

Post Quantum Cryptography

a.a. 2017/18

Alfredo De Santis

Dipartimento di Informatica
Università di Salerno

ads@unisa.it

<http://www.dia.unisa.it/professori/ads>



Dicembre 2017

Sommario

- Introduzione
- Algoritmi di Shor e di Groover
- Sperimentazioni
- Quantum Computer
- Proposte esistenti
- Standardizzazione del NIST
- Quantum Cryptography

Post Quantum Cryptography

- Algoritmi crittografici che resistono ad attacchi su un computer quantistico
- Con un computer quantistico si risolvono (in teoria) efficientemente:
 - Fattorizzazione
 - Logaritmo discreto
 - Logaritmo discreto su curve ellittiche
- Computer quantistici potrebbero essere costruiti nel breve
- Alcuni sistemi crittografici saranno a rischio

Se i computer quantistici fossero realtà

- Crittografia a chiave pubblica

- RSA, ECC

- Firma digitale

- RSA, DSS, ECDSA

- Accordo su chiave

- Diffie-Hellman

non più sicuri



- Cifrari simmetrici

- Funzioni hash

necessarie chiavi più lunghe
necessario output più lungo

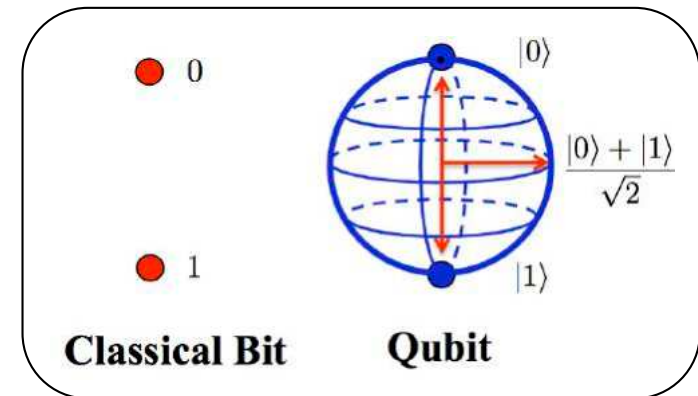
Quantum Computing

- Quantum bits "qubit"

- Superposition

 - Possono essere in più stati allo stesso tempo

- Potenzialmente possono accrescere la potenza computazionale oltre il limite classico

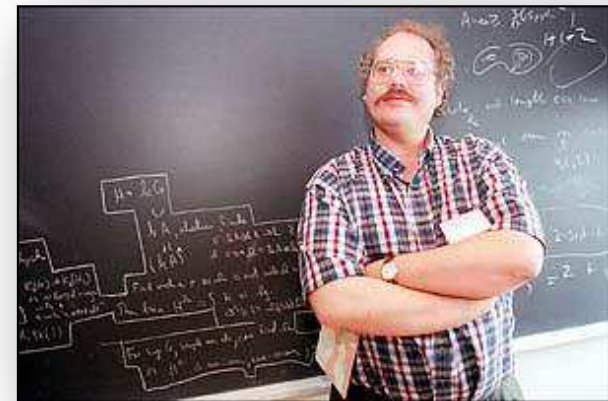


Algoritmo di Shor

Fattorizzare n usando

- $O((\log n)^2(\log \log n)(\log \log \log n))$ operazioni su
- un computer quantistico di grandezza $(\log n)^{1+o(1)}$

Peter Shor, Algorithms for Quantum Computation:
Discrete Logarithm and Factoring, 1994



Algoritmo di Shor

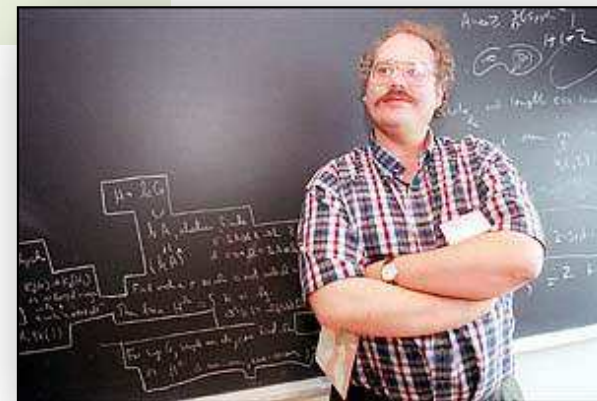
Fattorizzare n usando

- $O((\log n)^2(\log \log n)(\log \log \log n))$ operazioni su
- un computer quantistico di grandezza $(\log n)^{1+o(1)}$

Algoritmo di Shor per fattorizzare

- Parte classica che riduce il problema della fattorizzazione a quello di trovare l'ordine di un elemento
- Parte quantistica che calcola l'ordine di un elemento

Peter Shor, Algorithms for Quantum Computation:
Discrete Logarithm and Factoring, 1994



Algoritmo di Shor

Fattorizza (n)

Scegli a caso a

if $\gcd(a,n) = 1$ then "trovato fattore di n"

Calcola ordine di a: più piccolo r tale che $a^r = 1 \pmod n$

if r è pari e $a^{r/2} \not\equiv -1 \pmod n$

then $\gcd(a^{r/2}+1,n)$ e $\gcd(a^{r/2}-1,n)$ sono fattori di n

uso di un
algoritmo
quantistico

Algoritmo di Shor

Infatti:

$$a^r = 1 \pmod{n}$$

$$(a^{r/2})^2 - 1 = 0 \pmod{n}$$

$$(a^{r/2} + 1)(a^{r/2} - 1) = 0 \pmod{n}$$

Algoritmo di Shor

Infatti:

$$a^r = 1 \pmod n$$

$$(a^{r/2})^2 - 1 = 0 \pmod n$$

$$(a^{r/2} + 1)(a^{r/2} - 1) = 0 \pmod n$$

non può essere
 $a^{r/2} + 1 = 0 \pmod n$
perché viene escluso dall'if

non può essere
 $a^{r/2} - 1 = 0 \pmod n$
perché r è l'ordine di a

Algoritmo di Shor

Infatti:

$$a^r = 1 \pmod n$$

$$(a^{r/2})^2 - 1 = 0 \pmod n$$

$$(a^{r/2} + 1)(a^{r/2} - 1) = 0 \pmod n$$

quindi

$$n \mid (a^{r/2} + 1)(a^{r/2} - 1)$$

$$n \nmid (a^{r/2} - 1)$$

$$n \nmid (a^{r/2} + 1)$$

non può essere
 $a^{r/2} + 1 = 0 \pmod n$
perché viene escluso dall'if

non può essere
 $a^{r/2} - 1 = 0 \pmod n$
perché r è l'ordine di a

Algoritmo di Shor

Infatti:

$$a^r = 1 \pmod n$$

$$(a^{r/2})^2 - 1 = 0 \pmod n$$

$$(a^{r/2} + 1)(a^{r/2} - 1) = 0 \pmod n$$

quindi

$$n \mid (a^{r/2} + 1)(a^{r/2} - 1)$$

$$n \nmid (a^{r/2} - 1)$$

$$n \nmid (a^{r/2} + 1)$$

Esempio:

$$n=15 \quad a=7 \quad r=4$$

$$7^4 = 1 \pmod{15}$$

$$(7^2+1)(7^2-1) = 0 \pmod{15}$$

$$\gcd(7^2+1, 15) = \gcd(49+1, 15) = 5$$

$$\gcd(7^2-1, 15) = \gcd(49-1, 15) = 3$$

Esempio:

$$n=143 \quad a=21 \quad r=4$$

$$21^4 = 1 \pmod{143}$$

$$(21^2+1)(21^2-1) = 0 \pmod{143}$$

$$\gcd(21^2+1, 143) = \gcd(441+1, 143) = 13$$

$$\gcd(21^2-1, 143) = \gcd(441-1, 143) = 11$$

Algoritmo di Shor per il logaritmo discreto

- Per calcolare k tale che $h = g^k \bmod p$
- Uso di un algoritmo quantistico per il calcolo dei periodi di $g^e h^f \bmod p$

Quantum Computing realizzazioni

- Difficile da realizzare
 - Interazioni non volute tra il sistema e l'ambiente esterno, che introducono errori
 - Difficile mantenere l'informazione nel tempo
 - Osservare particelle quantistiche cambia la misurazione

Algoritmo di Groover

- Ricerca in un insieme non ordinato di N elementi usando \sqrt{N} quantum query
- Ricerca esaustiva per known-plaintext attack
 - su AES-128 si riduce a 2^{64}
 - su AES-256 si riduce a 2^{128}
- Quindi, basterà usare AES-256

Grover, L. K., A fast quantum mechanical algorithm for database search.
Proc. 28th Ann. ACM Symp. on Theory of Computing, 212-219, 1996

Sommario

- Introduzione
- Algoritmi di Shor e di Groover
- **Sperimentazioni**
- Quantum Computer
- Proposte esistenti
- Standardizzazione del NIST
- Quantum Cryptography

Quantum Computing realizzazioni

- Prima realizzazione, gruppo da IBM, 2001
 - fattorizzazione di 15

Quantum Computing sperimentazioni

PHYSICAL REVIEW LETTERS

[Highlights](#) [Recent](#) [Accepted](#) [Collections](#) [Authors](#) [Referees](#) [Search](#) [Press](#) [About](#) 

Quantum Factorization of 143 on a Dipolar-Coupling Nuclear Magnetic Resonance System

Nanyang Xu, Jing Zhu, Dawei Lu, Xianyi Zhou, Xinhua Peng, and Jiangfeng Du

Phys. Rev. Lett. **108**, 130501 – Published 30 March 2012; Erratum [Phys. Rev. Lett.](#) **109**, 269902 (2012)

Quantum Computing sperimentazioni



Cornell University
Library

We

arXiv.org > quant-ph > arXiv:1411.6758

Search or Article

(Help | Advanced search)

Quantum Physics

Quantum factorization of 56153 with only 4 qubits

Nikesh S. Dattani (Kyoto University, Oxford University), Nathaniel Bryans (University of Calgary)

(Submitted on 25 Nov 2014 (v1), last revised 27 Nov 2014 (this version, v3))

The largest number factored on a quantum device reported until now was 143. That quantum computation, which used only 4 qubits at 300K, actually also factored much larger numbers such as 3599, 11663, and 56153, without the awareness of the authors of that work. Furthermore, unlike the implementations of Shor's algorithm performed thus far, these 4-qubit factorizations do not need to use prior knowledge of the answer. However, because they only use 4 qubits, these factorizations can also be performed trivially on classical computers. We discover a class of numbers for which the power of quantum information actually comes into play. We then demonstrate a 3-qubit factorization of 175, which would be the first quantum factorization of a triprime.

New largest number factored on a quantum device is 56,153

November 28, 2014 by Lisa Zyga [report](#)

Table 5: Quantum factorization records

Number	# of factors	# of qubits needed	Algorithm	Year implemented	Implemented without prior knowledge of solution
15	2	8	Shor	2001 [2]	×
	2	8	Shor	2007 [3]	×
	2	8	Shor	2007 [3]	×
	2	8	Shor	2009 [5]	×
	2	8	Shor	2012 [6]	×
21	2	10	Shor	2012 [7]	×
143	2	4	minimization	2012 [1]	✓
56153	2	4	minimization	2012 [1]	✓

Sommario

- Introduzione
- Algoritmi di Shor e di Groover
- Sperimentazioni
- Quantum Computer
- Proposte esistenti
- Standardizzazione del NIST
- Quantum Cryptography

Quantum Computer

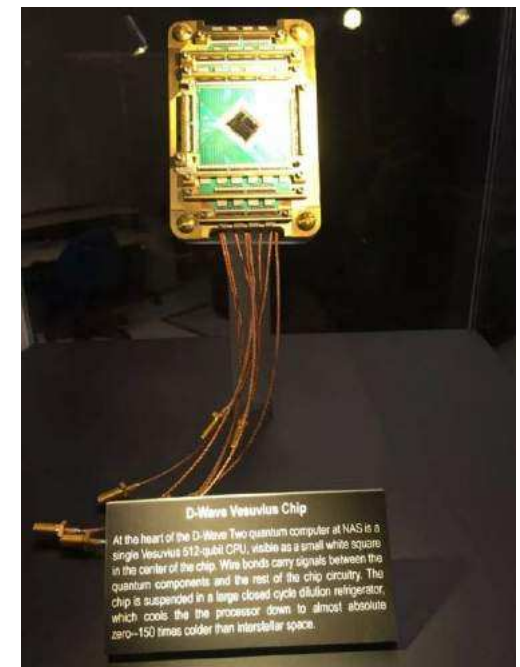


- D-Wave System, azienda canadese
- D-Wave One, 128-qubit, 10M\$, annunciato 11 maggio 2011
 - Primo computer quantistico commerciale



Quantum Computer

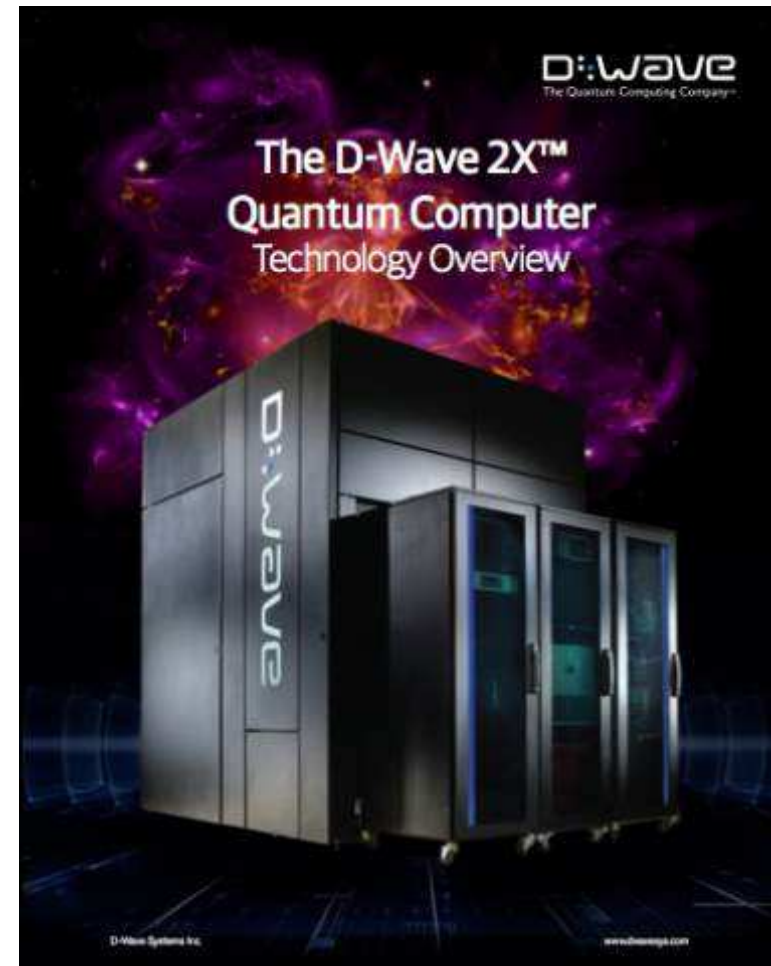
- D-Wave ha annunciato nel maggio 2013 che il Quantum Artificial Intelligence Center, NASA, collaborazione tra
 - NASA (National Aeronautics and Space Administration)
 - Google
 - Universities Space Research Associationha ordinato un
 - D-Wave Two, 512-qubit, 10M\$



D-Wave Vesuvius Chip
At the heart of the D-Wave Two quantum computer at NASA is a single Vesuvius 512-qubit CPU, visible as a small white square in the center of the chip. Wire bonds carry signals between the quantum components and the rest of the chip circuitry. The chip is suspended in a large closed cycle dilution refrigerator, which cools the processor down to almost absolute zero—150 times colder than interstellar space.

Quantum Computer

- D-Wave ha annunciato a settembre 2015
 - D-Wave 2X, 1.097-qubit, 15M\$



Quantum Computer

- D-Wave ha annunciato il 24 gennaio 2017
 - D-Wave 2000Q, 2000 qubits
 - primo acquirente: Temporal Defense Systems, un'azienda specializzata in cyber security



Perplexità sui computer quantistici costruiti

- D-Wave macchina single-purpose
- Non è più veloce di un computer tradizionale in diversi test sperimentati da ricercatori indipendenti
- Comunque è solo un primo passo nella realizzazione di computer quantistici

Defining and detecting quantum speedup, *Science*, 19 Jun 2014

NSA vuole costruire quantum computer

The Washington Post

National Security

NSA seeks to build quantum computer that could crack most types of encryption

By **Steven Rich** and **Barton Gellman** January 2, 2014 

In room-size metal boxes secure against electromagnetic leaks, the National Security Agency is racing to build a computer that could break nearly every kind of encryption used to protect banking, medical, business and government records around the world.

According to documents provided by former NSA contractor Edward Snowden, 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.

NSA vuole costruire quantum computer

Excerpts from the "black budget," Volume 2, "Combined Cryptologic Program":

(U) RESEARCH & TECHNOLOGY (U) PENETRATING HARD TARGETS

(U) Project Description

(S//SI//REL TO USA, FVEY) The Penetrating Hard Targets Project provides proof-of-concept technological solutions to {...} enable:

{...}

- (S//SI//REL TO USA, FVEY) Breaking strong encryption.

(TS//SI//REL TO USA, FVEY) This Project focuses on meeting those customer requirements that will directly impact the end-to-end SIGINT mission during the next decade and beyond. It provides advanced knowledge of technology trends and opportunities to steer IT products and standards in a SIGINT-friendly direction. This Project contains the Penetrating Hard Targets Sub-Project.

(U) Base resources in this project are used to:

{...}

- (S//SI//REL TO USA, FVEY) Conduct basic research in quantum physics and architecture/engineering studies to determine if, and how, a cryptologically useful quantum computer can be built.



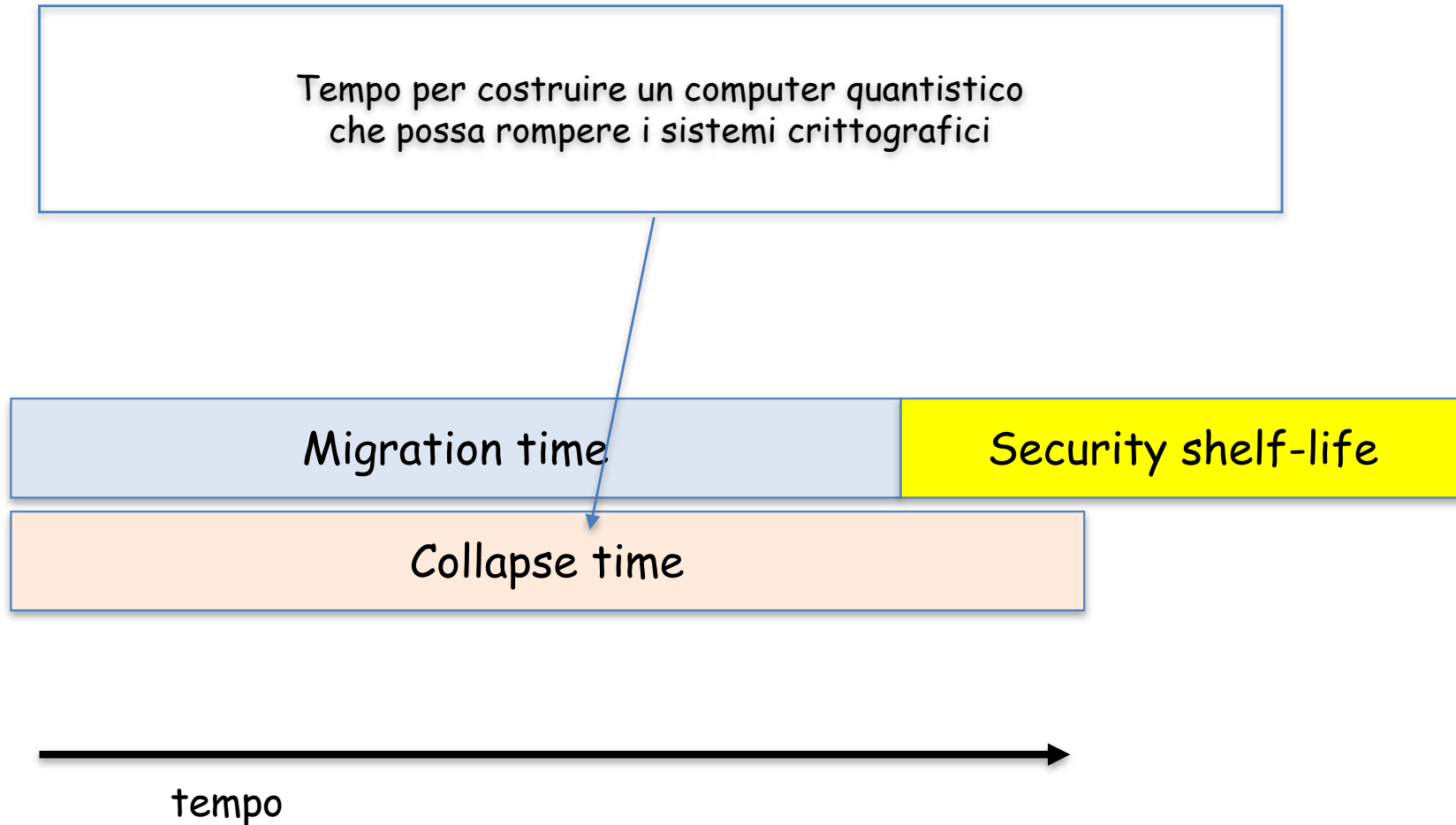
Uno scenario preoccupante

Tempo per sostituire gli algoritmi attuali

- 0 se dovessimo solo sostituire AES-128 con AES-256
- >15 anni se diversi attori devono concordare uno standard



Uno scenario preoccupante



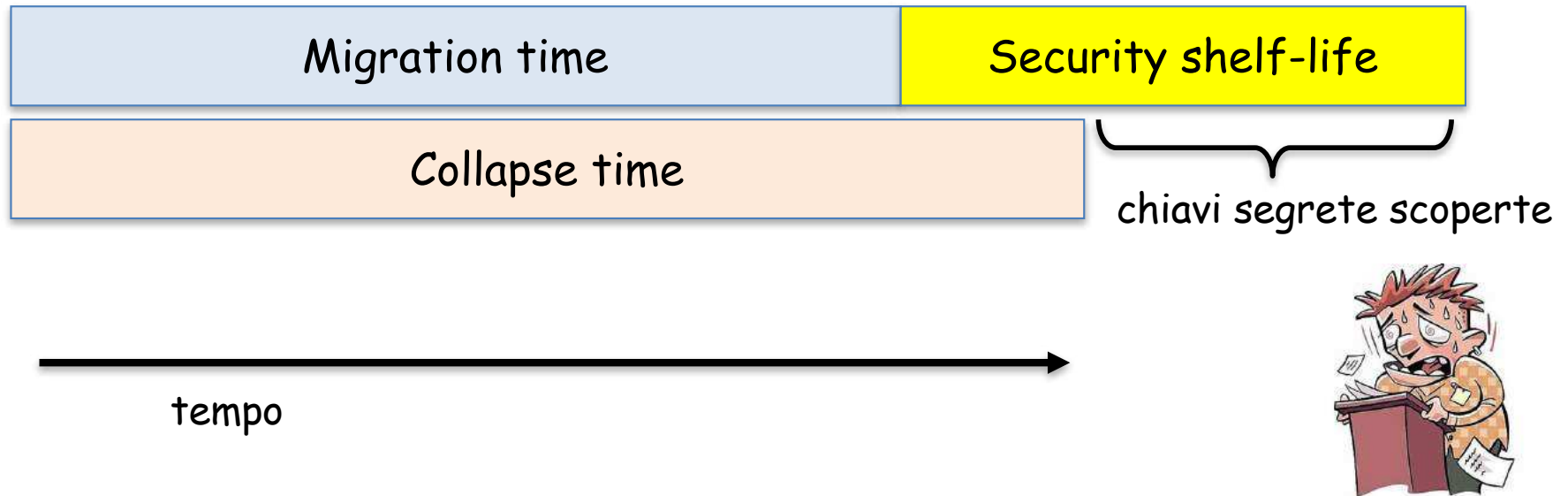
Uno scenario preoccupante

Quanto tempo devono rimanere sicure le chiavi. Per es.:

- 0 anni, per sicurezza real time
- 10 anni, personal health information
- 20 anni, trade secret
- 100 anni, informazioni sicurezza nazionale



Uno scenario preoccupante



Michele Mosca, University of Waterloo

Quando sarà costruito un quantum computer che possa fattorizzare?

"Rapid improvements in experimental quantum hardware suggest that a threshold for the design and the construction of fault-tolerant systems may be reached in the next five years"

"Quantum computing: An IBM perspective.",
IBM Journal of Research and Development 55, no. 5, paper 13, 2011

Quando sarà costruito un quantum computer che possa fattorizzare?

"There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a 1 in 2 chance of the same by 2031."

Dr. Michele Mosca, University of Waterloo, 2015



Quando sarà costruito un quantum computer che possa fattorizzare?

"There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a 1 in 2 chance of the same by 2031."

Dr. Michele Mosca, University of Waterloo, 2015

Diverse motivazioni, tra cui:

How many physical qubits will we need to break RSA-2048? This depends on a number of issues, including the efficiency of fault-tolerant error correcting codes, the physical error models and error rates of the physical quantum computer, optimizations in quantum factoring algorithms, and the efficiency of the synthesis of factoring algorithms into fault-tolerant gates. Current estimates range from tens of millions to a billion physical qubits.



Sommario

- Introduzione
- Algoritmi di Shor e di Groover
- Sperimentazioni
- Quantum Computer
- **Proposte esistenti**
- Standardizzazione del NIST
- Quantum Cryptography

Sperimentazioni di Google



Experimenting with Post-Quantum Cryptography

July 7, 2016

Posted by Matt Braithwaite, Software Engineer

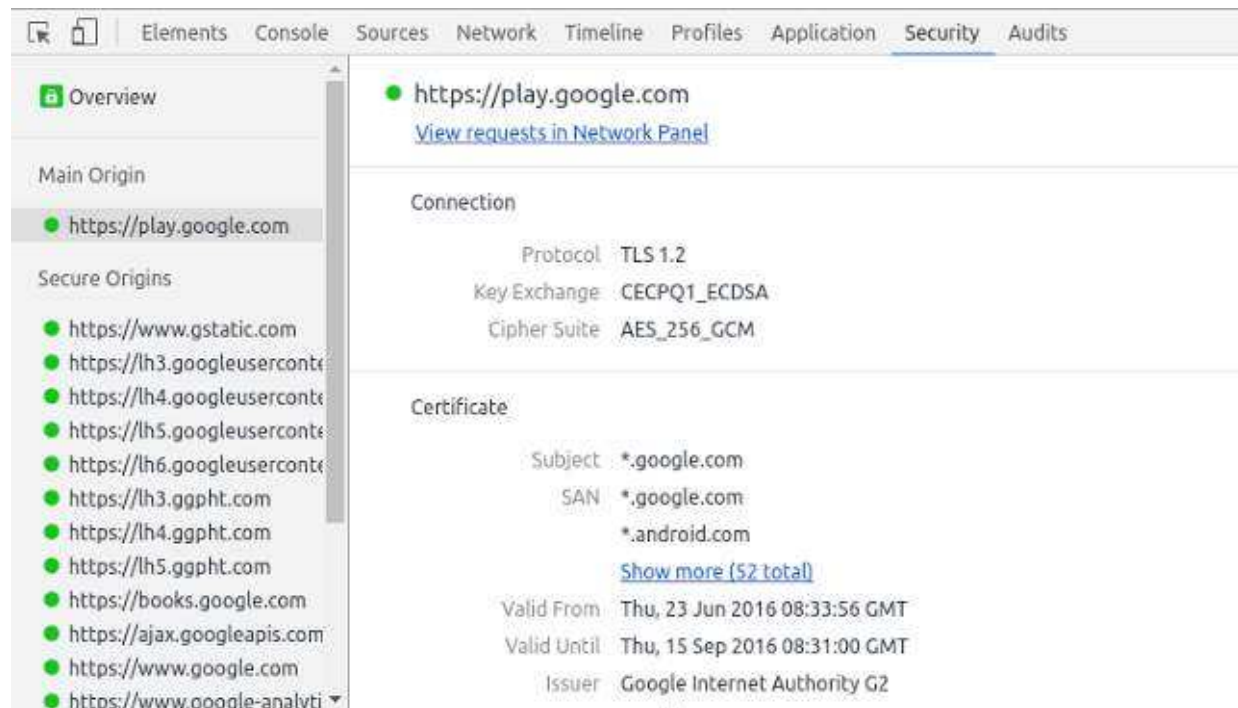
Quantum computers are a fundamentally different sort of computer that take advantage of aspects of quantum physics to solve certain sorts of problems dramatically faster than conventional computers can. While they will, no doubt, be of huge benefit in some areas of study, some of the problems that they are effective at solving are the ones that we use to secure digital communications. Specifically, if large quantum computers can be built then they may be able to break the asymmetric cryptographic primitives that are currently used in TLS, the security protocol behind HTTPS.

Sperimentazioni di Google

Algoritmo New Hope

E. Alkim, L. Ducas, T. Pöppelmann, P. Schwabe,

Post-quantum key exchange - a new hope, nov 2015



Proposte esistenti

- lattice-based cryptosystems,
 - code-based cryptosystems,
 - multivariate polynomial cryptosystems,
 - hash-based signatures,
 - altri
-
- Sono poco efficienti
 - Occorre ulteriore analisi della sicurezza, in particolare contro quantum computer

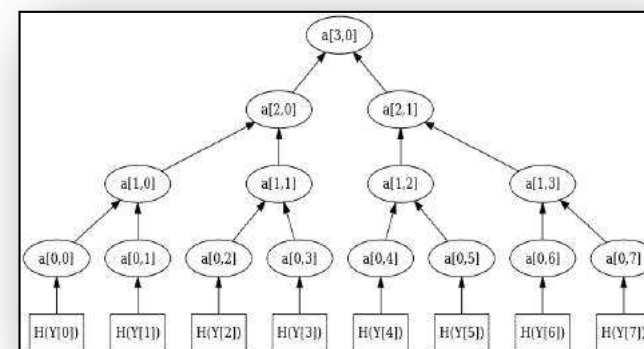


Code-based Cryptosystems

- Basata sulla difficoltà di decodificare un random linear code
- Sia cifratura che firma
- Schemi di cifratura includono:
 - McEliece (1978); Niederreiter (1986); e varianti
- Schema di Niederreiter è il più efficiente
- Chiavi pubbliche abbastanza grandi (65/192kBytes per 80/128-bit security)
- Vantaggi/Svantaggi
 - Sembra la più matura come PQ Crypto
 - Raramente usata in pratica per la grandezza della chiave pubblica

Hash-based Cryptosystems

- Schema di firma Lamport, 1979
 - Firma one-time (chiave privata può essere usata una sola volta)
 - Si basa su funzioni one-way, anche funzioni hash
 - Se una funzione hash risultasse insicura, basta sostituirla
- Schema di firma Merkle, XMSS (2011), SPHINCS (2015)
- Con alberi di hash, firme di più messaggi
- Vantaggi e svantaggi
 - Schemi più promettenti
 - Chiave pubblica/privata piccola
 - Uso limitato della chiave pubblica



Chiavi schema Lamport

firma singolo bit

chiave privata
 (x_0, x_1)



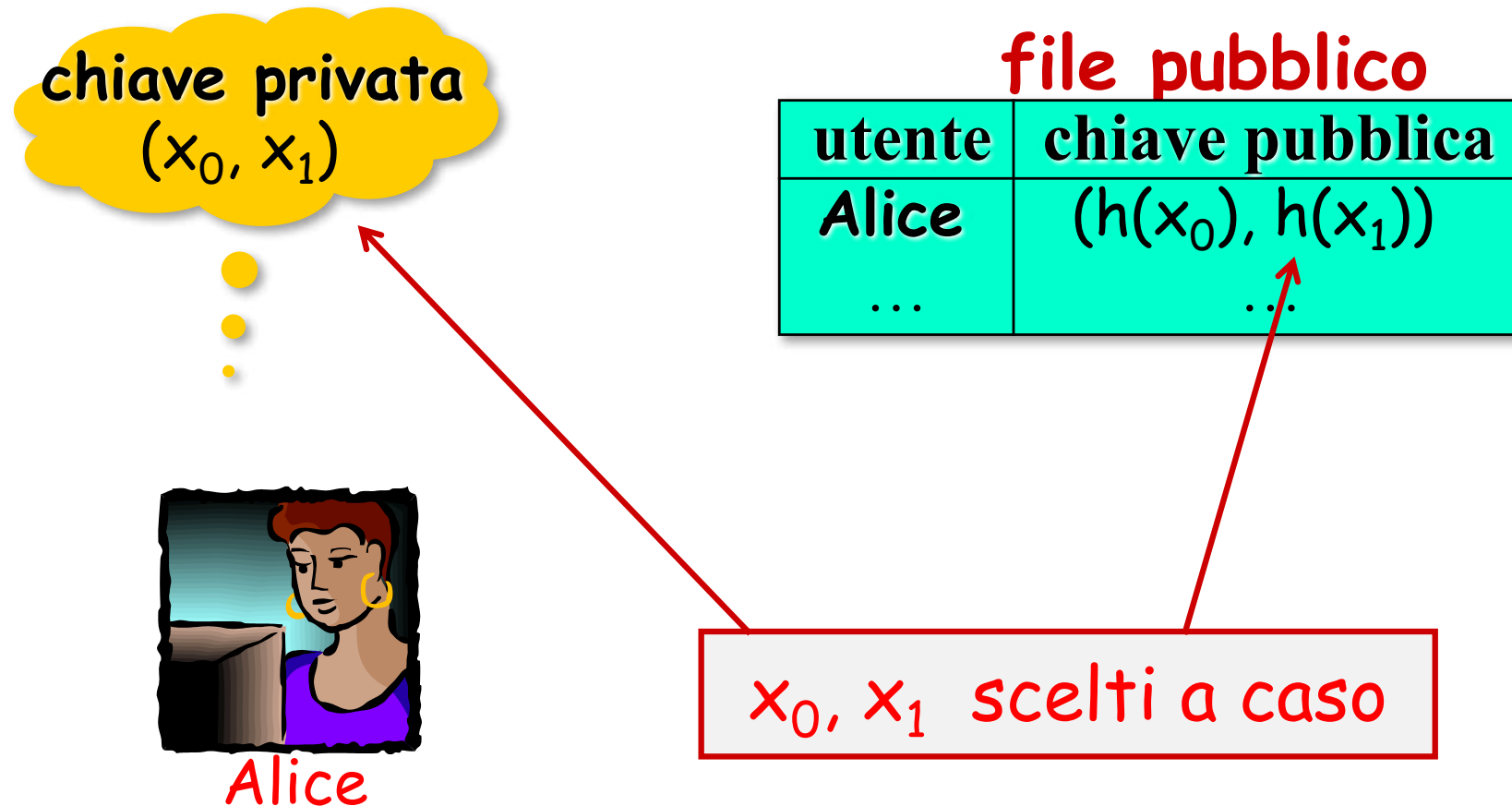
Alice

file pubblico

utente	chiave pubblica
Alice	$(h(x_0), h(x_1))$
...	...

Chiavi schema Lamport

firma singolo bit



Schema Lamport

firma singolo bit

chiave privata
 (x_0, x_1)

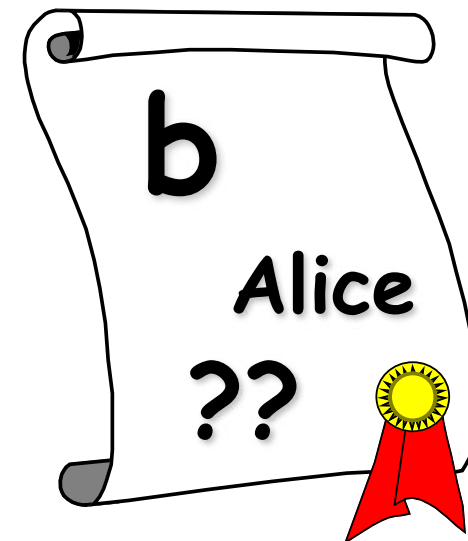
file pubblico

utente	chiave pubblica
Alice	$(h(x_0), h(x_1))$
...	...



Alice

Devo firmare b



Schema Lamport

firma singolo bit

chiave privata
 (x_0, x_1)

file pubblico

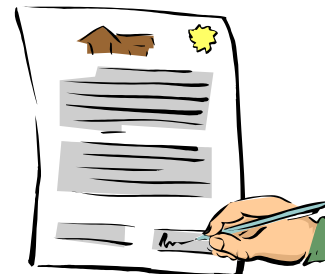
utente	chiave pubblica
Alice	$(h(x_0), h(x_1))$
...	...



Alice

Firma di b

$$F \leftarrow x_b$$

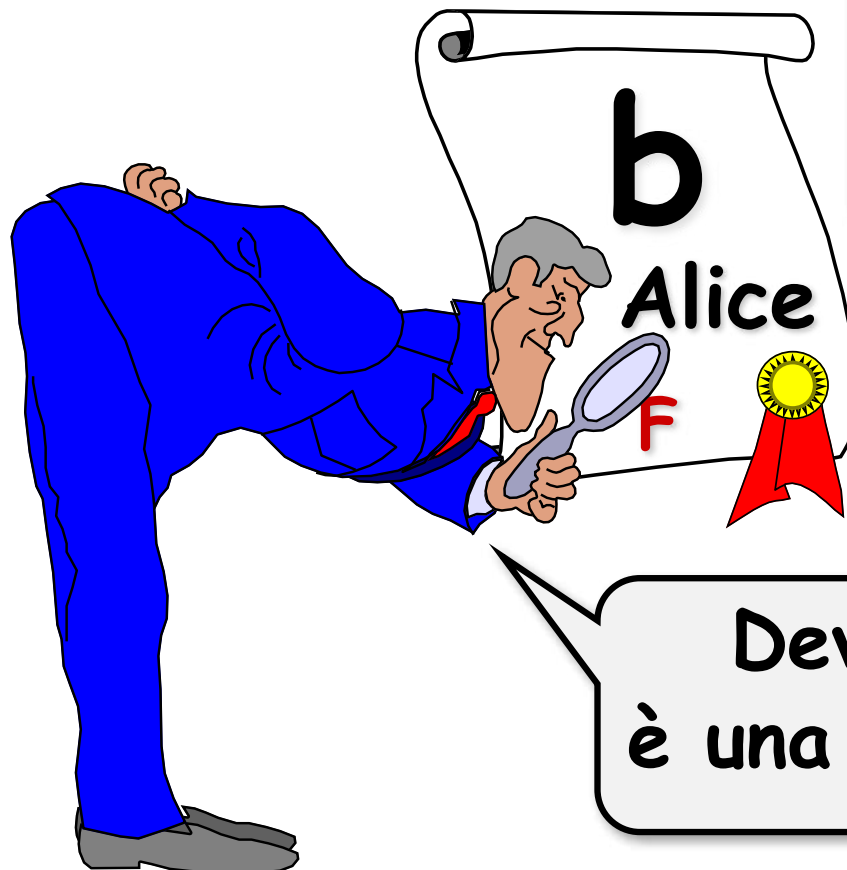


Schema Lamport

firma singolo bit

file pubblico

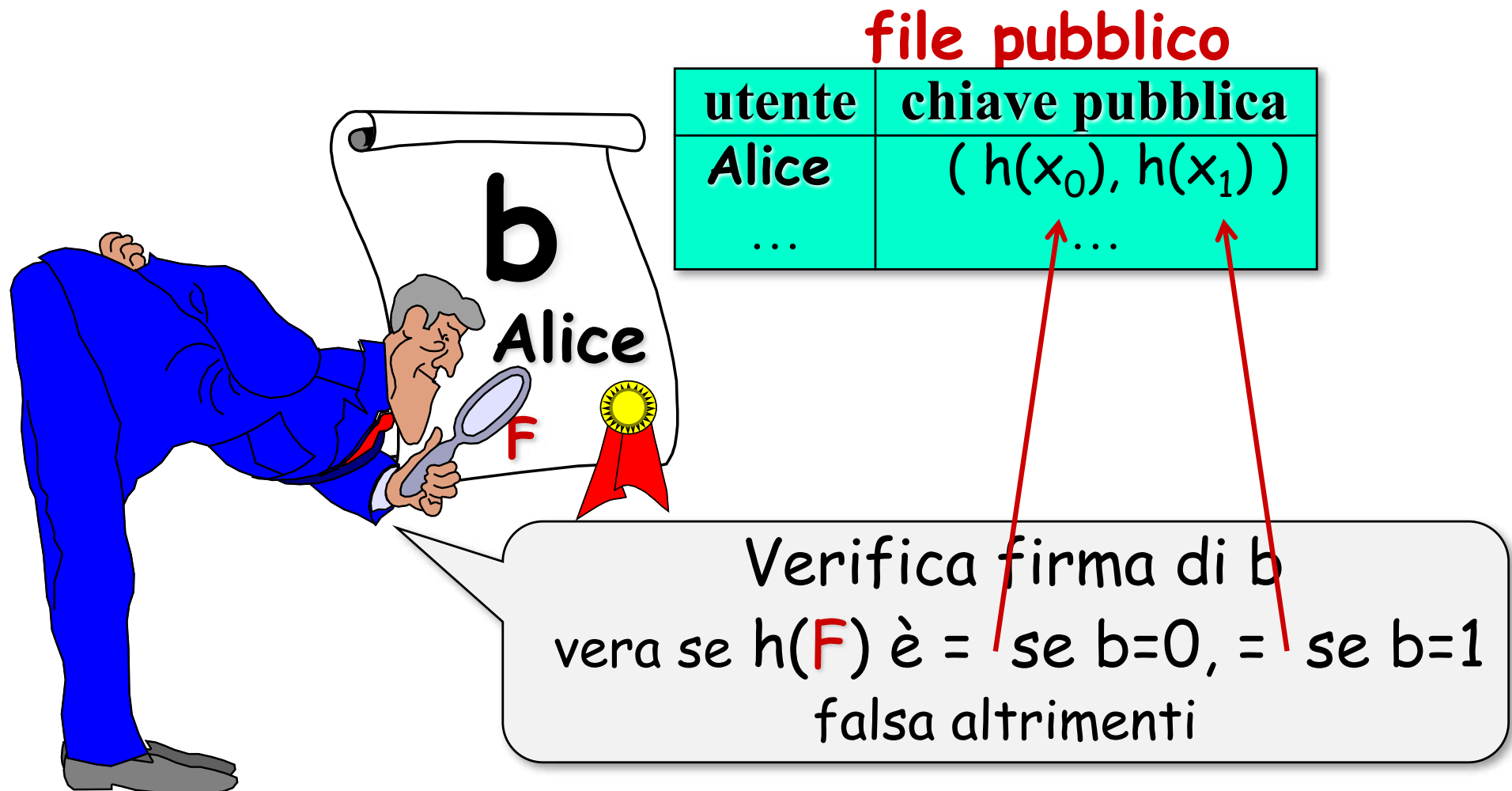
utente	chiave pubblica
Alice	$(h(x_0), h(x_1))$
...	...



Devo verificare se **F**
è una firma di Alice per **b**

Schema Lamport

firma singolo bit



Schema Lamport

firma messaggio

file pubblico

utente	chiave pubblica
Alice	$(h(x_{1,0}), h(x_{1,1})), \dots, (h(x_{n,0}), h(x_{n,1}))$
	$\dots \quad \dots$

Firma di $M = m_1, \dots, m_n$

$\mathbf{F} \leftarrow (x_{1,m_1}, \dots, x_{n,m_n})$

Schema Lamport

firma messaggio

file pubblico

utente	chiave pubblica
Alice	$(h(x_{1,0}), h(x_{1,1}), \dots, h(x_{256,0}), h(x_{256,1}))$...

Firma di $M = 1 \dots 0$

$\mathbf{F} \leftarrow (x_{1,1}, \dots, x_{256,0})$

Schema Lamport

lunghezze chiavi

Firma messaggio ed hash di 256 bit

- Chiave pubblica $(h(x_{1,0}), h(x_{1,1}), \dots, (h(x_{256,0}), h(x_{256,1}))$

Lunghezza $2 \cdot 256 \cdot 256 = 131.072$ bit

- Chiave privata $(x_{1,0}, x_{1,1}), \dots, (x_{256,0}, x_{256,1})$

Lunghezza $2 \cdot 256 \cdot 256 = 131.072$ bit

- Firma $x_{1,m_1}, \dots, x_{256,m_{256}}$

Lunghezza $256 \cdot 256 = 65.536$ bit

Schema Lamport

lunghezze chiavi

Firma messaggio ed hash di 256 bit

- Chiave pubblica $(h(x_{1,0}), h(x_{1,1}), \dots, (h(x_{256,0}), h(x_{256,1}))$

Lunghezza $2 \cdot 256 \cdot 256 = 131.072$ bit

256 bit

- Chiave privata $(x_{1,0}, x_{1,1}), \dots, (x_{256,0}, x_{256,1})$

Lunghezza $2 \cdot 256 \cdot 256 = 131.072$ bit

256 bit

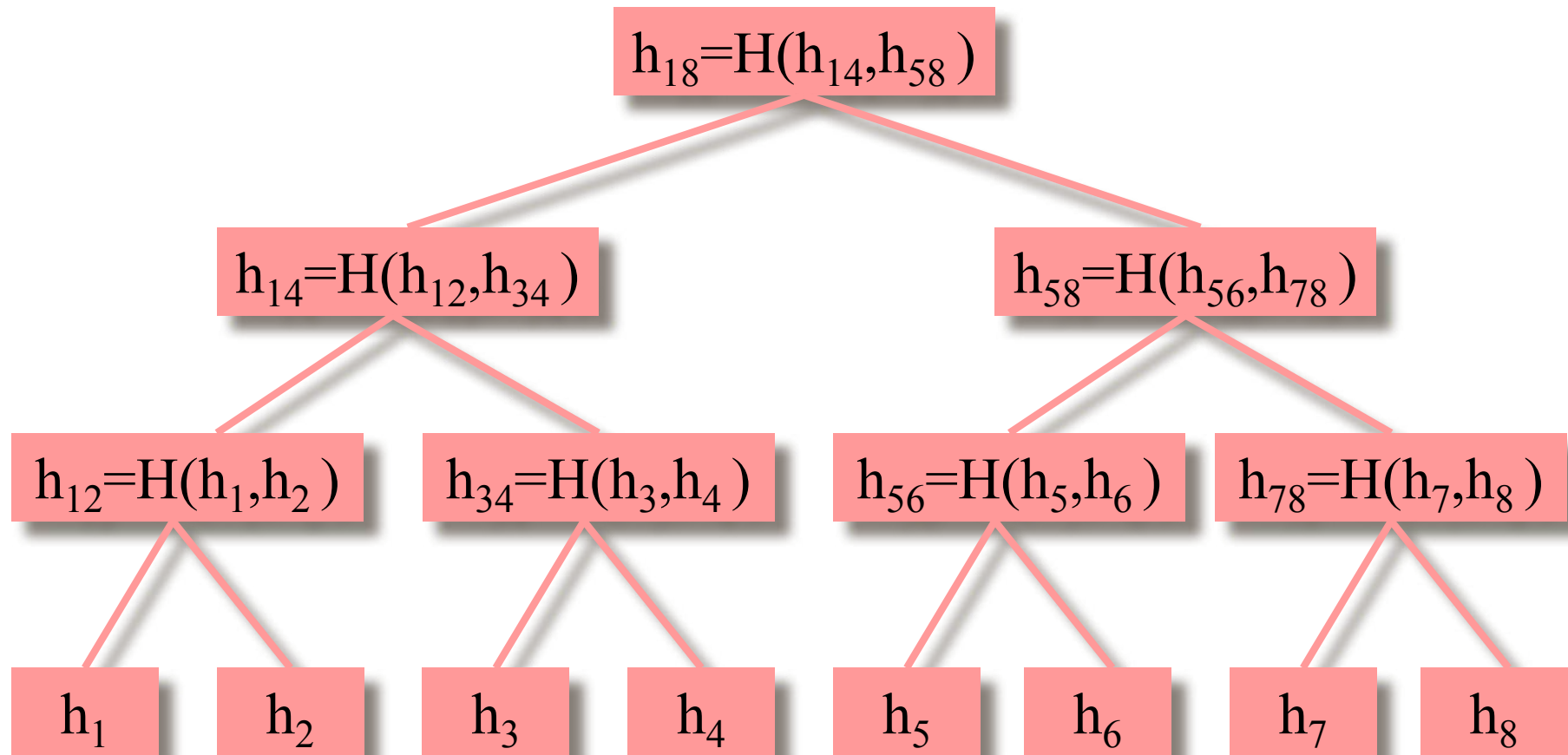
- Firma $x_{1,m_1}, \dots, x_{256,m_{256}}$

Lunghezza $256 \cdot 256 = 65.536$ bit

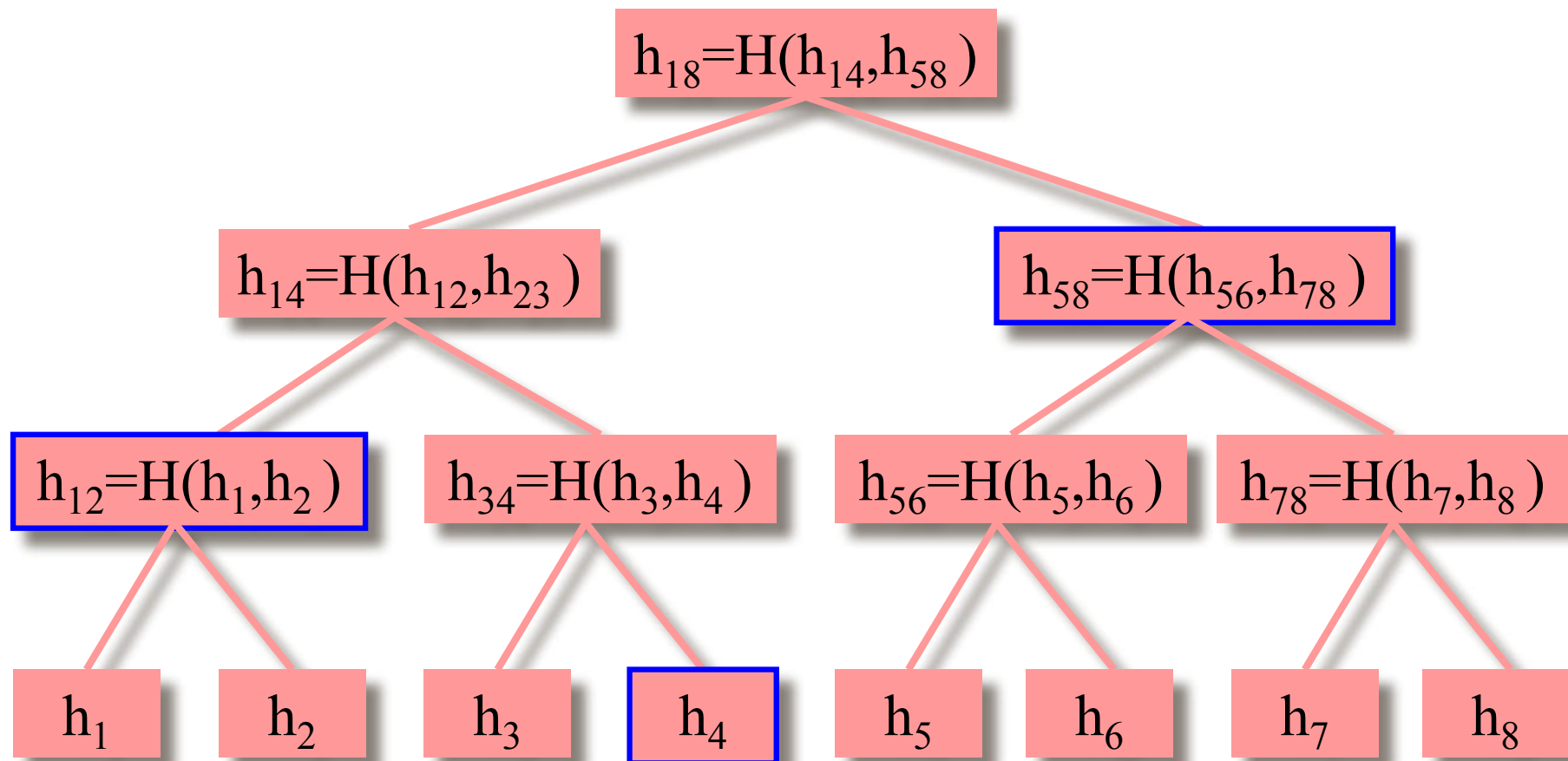
Riduzione lunghezza chiave pubblica e privata

- Alberi di hash (Merkle tree)
- Generatore pseudocasuale

Costruzione albero di hash



Info per verifica di "h₃ in albero con radice h₁₈"



Sicurezza albero di hash

Fissato il valore hash della radice,
non è possibile

- inserire un nuovo valore nell'albero di hash
- cambiare anche un solo valore nell'albero di hash

...altrimenti si determinerebbe una collisione
per la funzione hash

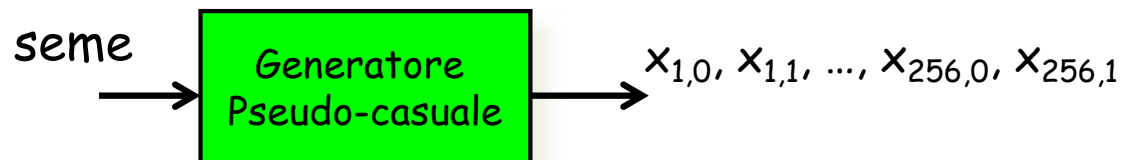
Schema Lamport

lunghezze chiave privata

Chiave privata $(x_{1,0}, x_{1,1}), \dots, (x_{256,0}, x_{256,1})$

Lunghezza $2 \cdot 256 \cdot 256 = 131.072$ bit

Generazione chiavi con generatore pseudocasuale

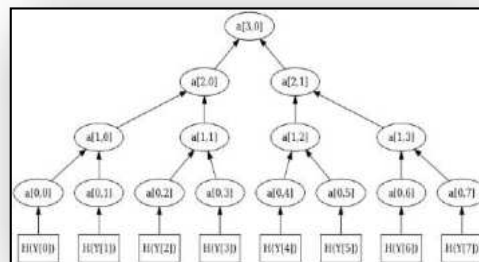


Schema Merkle

firme multiple, lunghezze

Supponiamo 2^{32} firme con messaggi ed hash di 256 bit

- Chiave pubblica
 - Hash radice di un albero di hash delle chiavi pubbliche
- Chiave privata
 - Seme per un generatore pseudocasuale
- Firma
 - $x_{1,m_1}, \dots, x_{256,m_{256}}$
 - Chiave pubblica firma singolo messaggio
 - info verifica (authentication path)
 - indice



Schema Merkle

firme multiple, lunghezze

Supponiamo 2^{32} firme con messaggi ed hash di 256 bit

➤ Chiave pubblica

Hash radice di un albero di hash delle chiavi pubbliche **256 bit**

➤ Chiave privata

Seme per un generatore pseudocasuale **256 bit**

➤ Firma

➤ $x_{1,m_1}, \dots, x_{256,m_{256}}$

➤ Chiave pubblica firma singolo messaggio

➤ info verifica (authentication path)

➤ indice

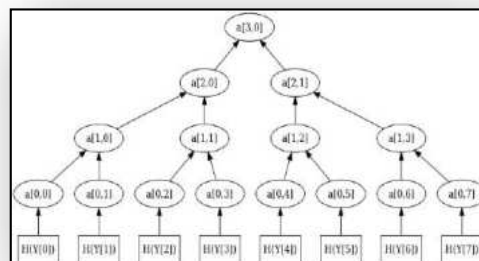
$256 \times 256 = 65.536$ bit

$2 \times 256 \times 256 = 131.072$ bit

$32 \times 256 = 8.192$ bit

32 bit

Totale 204.832 bit



Schema Merkle pratico?

- Firme lunghe
- Numero totale firme fissato
- Bisogna ricordare lo stato
 - i.e., fare update chiave privata dopo ogni firma
 - Non è compatibile con
 - Backup
 - Chiavi condivise tra device
 - Immagini macchine virtuali

Hash-based Signature

SPHINCS

- Stateless Practical Hash-based Incredibly Nice Collision-resilient Signatures, 2015
- Chiave pubblica 1 KByte, Chiave privata 1 Kbyte, Firma 41 KByte, Sicurezza 2^{128}
- <http://sphincs.cr.yp.to>

XMSS

- eXtended Merkle Signature Scheme, 2011
- <http://www.pqsignatures.org/index.html>

XMSSTM

- Estensione con Multi-Tree, 2013

McEliece Cryptosystem

- Uso di un codice lineare a correzione di errori
- Alla parola codice corrispondente al messaggio vengono aggiunti degli errori casuali
- La decodifica permette di trovare il messaggio in chiaro
- Decodificare un codice lineare è NP-hard
- Bisogna nascondere una trapdoor nel codice lineare da decodificare

McEliece, Robert J., A Public-Key Cryptosystem based on Algebraic Coding Theory.
Deep Space Network Progress Report 42-44
http://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF (1978)

Chiavi McEliece Cryptosystem

chiave privata

"info che permette
di decodificare"



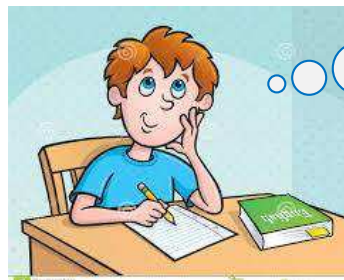
Alice

file pubblico

utente	chiave pubblica
Alice	G'
...	...

matrice $k \times n$

G' è la matrice
generatrice di un codice
lineare che corregge t
errori



Cifratura McEliece Cryptosystem

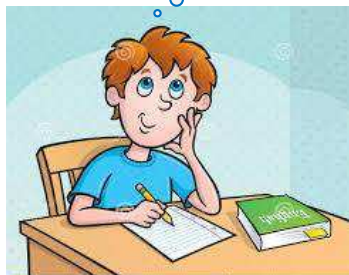
chiave privata

"info che permette
di decodificare"



Alice

e ha t "1"



file pubblico

utente	chiave pubblica
Alice	G'
...	...

canale insicuro

C



Bob

Cifratura di M per Alice

$$C \leftarrow MG' + e$$

Cifratura McEliece Cryptosystem

chiave privata

"info che permette
di decodificare"



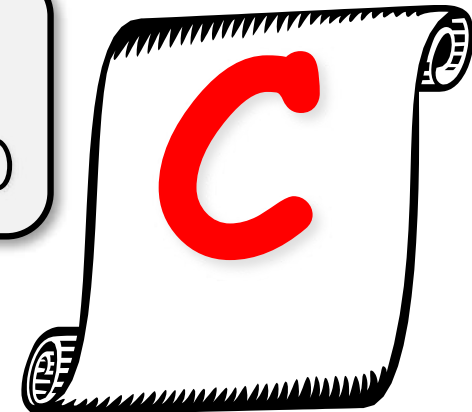
Alice

file pubblico

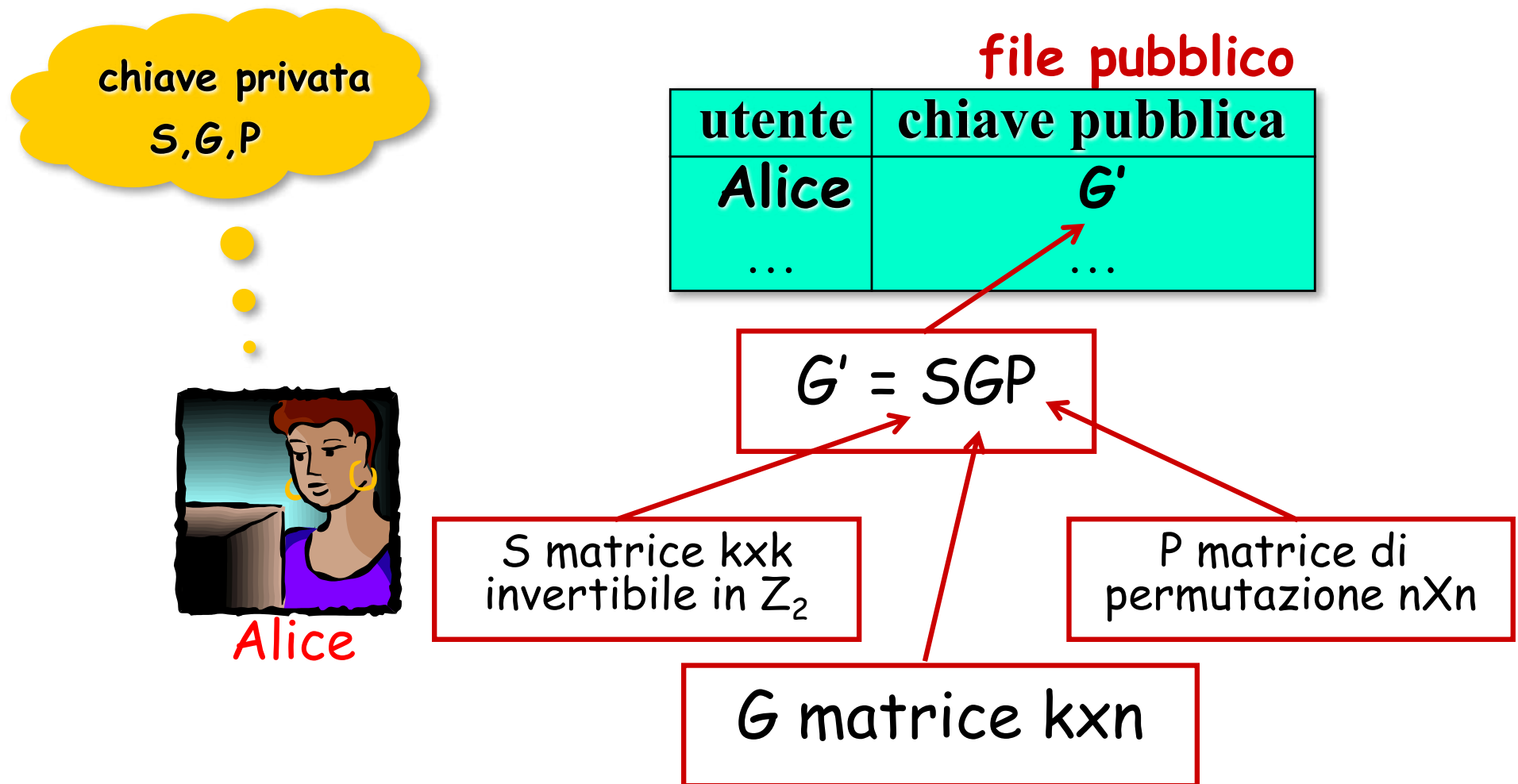
utente	chiave pubblica
Alice	G'
...	...

Decifratura di C

$M \leftarrow \text{decodifica}(C, \text{chiave privata})$



Chiavi McEliece Cryptosystem



Decifrazione di $C = MG' + e$

Chiave pubblica $G' = SGP$

Chiave privata S, G, P

- 1) Computa $C_1 = CP^{-1}$
- 2) Decodifica C_1 ed ottieni M_1
- 3) Computa $M = M_1S^{-1}$

Decifrazione di $C = MG' + e$

Chiave pubblica $G' = SGP$

Chiave privata S, G, P

1) Computa $C_1 = CP^{-1}$

$$\begin{aligned} C_1 &= CP^{-1} \\ &= MSGPP^{-1} + eP^{-1} \\ &= MSG + eP^{-1} \end{aligned}$$

2) Decodifica C_1 ed ottieni M_1

$$M_1 = MS$$

3) Computa $M = M_1S^{-1}$

eP^{-1} ha peso t

Codici Goppa binari

$$n = 2^m$$

$$k = n - mt$$

distanza tra parole codice $d = 2t + 1$

Facili da decodificare

N. J. Patterson (1975). "The algebraic decoding of Goppa codes".
IEEE Transactions on Information Theory. IT-21: 203-207.

Scelta dei valori

McEliece (1978) suggerisce $m=10$ e $t=50$ quindi:

$$n = 2^m = 1.024$$

$$k = n - mt = 524$$

Chiave pubblica: matrice 524×1.024

Testo in chiaro 524 bit

Testo cifrato 1.024 bit

Scelta dei valori

Bernstein (2010) suggerisce $m=12$ e $t=45$ quindi:

$$n = 2^m = 4.096$$

$$k = n - mt = 3.556$$

Chiave pubblica: matrice 3.556×4.096

Testo in chiaro 3.556 bit

Testo cifrato 4.096 bit

Bernstein, Daniel J. (2010). *Grover vs. McEliece*.

Post-quantum cryptography 2010. Lecture Notes in Computer Science **6061**. pp. 73-80.

Scelta dei valori

Per una sicurezza 2^{128} *post-quantum* si suggerisce $t=119$ e

$n = 6.960$

$k = 5.413$

Chiave pubblica: matrice 5.413×6.960

Testo in chiaro 5.413 bit

Testo cifrato 6.960 bit

Daniel Augot; et al., Initial recommendations of long-term secure post-quantum systems,
PQCRYPTO: Post-Quantum Cryptography for Long-Term Security. Sept. 2015

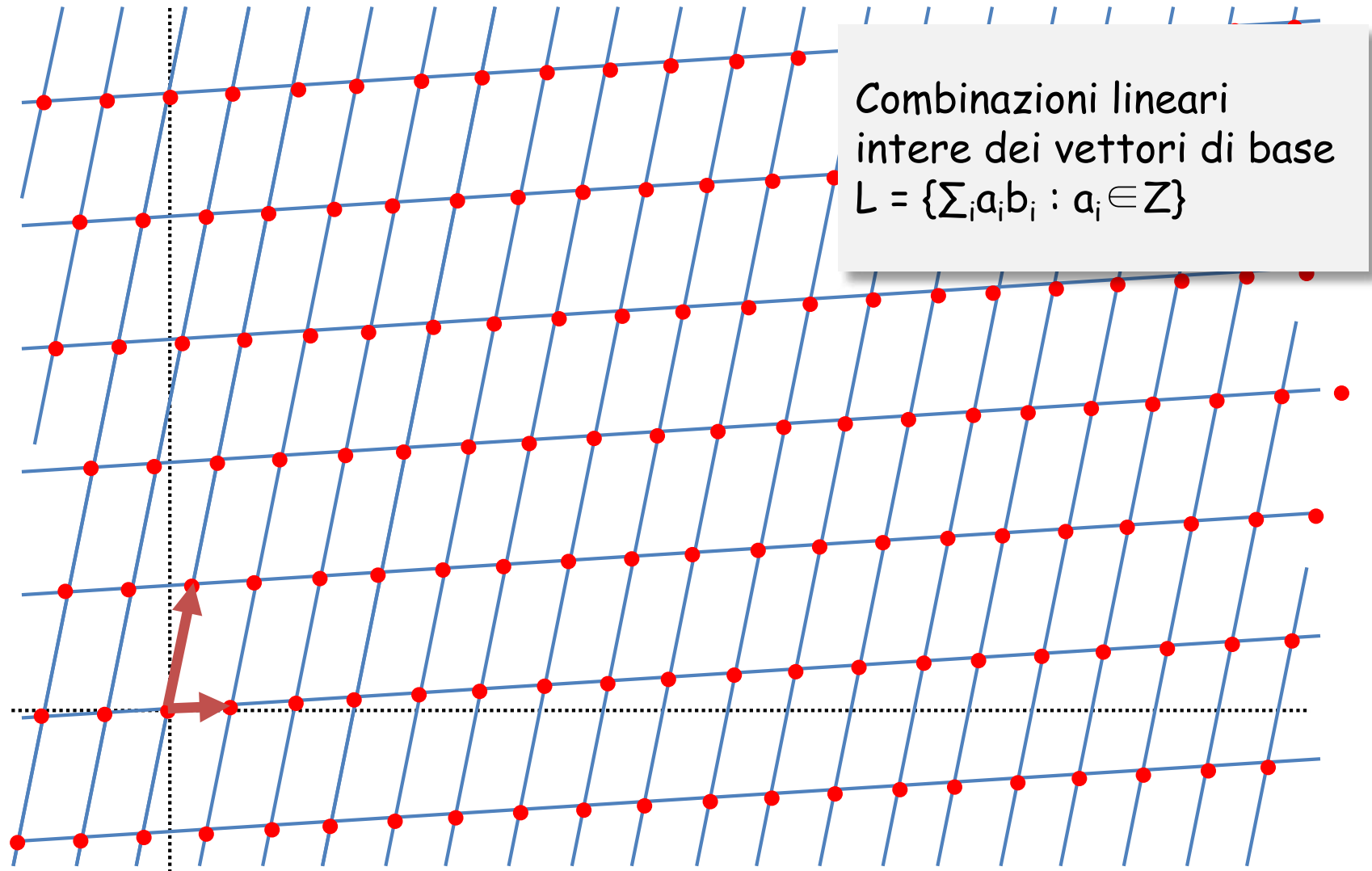
Multivariate Polynomial Cryptosystems

- Basati sulla difficoltà di risolvere un insieme di equazioni nonlineari Multivariate-Quadratic
- Esistono solo schemi di firma, ad es.:
Oil and Vinegar (1997); Rainbow (2005);
Quartz/HFE (1996); Matsumoto-Imai (1998)
- Grandi chiavi pubbliche / private (fino a 75kBytes)
- Vantaggi / Svantaggi
 - Operazioni implementabili efficientemente
 - Non adatto per device embedded per la grandezza delle chiavi

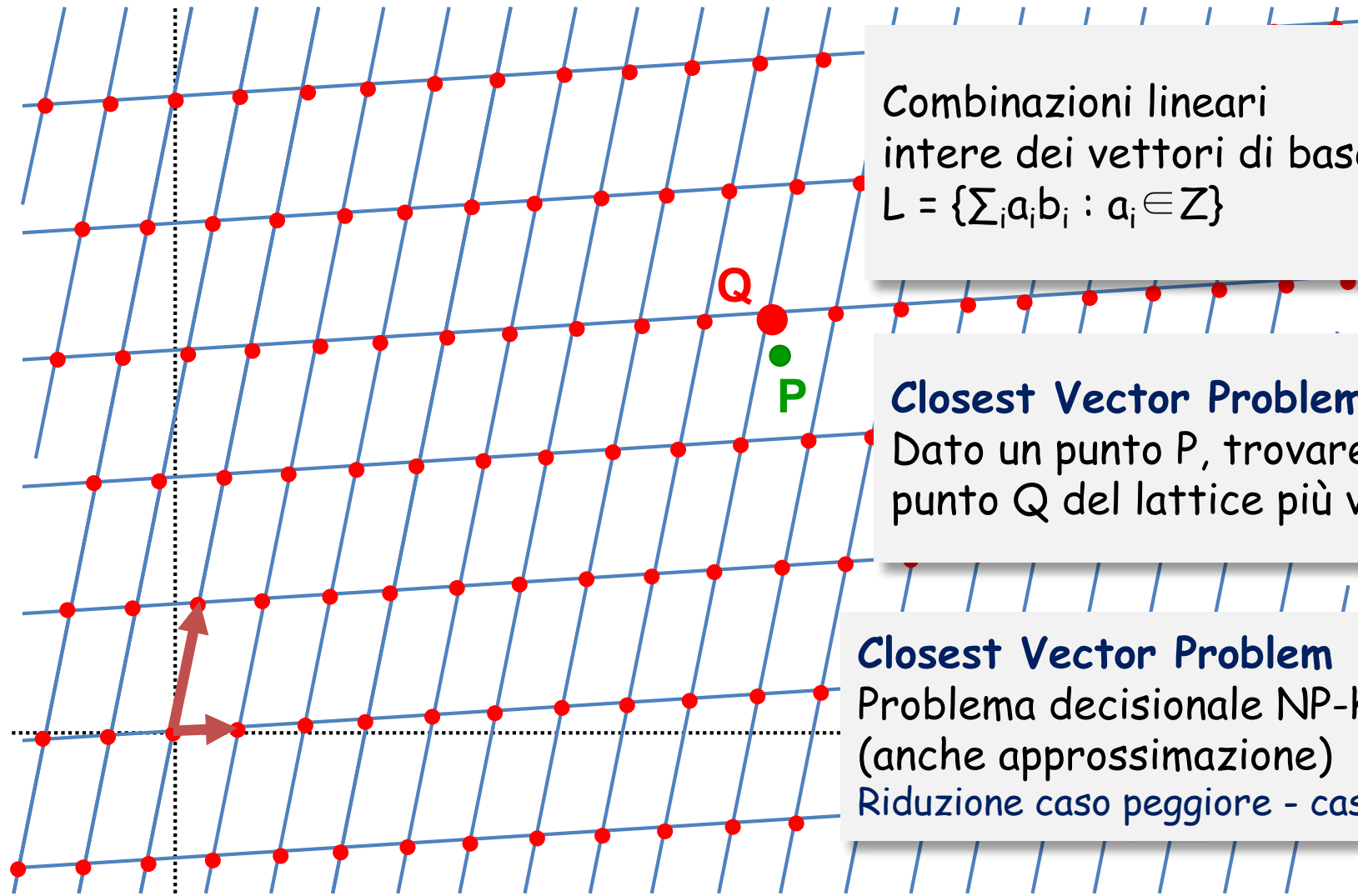
Crittosistemi Lattice-based

- Basati su shortest vector problem/closest vector problem

Lattice (reticolo)



Lattice (reticolo)



Combinazioni lineari
interne dei vettori di base
 $L = \{\sum_i a_i b_i : a_i \in \mathbb{Z}\}$

Closest Vector Problem

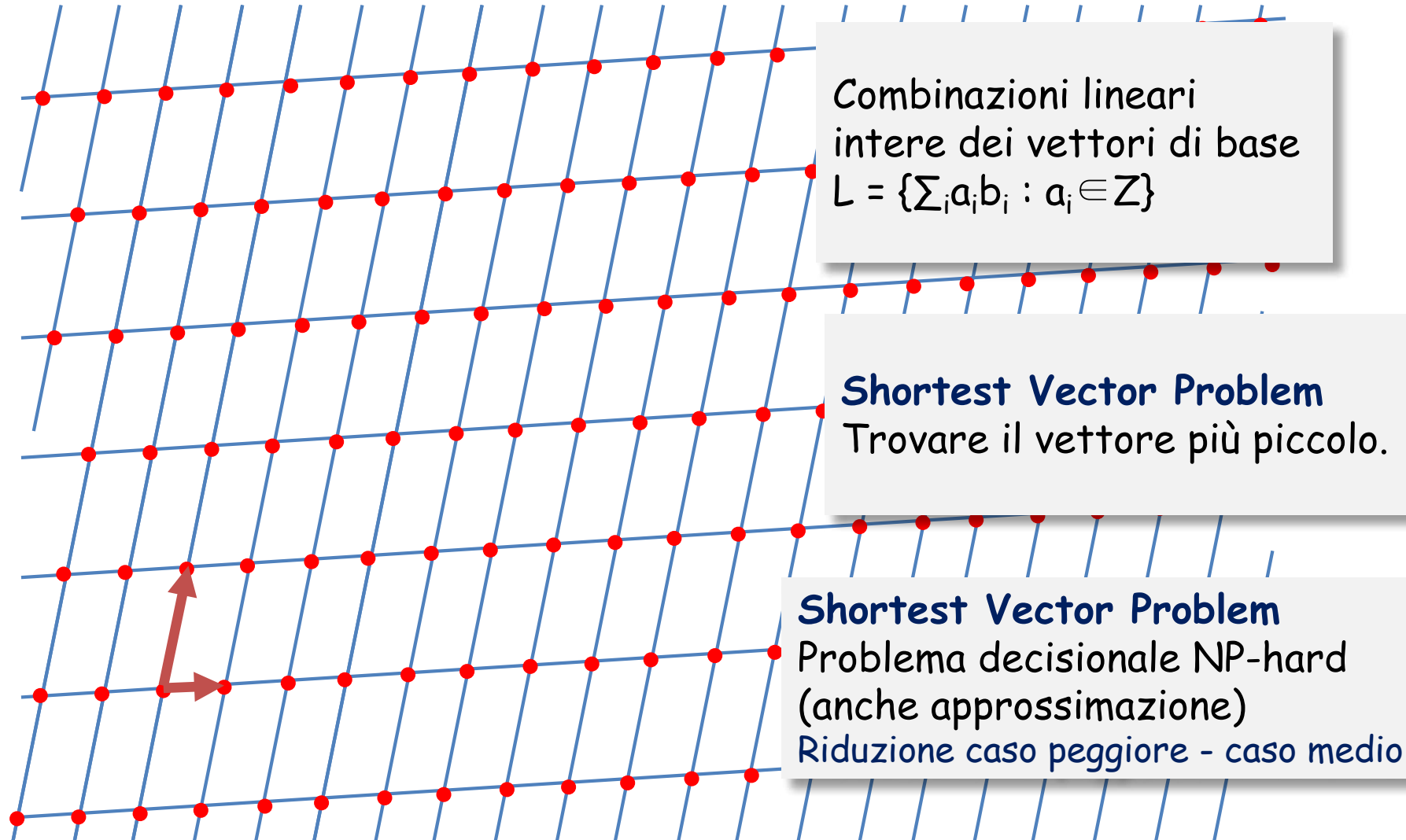
Dato un punto P , trovare il
punto Q del lattice più vicino.

Closest Vector Problem

Problema decisionale NP-hard
(anche approssimazione)

Riduzione caso peggiore - caso medio

Lattice (reticolo)



Crittosistemi Lattice-based

- Basati su shortest vector problem/closest vector problem
- Sia schemi di cifratura che di firma
Alcuni schemi di cifratura:
NTRU (1996); LWE (2005); R-LWE (2010);
- Grandi chiavi pubbliche / private (fino a 732kBytes)
- Vantaggi / Svantaggi
 - Operazioni implementabili efficientemente
 - Promettente
 - Possibili anche costruzioni per cifratura identity-based, cifratura omomorfica.

Sommario

- Introduzione
- Algoritmi di Shor e di Groover
- Sperimentazioni
- Quantum Computer
- Proposte esistenti
- Standardizzazione del NIST
- Quantum Cryptography

Necessità di uno standard ora

- Ci sono stati progressi recenti sia teorici che pratici per lo sviluppo di quantum computer
- La transizione tra algoritmi odierni e post quantistici
 - è lunga e
 - deve avvenire prima della costruzione di grandi quantum computer, senza esporre informazioni sensibili

Standardizzazione Post Quantum Cryptography



- Call for proposal, pubblicata 15 dicembre 2016
- Deadline invio proposte: 30 novembre 2017
- Workshop con presentazione delle proposte, First PQC Standardization Conference, co-located with PQCrypto 2018 - April 12-13, 2018
- Fase di analisi, con 1-2 workshop, 3-5 anni
- Draft standard, 2 anni dopo

<https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization>

Call for Proposal NIST



FEDERAL REGISTER

The Daily Journal of the United States Government

Notice

Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms

A Notice by the [National Institute of Standards and Technology](#) on 12/20/2016

PUBLISHED DOCUMENT

AGENCY:

National Institute of Standards and Technology (NIST), Commerce.

ACTION:

Notice and request for nominations for candidate post-quantum algorithms.

SUMMARY:

This notice solicits nominations from any interested party for candidate algorithms to be considered for public-key post-quantum standards. The submission requirements and the minimum acceptability requirements of a "complete and proper" candidate algorithm submission, as well as the evaluation criteria that will be used to appraise the candidate algorithms, can be found at <http://www.nist.gov/pqcrypto>.

DATES:

Proposals must be received by November 30, 2017. Further details are available at <http://www.nist.gov/pqcrypto>.

ADDRESSES:

Algorithm submission packages should be sent to Dr. Dustin Moody, Information Technology Laboratory, Attention: Post-Quantum Cryptographic

DOCUMENT DETAILS

Printed version:

[PDF](#)

Publication Date:

12/20/2016

Agencies:

[National Institute of Standards and Technology](#)

Dates:

Proposals must be received by November 30, 2017. Further details are available at <http://www.nist.gov/pqcrypto>.

Document Type:

Notice

Document Citation:

81 FR 92787

Page:

92787-92788 (2 pages)

Agency/Docket Number:

Docket No. 161116999-6999-02

Document Number:

2016-30615

DOCUMENT DETAILS

Proposte arrivate entro 30 novembre 2017

82 sottomissioni in totale

- 23 schemi di firma
- 59 schemi di cifratura / accordo su chiavi

	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



Proposte arrivate entro 30 novembre 2017

- BIG QUAKE
- BIKE
- CFPKM
- Classic McEliece
- Compact LWE
- CRYSTALS-DILITHIUM
- CRYSTALS-KYBER
- DAGS
- Ding Key Exchange
- DME
- DRS
- DualModeMS
- Edon-K
- EMBLEM and R.EMBLEM
- FALCON
- FrodoKEM
- GeMSS
- Giophantus
- Gravity-SPHINCS
- Guess Again
- Gui
- HILA5
- HiMQ-3
- HK17
- HQC
- KINDI
- LAC
- LAKE
- LEDAkem
- LEDApkc
- Lepton
- LIMA
- Lizard
- LOCKER
- LOTUS
- LUOV
- Mersenne-756839
- MQDSS
- NewHope
- NTRUEncrypt
- pqNTRUSign
- NTRU-HRSS-KEM
- NTRU Prime
- NTS-KEM
- Odd Manhattan
- OKCN/AKCN/CNKE
- Ouroboros-R
- Picnic
- Post-quantum RSA-Encryption
- Post-quantum RSA-Signature
- PqsigRM
- QC-MDPC KEM
- qTESLA
- RaCoSS
- Rainbow
- Ramstake
- RankSign
- RLCE-KEM
- Round2
- RQC
- RVB
- SABER
- SIKE
- SPHINCS+
- SRTPI
- Three Bears
- Titanium
- WalnutDSA

Standardizzazione

Post Quantum Cryptography

- Processo più complesso di AES o SHA-3
- Non c'è molta ricerca su algoritmi quantistici
- Probabilmente non ci sarà un "vincitore" ma diversi algoritmi come "good choice"
- Timeline può cambiare a seguito degli sviluppi nel campo

Sommario

- Introduzione
- Algoritmi di Shor e di Groover
- Sperimentazioni
- Quantum Computer
- Proposte esistenti
- Standardizzazione del NIST
- Quantum Cryptography

Post Quantum Cryptography e Quantum Cryptography

Non bisogna confondere:

- Post Quantum Cryptography
- Quantum Cryptography



Quantum Cryptography

- Uso della Meccanica Quantistica per realizzare primitive crittografiche
- Miglior esempio conosciuto: accordo di chiave
- Principio di indeterminazione di Heisenberg (1927)
 - per una particella non è possibile misurare un definito valore della posizione e della quantità di moto con precisione assoluta, ovvero con incertezza nulla
- Protocollo di Bennet e Brassard, 1984










Protocollo di Bennet e Brassard, 1984

- Alice e Bob usano un canale quantistico ed uno classico

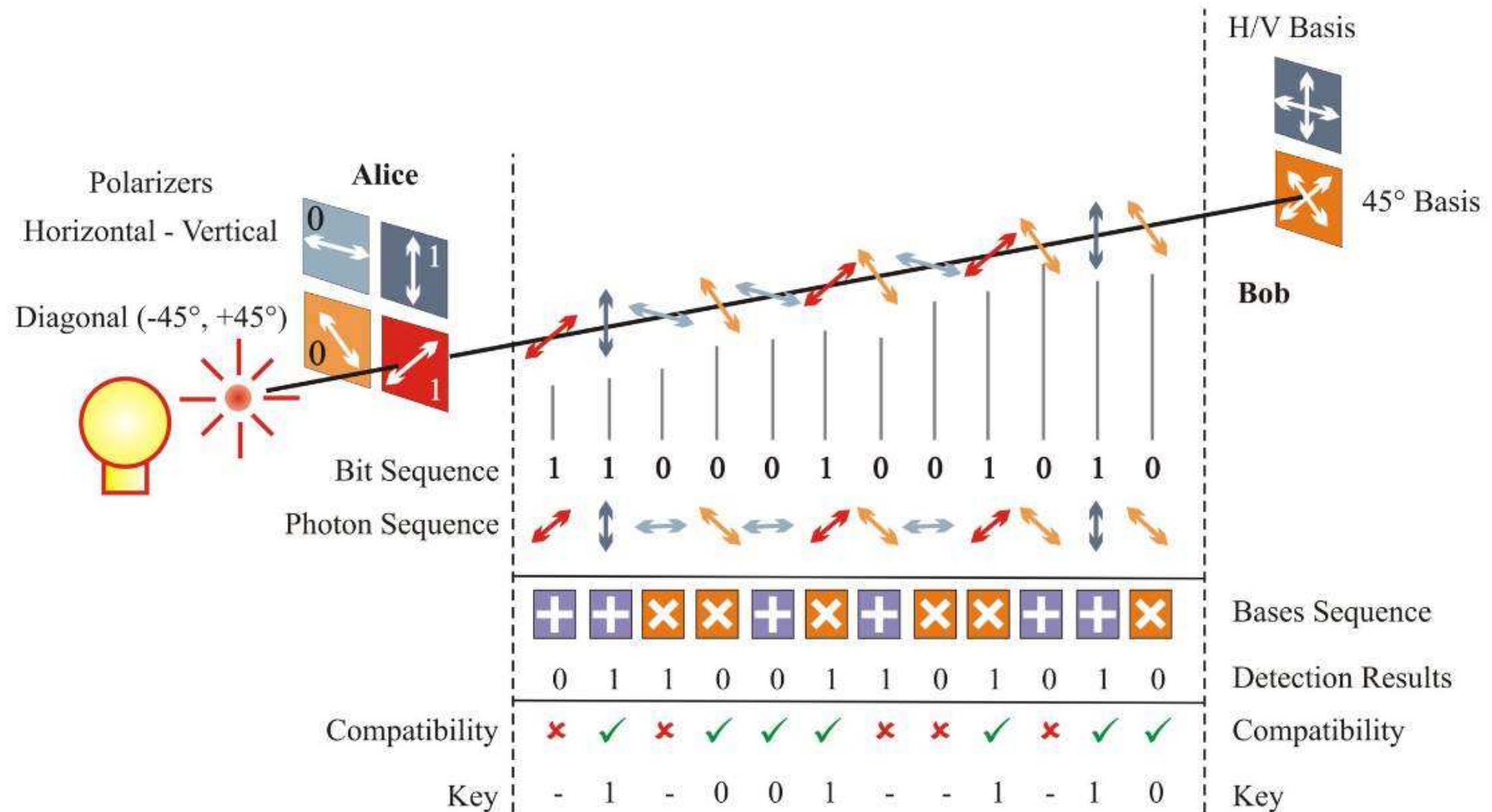


Protocollo di Bennet e Brassard, 1984

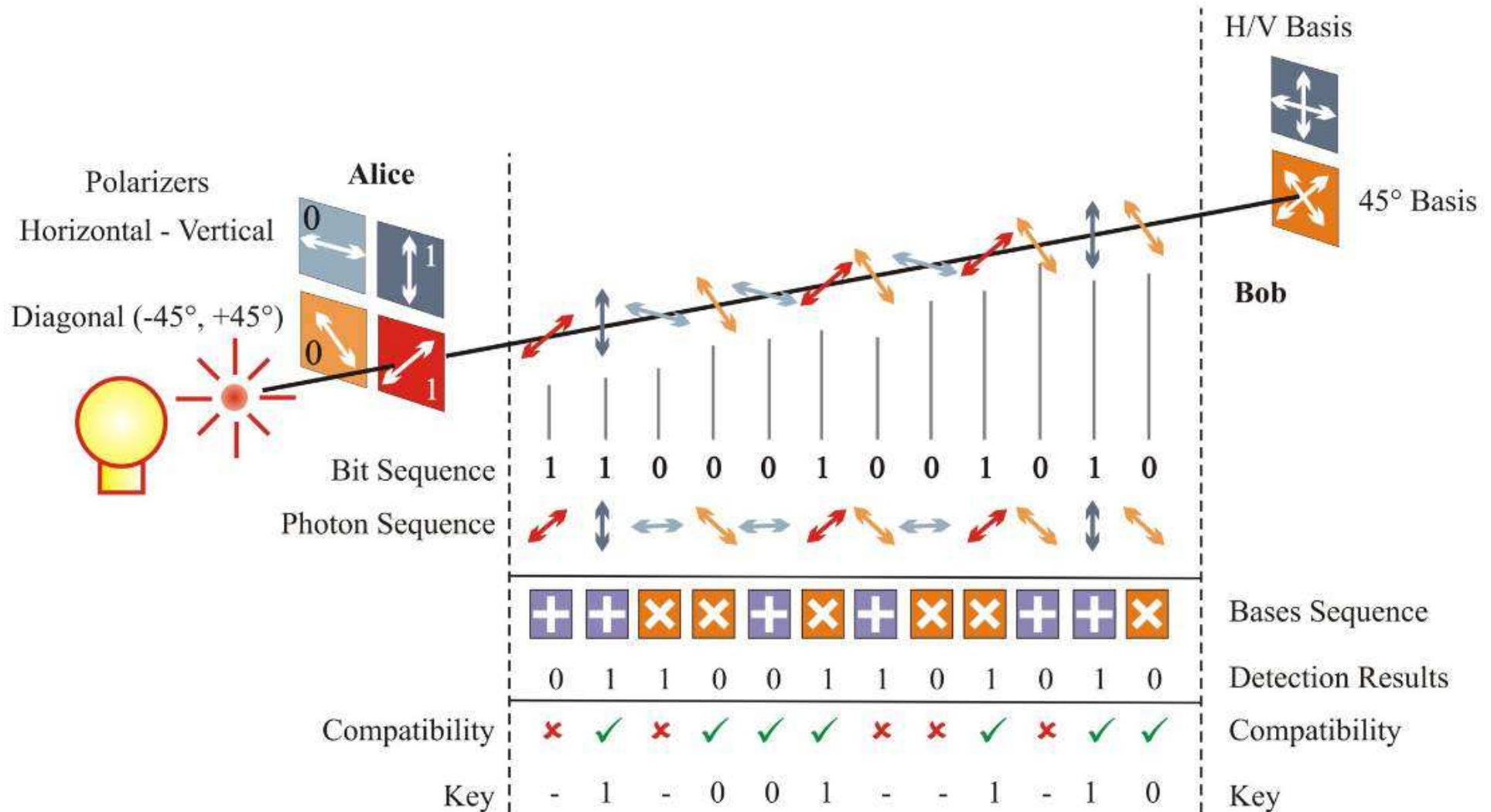
- Sul canale quantistico Alice invia fotoni con una determinata polarizzazione scelta a caso tra quattro possibili, 0° , 45° , 90° , 135°

- Le polarizzazioni determinano 2 basi non ortogonali tra loro
- Per ogni base, l'orientazione determina un bit
- Bob misura i fotoni in arrivo
 - Se sceglie la stessa base di Alice determina l'orientamento, quindi il bit
 - Se la base è diversa, ottiene un bit casuale
- Bob invia ad Alice le basi usate per le misure
- Alice invia a Bob le basi usate per le polarizzazioni
- Alice e Bob scartano le basi non compatibili
- Se un attaccante avesse effettuato delle misure avrebbe introdotto degli errori che vengono poi corretti

base	0	1
		
		

Quantum Cryptography



Quantum Cryptography



Svantaggi:

Costosa, richiede autenticazione, distanza limitata.

Domande?

