alice moltiplica per la chiave privata di Bob e ottiene n = MxB_{pr}
- Alice rimoltiplica per la sua chiave pubblica: e ottiene A_{pu}x(MxB_{pr})
- Eve può dividere per A_{pu}, ma, non conoscendo B_{pr} , non perviene a M
- Invece Bob conoscendo anche B_{pr}, esegue due divisioni e perviene a M

Crittografia moderna basata su una doppia chiave (semplificato) (3/4)

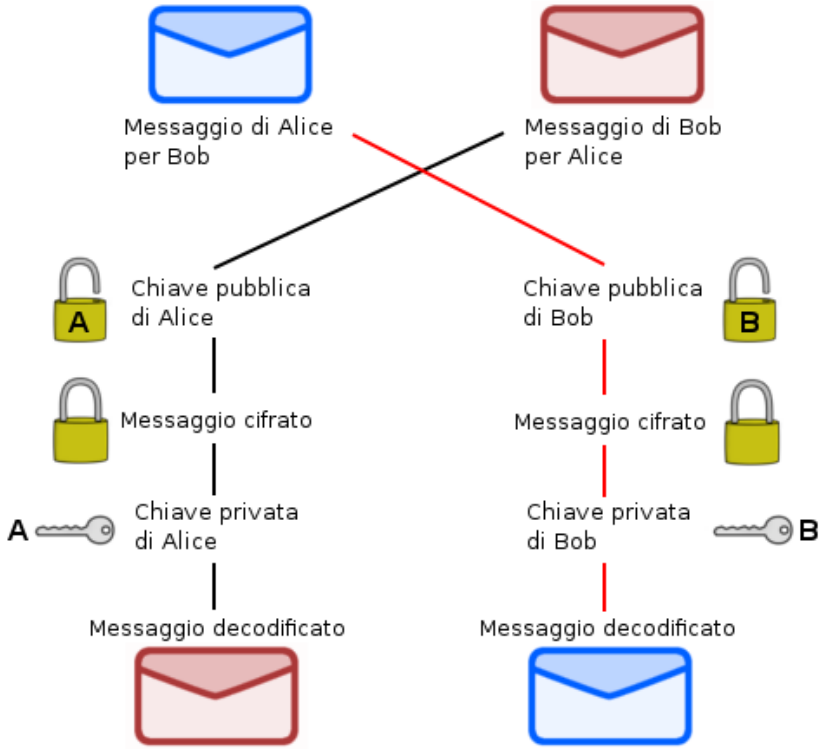
La chiave privata è costituita da un numero primo molto grande (dell'ordine di 2^m, con m = 1024).

La chiave pubblica è un numero più piccolo. Dell'ordine del numero totale degli utenti.



Difficoltà per Eve, che si inserisce in mezzo:
scomporre in fattori primi un numero n molto grande

Crittografia moderna basata su una doppia chiave (semplificato) (4/4)



Il sistema funziona in modo asimmetrico, ma pone tutti gli utenti su un piano di parità

Applicazioni della crittografia a doppia chiave

Sistemi di pagamento elettronici

Fornitura e consegna di beni acquistati on-line

Governo e pubblica amministrazione

Per l'adeguamento al **GDPR**, il testo di legge europeo cita espressamente la necessità di impiegare la crittografia

Transazioni basate su una blockchain

Blockchain (1/5)

La **blockchain** è un registro a disposizione di un gruppo chiuso di utenti, con transazioni tracciabili

Si basa sulla fiducia degli utenti

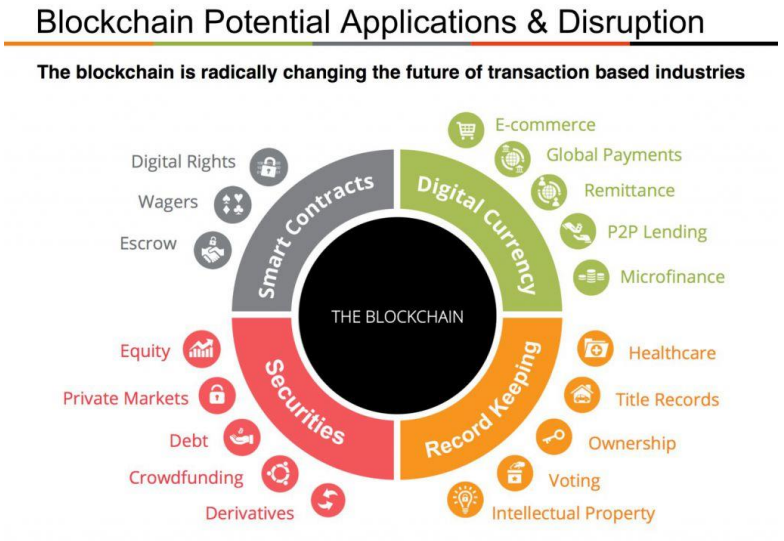
Un attacco, eseguito ad esempio con un **computer quantistico**, creerebbe delle falle che, a macchia di leopardo, incrinerebbero la fiducia nel sistema (e quindi la blockchain si dissolverebbe)

Blockchain (2/5)

Funzionamento

La rete genera a caso dei **codici** corrispondenti ad altrettante informazioni riservate, che gli utenti devono andare a recuperare eseguendo l'azione detta mining

Applicazioni potenziali



Ad ogni utente di una blockchain viene richiesto di effettuare operazioni di mining in un grande data base

Blockchain (3/5)

Uso della blockchain nella costruzione e gestione di **criptovalute**

Una **criptovaluta** viene accettata in conseguenza di una successione di transazioni annotate nella lista bloccata (blockchain)

Il *consenso distribuito*, necessario per accettare la criptovaluta, impone a tutti gli utenti di eseguire operazioni di data mining criptate (cioè sottoposte ad un *sistema crittografico a doppia chiave*)

Blockchain (4/5)

L’attività di mining criptato comporta un elevato **consumo di energia**

Si ipotizza che l’attuale consumo della rete Bitcoin ammonti a oltre 1 GW, come una città di un milione di abitanti

Questa potenza di calcolo è distribuita su tutto il mondo

Punto di forza, ma anche di debolezza

Blockchain (5/5)

Rischi intrinseci

Se un utente acquisisse più del 50 % della potenza di calcolo, potrebbe generare transazioni false

Ad esempio spendere due volte la stessa somma di Bitcoin

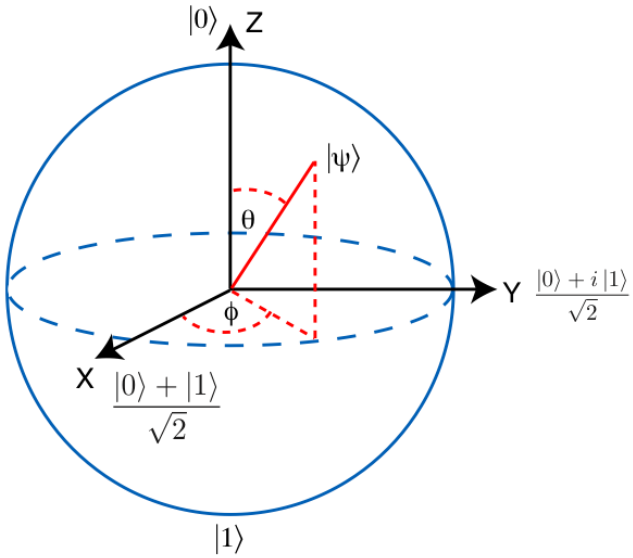
Le transazioni sono pubbliche, ma gli utenti sono protetti da anonimato, quindi tutto il sistema si può prestare a occultare informazioni …

Funzionamento di un computer quantistico (1/3)

Un bit tradizionale può essere soltanto 0 oppure 1.
Il Qubit può essere, al tempo stesso, in parte 0, in parte 1.

Funzione complessa a modulo unitario (simile a una probabilità).

Si usa una rappresentazione mediante una sfera.

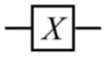
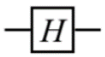


Dunque la quantità di informazione che si può memorizzare in un Qubit (o può essere trasportata per il suo tramite) è **molto superiore** a quella che è assegnata a un bit tradizionale.

Funzionamento di un computer quantistico (2/3)

Le probabilità dei due stati quantici vengono manipolate da gate quantici

Esempi:

Gate	Notation	Matrix
NOT (Pauli-X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Z		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
CNOT (Controlled NOT)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

Alla fine, una misura fa diventare certo uno stato quantico definito, che risulta la risposta al problema

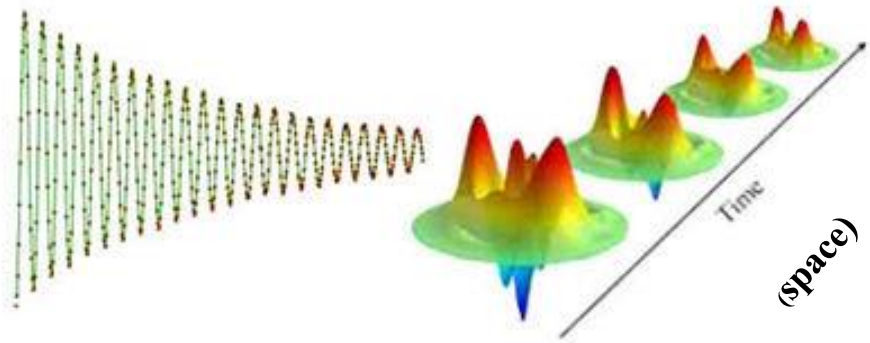
Problemi con complessità computazionale esponenziale
possono essere risolti, da un calcolatore quantistico, con complessità computazionale lineare

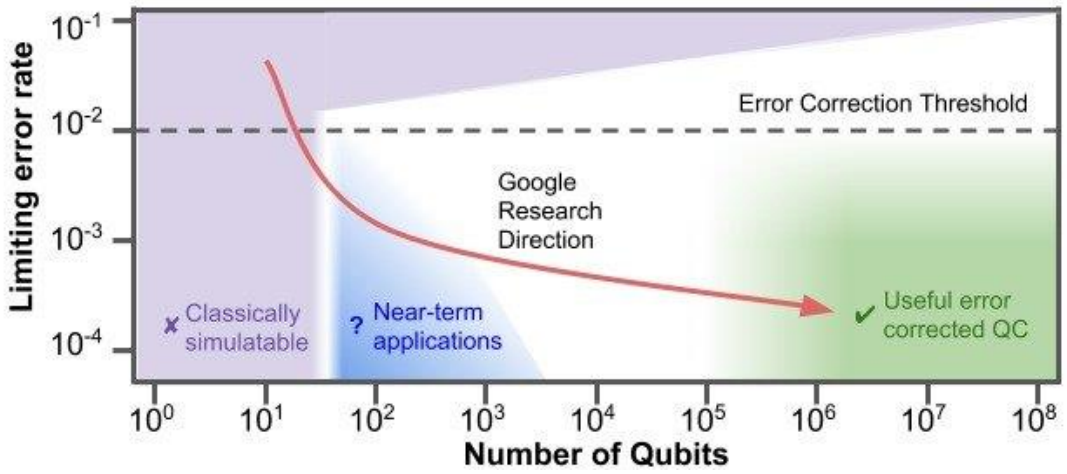
Funzionamento di un computer quantistico (3/3)

Purtroppo non tutto va come si vorrebbe.
C'è il problema della **perdita di coerenza** (nel tempo) da parte degli stati quantici.

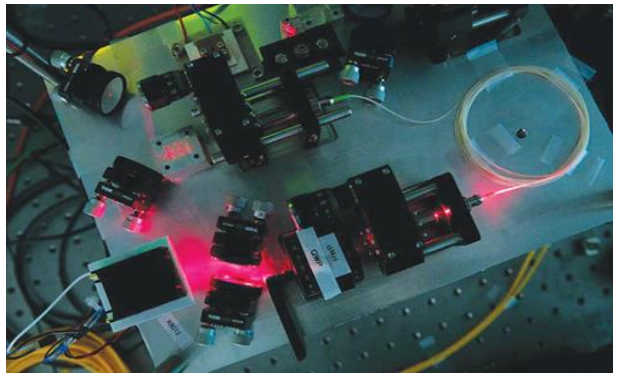
Con l'uso di fotoni, impiegando lo stato di polarizzazione come variabile quantica, questo problema insorge nel trasferire l'informazione nello spazio (dentro il computer quantistico o fuori).

L'inconveniente viene combattuto con l'uso della **codifica di canale**





Trasferimento di informazioni quantistiche a distanza (primo accenno alla crittografia quantistica)



E' stata provata sperimentalmente la possibilità di coprire una distanza di alcune centinaia di km su una **fibra ottica speciale**.

In alternativa, si possono usare **satelliti** (esperimento tra Vienna e Pechino nel gennaio 2018).

Tuttavia si può costruire un sistema di **crittografia quantistica** soltanto **simmetrico** e a **singola chiave**

In pratica, si usa questa tecnica solo per effettuare una **distribuzione sicura delle <u>chiavi</u> crittografiche <u>private</u>** (in un sistema a doppia chiave tradizionale)

QKD:
Quantum Key Distribution

Progresso nei computer quantistici

- Ottobre **2011**

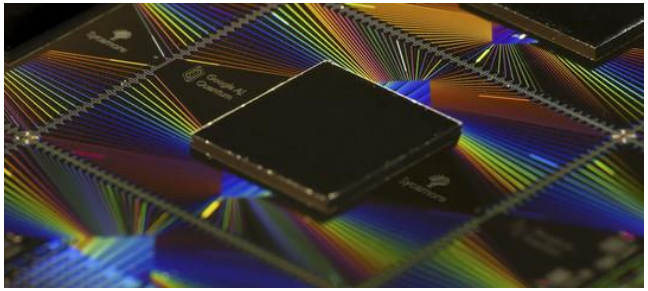
  Primo **centro pubblico-privato** di quantum computing (Univ. South California, Lockheed Martin e D-Wave Systems)

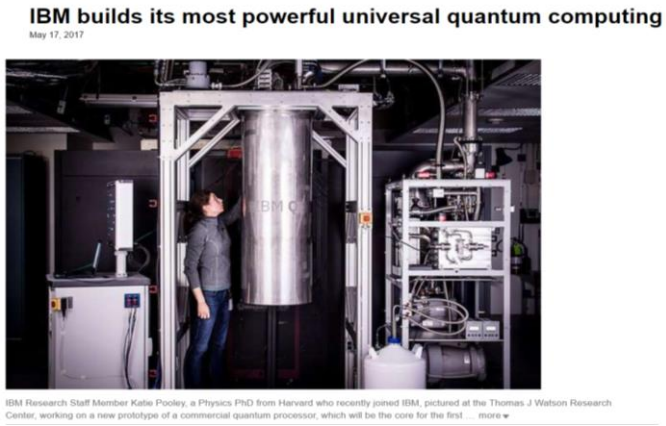
- Novembre **2016**

  D-Wave annuncia la possibilità di costruire un quantum computer a **2000 Qubit**

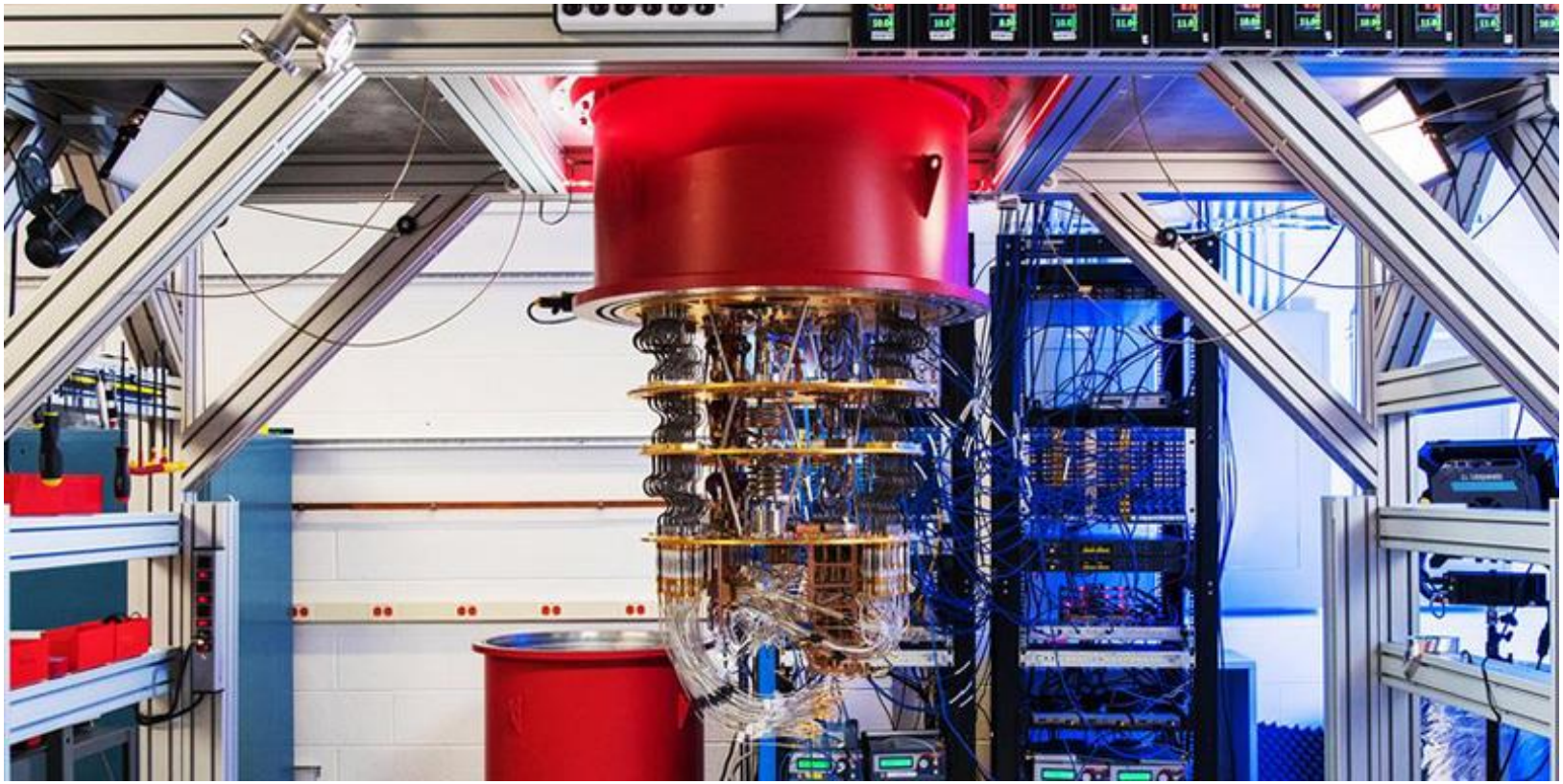
- Settembre **2019**

  IBM costruisce e commercializza un quantum computer a **54 Qubits**





Computer quantistici raffreddati



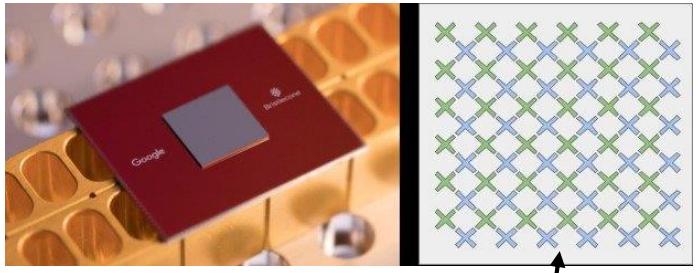
Google afferma di aver raggiunto la
supremazia quantistica

Spiegazione del Quantum Supremacy

Il processore **Sycamore** (di **Google**) a 53 Qubit ha svolto in 3 minuti e 20 secondi un calcolo che avrebbe richiesto 10 mila anni a un super-PC sviluppato da **IBM**

(*pubblicato su Nature il 23 ottobre 2019*)

Nel Quantum AI Lab di **Google** sarebbe stato creato anche un chip per computer quantistici da 72 Qubit, chiamato **Bristlecone**



I computer quantistici di Google sembra che possano essere ***general purpose***, e non costruiti per risolvere solo determinati problemi

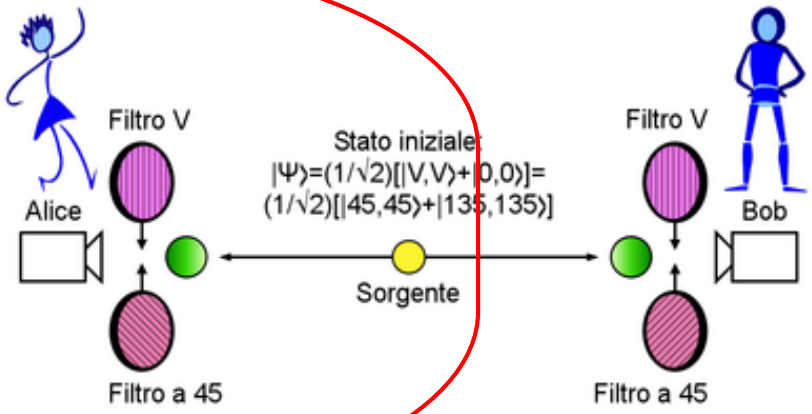
Disposizione spaziale dei Qubit

Come un **computer quantistico** potrebbe forzare sistemi crittografici tradizionali

Trovare i fattori primi di un numero **n** molto grande è un problema che i calcolatori tradizionali risolvono in un **tempo proporzionale ad n (metodo della forza bruta)** o eventualmente **proporzionale a $\sqrt{n}$ (crivello di Eratostene)**.

Invece i **computer quantistici** sono in grado di risolverlo in un **tempo proporzionale a log(n)**.

Crittografia quantistica (1/2)

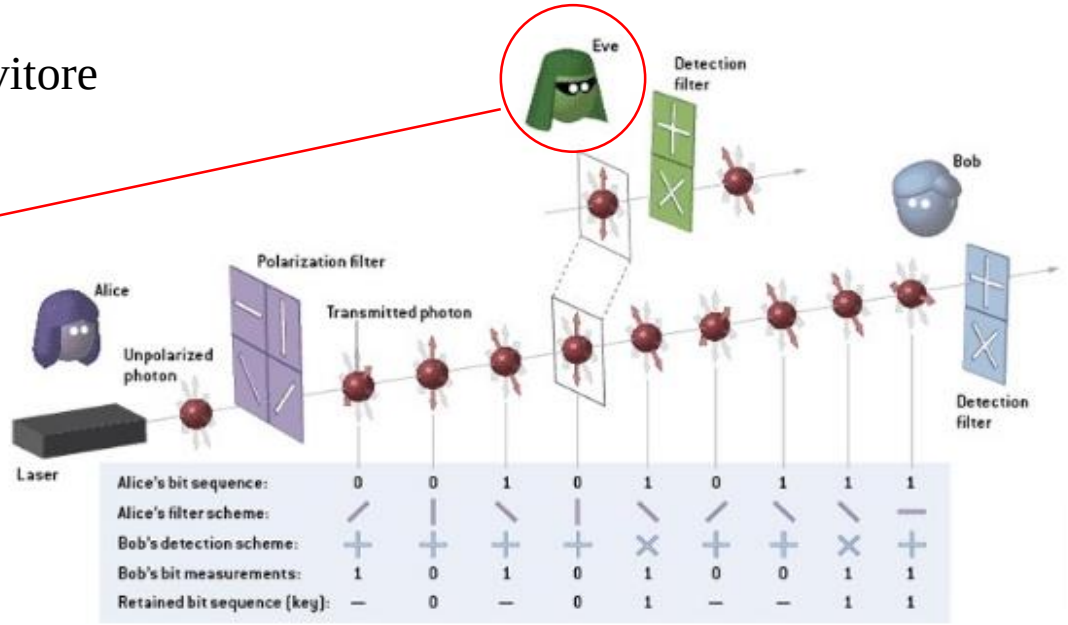


Trasmettitore

Ricevitore

I due fotoni emessi dalla sorgente restano legati.

Qualunque azione Eve possa esercitare sul messaggio, ne hanno contezza sia Alice, sia Bob.

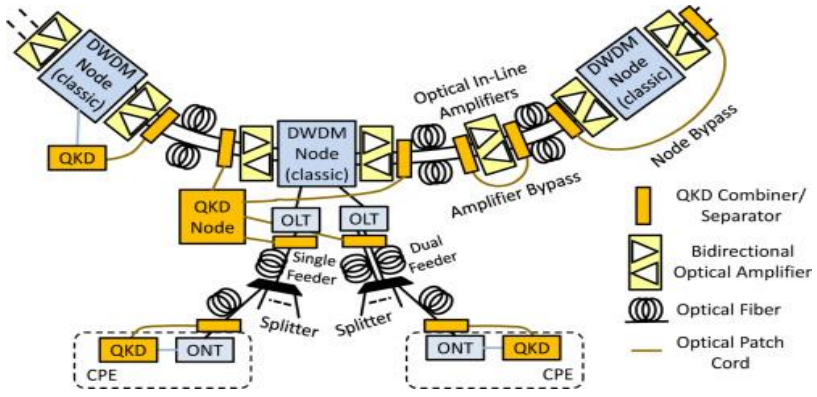


Crittografia quantistica (2/2)

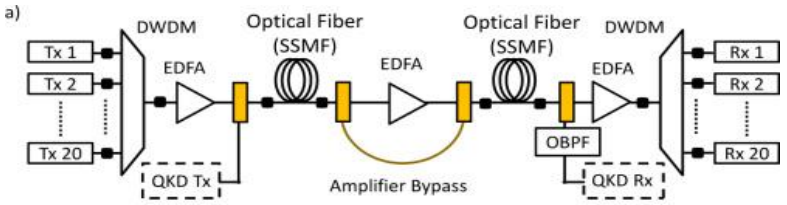
Si può creare una **chiave sicura**, che un destinatario non autorizzato inevitabilmente deteriorerebbe, facendosi scoprire.

Lo **stato quantico** di un sistema è uno stato probabilistico.
Ad esempio un fotone può essere manipolato fino a fargli assumere un certo *stato quantico imbrigliato* (entagled quantum state).
E viene lasciando un *gemello* presso colui che lo ha manipolato.

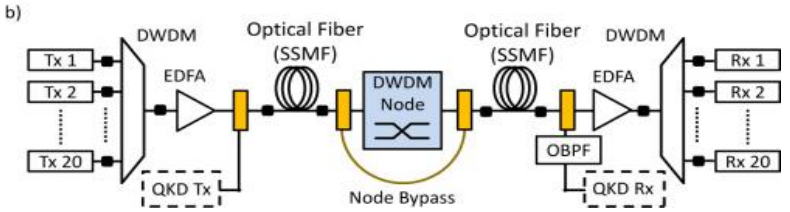
Ma non tutto è così semplice!



Struttura della rete di trasporto ottica

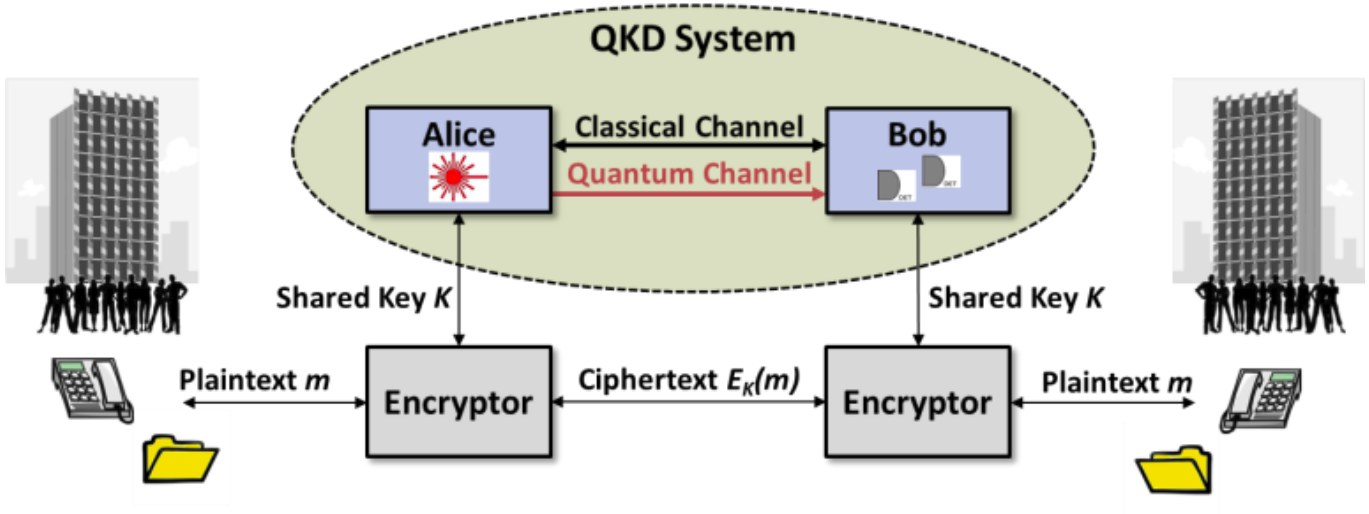


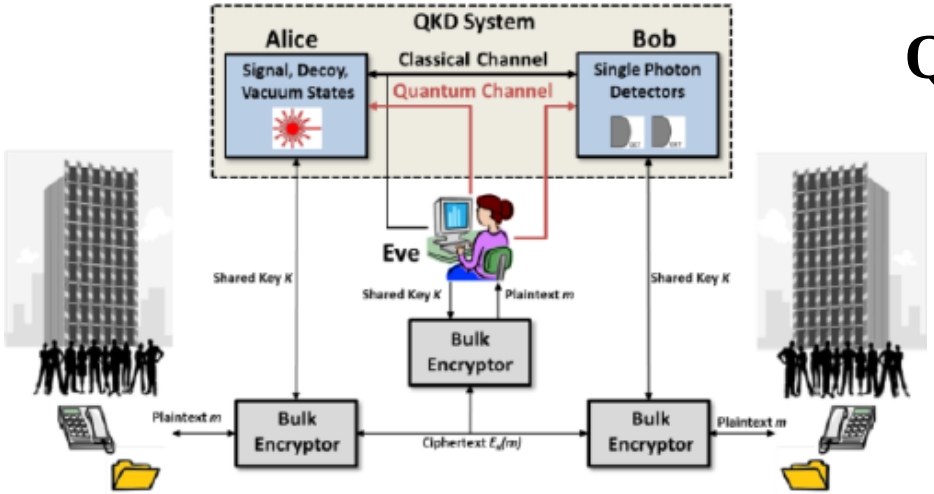
By-pass di amplificatori ottici



By-pass di nodi DWDM

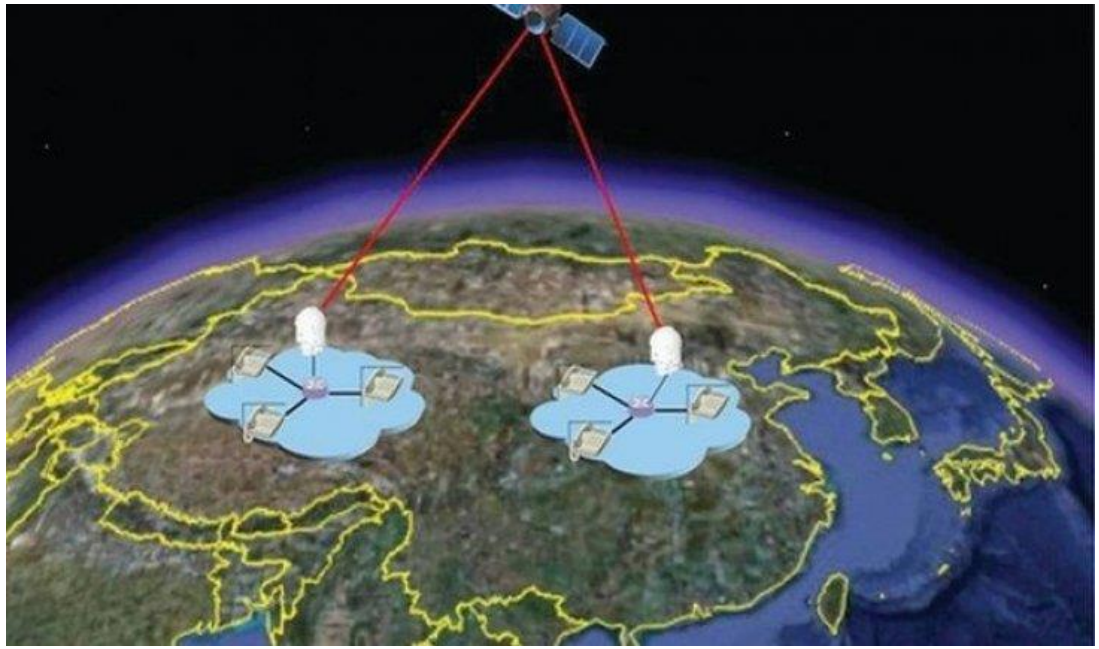
Rete in fibra ottica messa a punto dalla Rep. Popolare Cinese (massima lunghezza di tratta: 421 km)





Quantum Key Distribution

Esperimenti con satelliti artificiali LEO (sistema Micius)



LEO: Low Earth Orbit satellite

Quantum Key Distribution

Anche qui ci possono essere problemi: nell'attraversamento dell'atmosfera si possono avere rotazioni indesiderate della polarizzazione

Aspetti commerciali e altri esperimenti

Ci sono attualmente 4 aziende che offrono sistemi commerciali di QKD:
ID Quantique (Ginevra, Svizzera),
MagiQ Technologies, Inc. (New York, Stati Uniti),
QuintessenceLabs (Australia),
SeQureNet (Parigi, Francia).

Esperimento italiano CNR-INO
(Istituto Nazionale di Ottica di Firenze)

Un sistema di **crittografia quantistica** non è in grado di sopperire da solo alle vulnerabilità dei sistemi attuali.
Perché resta sempre uno-a-uno. (crittografia simmetrica)

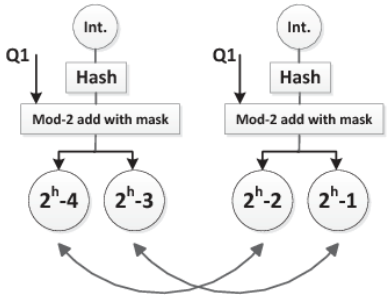
Crittografia **post-quantistica** (1/3)

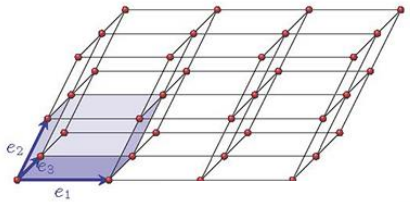
(cioè di tipo tradizionale, ma in grado di resistere ad attacchi effettuati mediante un computer quantistico)

Occorre impiegare algoritmi la cui forzatura richieda un tempo esponenziale, anche da parte di un calcolatore quantistico.

Possibili procedure:

- Funzioni Hash, che spezzettano il messaggio da proteggere;
- Vettori piccoli in grandi reticoli, metodo che richiede di trovare il vettore più corto;
- Soluzioni di equazioni quadratiche a molte variabili in campi finiti;
- **Passaggio attraverso un codice per la correzione di errori**.





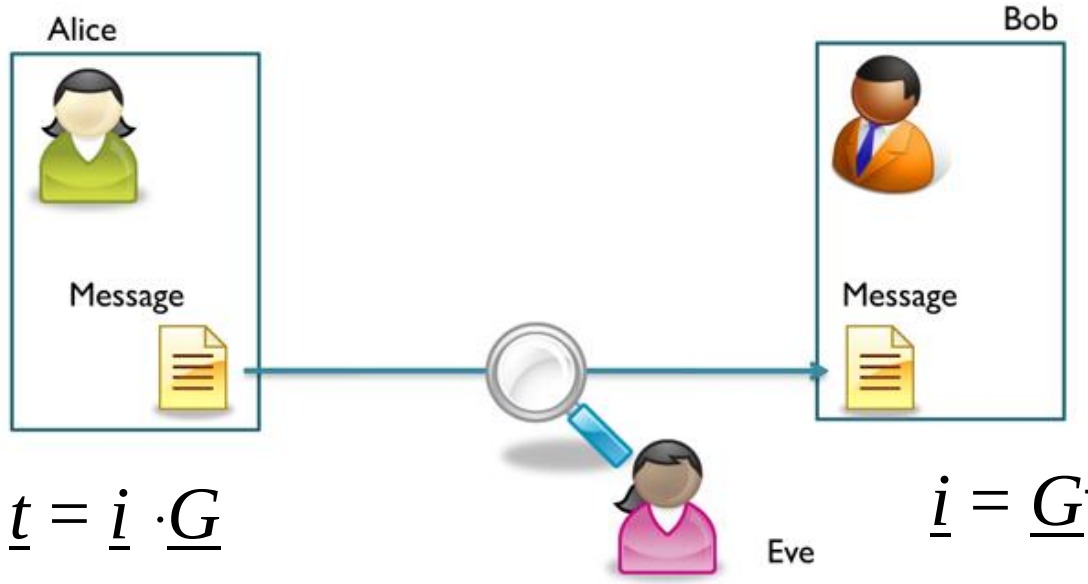
Quadratic Equations

- Babylon 2000 BCE – algorithm to solve system of the form $x + y = p$, $xy = q$ which is equivalent to the quadratic equation $x^2 + q = px$

Crittografia **post-quantistica** (2/3)

(cioè di tipo tradizionale, ma in grado di resistere ad attacchi effettuati mediante un computer quantistico)

Quantum-crypto based on channel coding



$\underline{t} = \underline{i} \cdot \underline{G}$

$\underline{i} = \underline{G}^{-1} \cdot \underline{t}$

0 X 1 0 0 1 0 1 X 0 1 X 0 0 1 0 1 1 0 1 0 0 1 1 X 0 1 1 1 0

Crittografia **post-quantistica** (3/3)

(cioè di tipo tradizionale, ma in grado di resistere ad attacchi effettuati mediante un computer quantistico)

Lavoro degli Enti di standardizzazione

Posizione del **NIST**
(National Institute of Standards and Technologies):
"It is necessary to protect sensitive electronic information from the threat of **quantum computers**, which one day could render many of our current encryption methods obsolete."
https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals

Tutti i sistemi proposti hanno il difetto di impiegare chiavi pubbliche molto lunghe.

Crittografia **post-quantistica**

con la tecnica della codifica a correzione di errori

- Tecniche attualmente in fase di prova e standardizzazione sotto il coordinamento del **NIST**.
- **UnivPM** ha proposto sistemi post-quantistici per crittografia asimmetrica e firma digitale.

US 20140105403A1

(19) **United States**

(12) **Patent Application Publication**

Baldi et al.

(10) **Pub. No.: US 2014/0105403 A1**

(43) **Pub. Date: Apr. 17, 2014**

(54) **METHOD AND APPARATUS FOR PUBLIC-KEY CRYPTOGRAPHY BASED ON ERROR CORRECTING CODES**

(75) Inventors: **Marco Baldi**, Macerata (MC) (IT); **Marco Bianchi**, Fanu (PU) (IT); **Franco Chiaraluce**, Osimo (AN) (IT); **Joachim Jakob Rosenthal**, Zollikon (CH); **Davide Mose' Schipani**, Zurich (CH)

(73) Assignee: **UNIVERSITAT ZURICH**, Zurich (CH)

(21) Appl. No.: **14/110,448**

(22) PCT Filed: **Apr. 2, 2012**

(86) PCT No.: **PCT/EP12/56005**

§ 371 (c)(1), (2), (4) Date: **Dec. 9, 2013**

(30) **Foreign Application Priority Data**

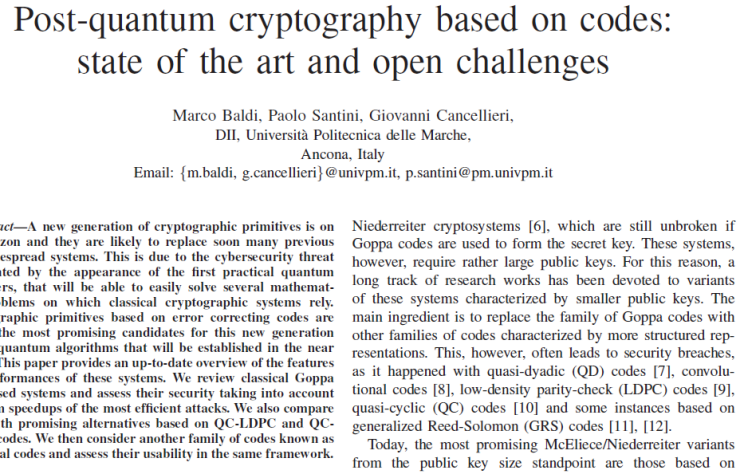
Apr. 9, 2011 (CH) 0635/11
Jul. 7, 2011 (CH) 1140/11

Publication Classification

(52) **U.S. Cl.**
CPC *H04L 9/0819* (2013.01)
USPC **380/282**

(57) **ABSTRACT**

Methods and apparatus for generating a private-public key pair, for encrypting a message for transmission through an unsecure communication medium (**30**), and for decrypting the message are disclosed. The methods are based on the well-known McEliece cryptosystem or on its Niederreiter variant. More general transformation matrices Q are used in place of permutation matrices, possibly together with an appropriate selection of the intentional error vectors. The transformation matrices Q are non-singular nxn matrices having the form $Q=R*T$, where the matrix R is a rank-z matrix and the matrix T is some other matrix rendering Q non-singular. The new Q matrices, though at least potentially being dense, have a limited propagation effect on the intentional error vectors for the authorized receiver. The use of this kind of matrices allows to better disguise the private key into the public one, without yielding any further error propagation effect. Based on this family of Q matrices, the presently proposed cryptosystem enables the use of different families



Post-quantum cryptography based on codes: state of the art and open challenges

Marco Baldi, Paolo Santini, Giovanni Cancellieri,
DII, Università Politecnica delle Marche,
Ancona, Italy
Email: {m.baldi, g.cancellieri}@univpm.it, p.santini@pm.univpm.it

***Abstract*—A new generation of cryptographic primitives is on the horizon and they are likely to replace soon many previous and widespread systems. This is due to the cybersecurity threat represented by the appearance of the first practical quantum computers, that will be able to easily solve several mathematical problems on which classical cryptographic systems rely. Cryptographic primitives based on error correcting codes are among the most promising candidates for this new generation of post-quantum algorithms that will be established in the near future. This paper provides an up-to-date overview of the features and performances of these systems. We review classical Goppa code-based systems and assess their security taking into account quantum speedups of the most efficient attacks. We also compare them with promising alternatives based on QC-LDPC and QC-MDPC codes. We then consider another family of codes known as monomial codes and assess their usability in the same framework.**

Niederreiter cryptosystems [6], which are still unbroken if Goppa codes are used to form the secret key. These systems, however, require rather large public keys. For this reason, a long track of research works has been devoted to variants of these systems characterized by smaller public keys. The main ingredient is to replace the family of Goppa codes with other families of codes characterized by more structured representations. This, however, often leads to security breaches, as it happened with quasi-dyadic (QD) codes [7], convolutional codes [8], low-density parity-check (LDPC) codes [9], quasi-cyclic (QC) codes [10] and some instances based on generalized Reed-Solomon (GRS) codes [11], [12].

Today, the most promising McEliece/Niederreiter variants from the public key size standpoint are those based on