Università di Genova | DIMA DIPARTIMENTO DI MATEMATICA

Introduzione alla crittografia post-quantum

Alessio Caminata

Finali delle Olimpiadi di Matematica 2026,
Cesenatico, 8 maggio 2026

Alessio Caminata

- nato nei favolosi anni ’80 .

Immagine da
www.cinematographe.it

Alessio Caminata

- nato nei favolosi anni ’80 .
- nel 2005 e 2006 ero a Cesenatico!

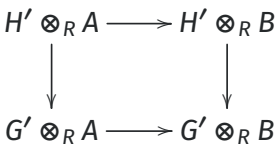
Immagine da www.flickr.com

Alessio Caminata

- nato nei favolosi anni ’80 .
- nel 2005 e 2006 ero a Cesenatico!
- studiato matematica all’Università di Genova

Alessio Caminata

- nato nei favolosi anni '80 .
- nel 2005 e 2006 ero a Cesenatico!
- studiato matematica all'Università di Genova
- dottorato in Germania in algebra commutativa, una branca della matematica *pura*.



Alessio Caminata

- nato nei favolosi anni ’80 .
- nel 2005 e 2006 ero a Cesenatico!
- studiato matematica all’Università di Genova
- dottorato in Germania in algebra commutativa, una branca della matematica *pura*.
- esperienze di ricerca in Spagna e in Svizzera, dove inizio ad interessarmi alle applicazioni della matematica alla crittografia.

Alessio Caminata

- nato nei favolosi anni ’80 .
- nel 2005 e 2006 ero a Cesenatico!
- studiato matematica all’Università di Genova
- dottorato in Germania in algebra commutativa, una branca della matematica *pura*.
- esperienze di ricerca in Spagna e in Svizzera, dove inizio ad interessarmi alle applicazioni della matematica alla crittografia.
- da ottobre 2020 ricercatore all’Università di Genova

Programma

1. Crittografia classica
2. Crittografia a chiave pubblica
3. Crittografia post-quantum
4. Crittografia multivariata (branca di post-quantum)

Part I

Crittografia classica

Che cos'è la crittografia?

Definizione (da Wikipedia)

La *crittografia* (o *criptografia*, dal greco [kryptós], "nascosto", e [graphía], "scrittura") è la branca della crittologia che tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile/intelligibile a persone non autorizzate a leggerlo. Un tale messaggio si chiama comunemente crittogramma e i metodi usati sono detti tecniche di cifratura.

Che cos'è la crittografia? Secondo tentativo...

Alice vorrebbe inviare un messaggio d'amore a Bob, ma ha un piccolo problema...

Alice

Bob

Immagine di Ilaria Caminata

Che cos'è la crittografia? Secondo tentativo...

Alice vorrebbe inviare un messaggio d'amore a Bob, ma ha un piccolo problema...

Alice

Edoardo

Bob

Edoardo, fidanzato di Alice, è molto geloso e le controlla sempre il cellulare!

Immagine di Ilaria Caminata

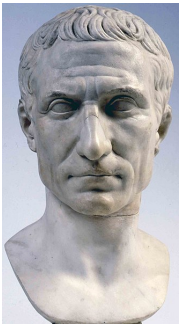
Il cifrario di Cesare

Cifratura: Sostituire ciascuna lettera con quella che si trova 3 posizioni **dopo** nell'alfabeto.

A	B	C	···	W	X	Y	Z
D	E	F	···	Z	A	B	C

Ad esempio

CESAR ⟶ FHVDU



Decifratura: Sostituire ciascuna lettera con quella che si trova 3 posizioni **prima** nell'alfabeto.

FHVDU ⟶ CESAR

Immagine da Musei Vaticani

Il cifrario di Cesare

Rappresentiamo ogni lettera con un numero:

$$A = 1, B = 2, C = 3, \ldots, Z = 26$$

Chiave: Fissiamo un intero $1 \leq k \leq 25$. Cesare usava $k = 3$.

Cifratura: È la funzione

$$x \longmapsto x + k$$

Decifratura: È la funzione

$$y \longmapsto y - k$$

La canzone d'amore

Alice decide di inviare a Bob il testo di una canzone d'amore.

"Un Milione"
di Boomdabash

Ti aspetto come i lidi aspettano l'estate
Come le mogli dei soldati aspettano i mariti
Ti aspetto come i bimbi aspettano il Natale
Come i signori col cartello aspettano agli arrivi
E non è mai per me
Ti aspetterò
Come il caffè a letto a colazione
Come ad un concerto dall'inizio
Si aspetta il ritornello di quella canzone
Ti aspetterò

Perché sei tu che porti il sole
E non c'è niente al mondo
Di migliore di te
Nemmeno vincere un milione
Non c'è niente al mondo
Che vorrei di più di te
Di più di quel che adesso c'è già fra di noi
Nemmeno un milione
Non c'è niente al mondo che farei io senza te
Perché io non ti cambierei nemmeno per...
Nemmeno per un milione

La canzone d'amore

Alice usa la chiave ($k = 5$) concordata in precedenza con Bob per cifrare la canzone con il metodo di Cesare.

yn fxujyyt htrj n qnin fxujyyfst q'jxyfyj
htrj qj rtlqn ijn xtqifyn fxujyyfst n rfwnyn
yn fxujyyt htrj n gnrgn fxujyyfst nq sfyfqj
htrj n xnlstwn htq hfwyjqqt fxujyyfst flqn fwwnan
j sts j' rfn ujw rj
yn fxujyyjwt'
htrj nq hfkkj f qjyyt f htqfentsj
htrj fi zs htshjwyt ifqq'nsnent
xn fxujyyf nq wnytwsjqqt in vzjqqf hfsetsj
yn fxujyyjwt'

ujwhmj' xjn yz hmj utwyn nq xtqj
j sts h'j' snjsyj fq rtsit
in rnlqntwj in yj
sjrrjst anshjwj zs rnqntsj
sts h'j' snjsyj fq rtsit
hmj atwwjn in unz in yj
in unz in vzjq hmj fijxxt h'j' lnf' kwf in stn
sjrrjst zs rnqntsj
sts h'j' snjsyj fq rtsit hmj kfwjn nt xjsef yj
ujwhmj' nt sts yn hfrgnjwjn sjrrjst ujw...
sjrrjst ujw zs rnqntsj

La canzone d'amore

Alice invia la canzone cifrata a Bob che conosce la chiave ed è in grado di decifrarla.

Immagine di Ilaria Caminata

La canzone d'amore

Il fidanzato geloso Edoardo intercetta il messaggio cifrato...

yn fxujyyt htrj n qnin...

?

Ma non conosce la chiave!

Immagine di Ilaria Caminata

La canzone d'amore

Il fidanzato geloso Edoardo intercetta il messaggio cifrato...

yn fxujyyt htrj n qnin...

?

Ma non conosce la chiave!

Tuttavia può provare a decifrare testando tutte le possibili chiavi...

Immagine di Ilaria Caminata

La canzone d'amore

Edoardo prova tutte le possibili chiavi...

- Usando la chiave $k = 1$ (cioè $A \mapsto B$, $B \mapsto C$, ...) ottiene

  xm ewtixxs gsqi m pmhm ...

  che non ha senso.

La canzone d'amore

Edoardo prova tutte le possibili chiavi...

- Usando la chiave $k = 1$ (cioè $A \mapsto B$, $B \mapsto C$, ...) ottiene

  xm ewtixxs gsqi m pmhm ...

  che non ha senso.
- Usando la chiave $k = 2$ (cioè $A \mapsto C$, $B \mapsto D$, ...) ottiene

  wl dvshwwr frph l olgl ...

  che non ha senso.

La canzone d'amore

Edoardo prova tutte le possibili chiavi...

- Usando la chiave $k = 1$ (cioè $A \mapsto B$, $B \mapsto C$, ...) ottiene

  xm ewtixxs gsqi m pmhm ...

  che non ha senso.
- Usando la chiave $k = 2$ (cioè $A \mapsto C$, $B \mapsto D$, ...) ottiene

  wl dvshwwr frph l olgl ...

  che non ha senso.
- ...

La canzone d'amore

Edoardo prova tutte le possibili chiavi...

- Usando la chiave $k = 1$ (cioè $A \mapsto B$, $B \mapsto C$, ...) ottiene

  xm ewtixxs gsqi m pmhm ...

  che non ha senso.
- Usando la chiave $k = 2$ (cioè $A \mapsto C$, $B \mapsto D$, ...) ottiene

  wl dvshwwr frph l olgl ...

  che non ha senso.
- ...
- Usando la chiave $k = 5$ (cioè $A \mapsto F$, $B \mapsto G$, ...) ottiene

  ti aspetto come i lidi ...

  che è il messaggio corretto!

Crittanalisi del cifrario di Cesare

Il problema principale del cifrario di Cesare è che ci sono soltanto 25 possibili chiavi *k*. Si può sempre fare un attacco di *forza bruta* come quello fatto da Edoardo!

Si può cercare di ovviare a questo problema aumentando il numero di chiavi possibili...

Cifrari di permutazione

Cifratura: Sostituire ciascuna lettera del messaggio secondo una tabella fissata che costituisce la **chiave**.

Decifratura: La sostituzione inversa seguendo la tabella.

Chiave: Possiamo usare qualunque tipo di tabella, come le seguenti

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
P	R	I	V	A	C	Y	B	D	E	F	G	H	J	K	L	M	N	O	Q	S	T	U	W	X	Z

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
Q	S	T	U	W	X	Z	P	R	I	V	A	C	Y	B	D	E	F	G	H	J	K	L	M	N	O

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
Y	C	A	B	D	E	F	G	X	Z	H	M	N	O	J	K	L	Q	S	T	U	W	V	P	R	I

Cifrari di permutazione

La chiave è una funzione bigettiva

$$k : \{A, B, \ldots, Z\} \longrightarrow \{A, B, \ldots, Z\}$$

cioè una permutazione.
Ci sono

$$\begin{aligned} 26! &= 26 \cdot 25 \cdot 24 \cdots 3 \cdot 2 \cdot 1 \\ &= 403\,291\,461\,126\,605\,635\,584\,000\,000 \\ &\cong 4,032 \times 10^{26} \end{aligned}$$

possibili chiavi!!

Sono troppe per un tentare un attacco di *forza bruta* come il precedente, anche utilizzando i moderni computer.

Cifrari di permutazione

Alice usa la seguente chiave concordata in precedenza con Bob per cifrare la canzone con un cifrario di permutazione:

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
Y	C	A	B	D	E	F	G	X	Z	H	M	N	O	J	K	L	Q	S	T	U	W	V	P	R	I

tx yskdttj ajnd x mxbx yskdttyoj m'dstytd
ajnd md njfmx bdx sjmbytx yskdttyoj x nyqxtx
tx yskdttj ajnd x cxncx yskdttyoj xm oytymd
ajnd x sxfojqx ajm ayqtdmmj yskdttyoj yfmx yqqxwx
d ojo d' nyx kdq nd
tx yskdttdqj'
ajnd xm ayeed y mdttj y ajmyixjod
ajnd yb uo ajoadqtj bymm'xoxixj
sx yskdtty xm qxtjqodmmj bx ludmmy ayoijod
tx yskdttdqj'

kdqagd' sdx tu agd kjqtx xm sjmd
d ojo a'd' oxdotd ym njobj
bx nxfmxjqd bx td
odnndoj wxoadqd uo nxmxjod
ojo a'd' oxdotd ym njobj
agd wjqqdx bx kxu bx td
bx kxu bx ludm agd ybdssj a'd' fxy' eqy bx ojx
odnndoj uo nxmxjod
ojo a'd' oxdotd ym njobj agd eyqdx xj sdoiy td
kdqagd' xj ojo tx ayncxdqdx odnndoj kdq...
odnndoj kdq uo nxmxjod

Cifrari di permutazione

Il fidanzato geloso Edoardo intercetta il messaggio cifrato...

tx yskdttj ajnd x mxbx...

Ma non conosce la chiave, e non può provare a decifrare testando tutte le possibili chiavi perchè sono troppe!

Cifrari di permutazione

Il fidanzato geloso Edoardo intercetta il messaggio cifrato...

tx yskdttj ajnd x mxbx...

Ma non conosce la chiave, e non può provare a decifrare testando tutte le possibili chiavi perchè sono troppe!

Però...

Cifrari di permutazione

Edoardo nota che c'è una lettera che appare molto più delle altre...

tx yskdttj ajnd x mxbx yskdttyoj m'dstytd
ajnd md njfmx bdx sjmbytx yskdttyoj x
nyqxtx
tx yskdttj ajnd x cxncx yskdttyoj xm
oytymd
ajnd x sxfojqx ajm ayqtdmmj yskdttyoj
yfmx yqqxwx
d ojo d' nyx kdq nd
tx yskdttdqj'
ajnd xm ayeed y mdttj y ajmyixjod
ajnd yb uo ajoadqtj bymm'xoxixj
sx yskdtty xm qxtjqodmmj bx ludmmy
ayoijod
tx yskdttdqj'

kdqagd' sdx tu agd kjqtx xm sjmd
d ojo a'd' oxdotd ym njobj
bx nxfmxjqd bx td
odnndoj wxoadqd uo nxmxjod
ojo a'd' oxdotd ym njobj
agd wjqqdx bx kxu bx td
bx kxu bx ludm agd ybdssj a'd' fxy' eqy bx
ojx
odnndoj uo nxmxjod
ojo a'd' oxdotd ym njobj agd eyqdx xj
sdoiy td
kdqagd' xj ojo tx ayncxdqdx odnndoj
kdq...
odnndoj kdq uo nxmxjod

Cifrari di permutazione

Ad essere precisi, alcune lettere (d, j, x) appaiono molto di più di altre e addirittura alcune (v,p,r) non appaiono affatto!

tx yskdttj ajnd x mxbx yskdttyoj m'dstytd
ajnd md njfmx bdx sjmbytx yskdttyoj x
nyqxtx
tx yskdttj ajnd x cxncx yskdttyoj xm
oytymd
ajnd x sxfojqx ajm ayqtdmmj yskdttyoj
yfmx yqqxwx
d ojo d' nyx kdq nd
tx yskdttdqj'
ajnd xm ayeed y mdttj y ajmyixjod
ajnd yb uo ajoadqtj bymm'xoxixj
sx yskdtty xm qxtjqodmmj bx ludmmy
ayoijod
tx yskdttdqj'

kdqagd' sdx tu agd kjqtx xm sjmd
d ojo a'd' oxdotd ym njobj
bx nxfmxjqd bx td
odnndoj wxoadqd uo nxmxjod
ojo a'd' oxdotd ym njobj
agd wjqqdx bx kxu bx td
bx kxu bx ludm agd ybdssj a'd' fxy' eqy bx
ojx
odnndoj uo nxmxjod
ojo a'd' oxdotd ym njobj agd eyqdx xj
sdoiy td
kdqagd' xj ojo tx ayncxdqdx odnndoj
kdq...
odnndoj kdq uo nxmxjod

Cifrari di permutazione

Edoardo costruisce una tabella

d	81
x	66
j	54
o	49
t	41
y	40
m	31
n	27
a	25
q	23
s	18
b	17
k	17
u	9
g	6
f	5
e	4
i	4
c	3
w	3
l	2

Quali lettere compaiono più frequentemente nella lingua italiana?

Cifrari di permutazione

Edoardo costruisce una tabella

d	81
x	66
j	54
o	49
t	41
y	40
m	31
n	27
a	25
q	23
s	18
b	17
k	17
u	9
g	6
f	5
e	4
i	4
c	3
w	3
l	2

Quali lettere compaiono più frequentemente nella lingua italiana?

Le vocali!!!

Cifrari di permutazione

Conteggio delle lettere nel testo

d	81
x	66
j	54
o	49
t	41
y	40
m	31
n	27
a	25
q	23
s	18
b	17
k	17
u	9
g	6
f	5
e	4
i	4
c	3
w	3
l	2

Analisi delle frequenze della lingua italiana

E	11,79%
A	11,74%
I	11,28%
O	9,83%
N	6,88%
L	6,51%
R	6,37%
T	5,62%
S	4,98%
C	4,50%
D	3,73%
P	3,05%
U	3,01%
M	2,51%
V	2,10%
G	1,64%
H	1,54%
F	0,95%
B	0,92%
Q	0,51%
Z	0,49%

Cifrari di permutazione

Edoardo congettura che la lettera d sia la cifratura di E e sostituisce di conseguenza...

tx yskdttj ajnd x mxbx yskdttyoj m'dstytd
ajnd md njfmx bdx sjmbytx yskdttyoj x nyqxtx
tx yskdttj ajnd x cxncx yskdttyoj xm oytymd
ajnd x sxfojqx ajm ayqtdmmj yskdttyoj yfmx yqqxwx
d ojo d' nyx kdq nd
tx yskdttdqj'
ajnd xm ayeed y mdttj y ajmyixjod
ajnd yb uo ajoadqtj bymm'xoxixj
sx yskdtty xm qxtjqodmmj bx ludmmy ayoijod
tx yskdttdqj'

kdqagd' sdx tu agd kjqtx xm sjmd
d ojo a'd' oxdotd ym njobj
bx nxfmxjqd bx td
odnndoj wxoadqd uo nxmxjod
ojo a'd' oxdotd ym njobj
agd wjqqdx bx kxu bx td
bx kxu bx ludm agd ybdssj a'd' fxy' eqy bx ojx
odnndoj uo nxmxjod
ojo a'd' oxdotd ym njobj agd eyqdx xj sdoiy td
kdqagd' xj ojo tx ayncxdqdx odnndoj kdq...
odnndoj kdq uo nxmxjod

Cifrari di permutazione

Edoardo congettura che la lettera d sia la cifratura di E e sostituisce di conseguenza...

tx yskEttj ajnE x mxbx yskEttyoj m'EstytE
ajnE mE njfmx bEx sjmbytx yskEttyoj x nyqxtx
tx yskEttj ajnE x cxncx yskEttyoj xm oytymE
ajnE x sxfojqx ajm ayqtEmmj yskEttyoj yfmx yqqxwx
E ojo E' nyx kEq nE
tx yskEttEqj'
ajnE xm ayeeE y mEttj y ajmyixjoE
ajnE yb uo ajoaEqtj bymm'xoxixj
sx yskEtty xm qxtjqoEmmj bx luEmmy ayoijoE
tx yskEttEqj'

kEqagE' sEx tu agE kjqtx xm sjmE
E ojo a'E' oxEotE ym njobj
bx nxfmxjqE bx tE
oEnnEoj wxoaEqE uo nxmxjoE
ojo a'E' oxEotE ym njobj
agE wjqqEx bx kxu bx tE
bx kxu bx luEm agE ybEssj a'E' fxy' eqy bx ojx
oEnnEoj uo nxmxjoE
ojo a'E' oxEotE ym njobj agE eyqEx xj sEoiy tE
kEqagE' xj ojo tx ayncxEqEx oEnnEoj kEq...
oEnnEoj kEq uo nxmxjoE

Cifrari di permutazione

Le seconde due lettere più presenti, j e x, potrebbero essere due delle altre tre vocali più diffuse: A, I, e O.

d	81
x	66
j	54
o	49
t	41
y	40
m	31
n	27
a	25
q	23
s	18

b	17
k	17
u	9
g	6
f	5
e	4
i	4
c	3
w	3
l	2

E	11,79%
A	11,74%
I	11,28%
O	9,83%
N	6,88%
L	6,51%
R	6,37%
T	5,62%
S	4,98%
C	4,50%
D	3,73%

P	3,05%
U	3,01%
M	2,51%
V	2,10%
G	1,64%
H	1,54%
F	0,95%
B	0,92%
Q	0,51%
Z	0,49%

Cifrari di permutazione

Edoardo fa alcuni tentativi e dopo un po' arriva all'associazione

$$d \mapsto E,\ j \mapsto O,\ x \mapsto I$$

che sembra corretta.

tx yskdttj ajnd x mxbx yskdttyoj m'dstytd
ajnd md njfmx bdx sjmbytx yskdttyoj x
nyqxtx
tx yskdttj ajnd x cxncx yskdttyoj xm
oytymd
ajnd x sxfojqx ajm ayqtdmmj yskdttyoj
yfmx yqqxwx
d ojo d' nyx kdq nd
tx yskdttdqj'
ajnd xm ayeed y mdttj y ajmyixjod
ajnd yb uo ajoadqtj bymm'xoxixj
sx yskdtty xm qxtjqodmmj bx ludmmy
ayoijod
tx yskdttdqj'

kdqagd' sdx tu agd kjqtx xm sjmd
d ojo a'd' oxdotd ym njobj
bx nxfmxjqd bx td
odnndoj wxoadqd uo nxmxjod
ojo a'd' oxdotd ym njobj
agd wjqqdx bx kxu bx td
bx kxu bx ludm agd ybdssj a'd' fxy' eqy bx
ojx
odnndoj uo nxmxjod
ojo a'd' oxdotd ym njobj agd eyqdx xj
sdoiy td
kdqagd' xj ojo tx ayncxdqdx odnndoj
kdq...
odnndoj kdq uo nxmxjod

Cifrari di permutazione

Edoardo fa alcuni tentativi e dopo un po' arriva all'associazione

$$d \mapsto E,\ j \mapsto O,\ x \mapsto I$$

che sembra corretta.

tI yskEttO aOnE I mIbI yskEttyoO m'EstytE
aOnE mE nOfmI bEI sOmbytI yskEttyoO I
nyqItI
tI yskEttO aOnE I cIncI yskEttyoO Im
oytymE
aOnE I sIfoOqI aOm ayqtEmmO yskEttyoO
yfmI yqqIwI
E oOo E' nyI kEq nE
tI yskEttEqO'
aOnE Im ayeeE y mEttO y aOmyiIOoE
aOnE yb uo aOoaEqtO bymm'IoIiIO
sI yskEtty Im qItOqoEmmO bI luEmmy
ayoiOoE
tI yskEttEqO'

kEqagE' sEI tu agE kOqtI Im sOmE
E oOo a'E' oIEotE ym nOobO
bI nIfmIOqE bI tE
oEnnEoO wIoaEqE uo nImIOoE
oOo a'E' oIEotE ym nOobO
agE wOqqEI bI kIu bI tE
bI kIu bI luEm agE ybEssO a'E' fIy' eqy bI
oOI
oEnnEoO uo nImIOoE
oOo a'E' oIEotE ym nOobO agE eyqEI IO
sEoiy tE
kEqagE' IO oOo tI ayncIEqEI oEnnEoO
kEq...
oEnnEoO kEq uo nImIOoE

Cifrari di permutazione

Edoardo fa alcuni tentativi e dopo un po' arriva all'associazione

$$d \mapsto E,\ j \mapsto O,\ x \mapsto I$$

che sembra corretta.

tI yskEttO aOnE I mIbI yskEttyoO m'EstytE
aOnE mE nOfmI bEI sOmbytI yskEttyoO I
nyqItI
tI yskEttO aOnE I cIncI yskEttyoO Im
oytymE
aOnE I sIfoOqI aOm ayqtEmmO yskEttyoO
yfmI yqqIwI
E oOo E' nyI kEq nE
tI yskEttEqO'
aOnE Im ayeeE y mEttO y aOmyiIOoE
aOnE yb uo aOoaEqtO bymm'IoIiIO
sI yskEtty Im qItOqoEmmO bI luEmmy
ayoiOoE
tI yskEttEqO'

kEqagE' sEI tu agE kOqtI Im sOmE
E oOo a'E' oIEotE ym nOobO
bI nIfmIOqE bI tE
oEnnEoO wIoaEqE uo nImIOoE
oOo a'E' oIEotE ym nOobO
agE wOqqEI bI kIu bI tE
bI kIu bI luEm agE ybEssO a'E' fly' eqy bI
oOI
oEnnEoO uo nImIOoE
oOo a'E' oIEotE ym nOobO agE eyqEI IO
sEoiy tE
kEqagE' IO oOo tI ayncIEqEI oEnnEoO
kEq...
oEnnEoO kEq uo nImIOoE

Cifrari di permutazione

Edoardo continua in questo modo con l'analisi delle frequenze e aiutandosi con alcune parole particolari...

tI yskEttO aOnE I mIbI yskEttyoO m'EstytE
aOnE mE nOfmI bEI sOmbytI yskEttyoO I
nyqItI
tI yskEttO aOnE I cIncI yskEttyoO Im
oytymE
aOnE I sIfoOqI aOm ayqtEmmO yskEttyoO
yfmI yqqIwI
E oOo E' nyI kEq nE
tI yskEttEqO'
aOnE Im ayeeE y mEttO y aOmyiIOoE
aOnE yb uo aOoaEqtO bymm'IoIiIO
sI yskEtty Im qItOqoEmmO bI luEmmy
ayoiOoE
tI yskEttEqO'

kEqagE' sEI tu agE kOqtI Im sOmE
E oOo a'E' oIEotE ym nOobO
bI nIfmIOqE bI tE
oEnnEoO wIoaEqE uo nImIOoE
oOo a'E' oIEotE ym nOobO
agE wOqqEI bI kIu bI tE
bI kIu bI luEm agE ybEssO a'E' fIy' eqy bI
oOI
oEnnEoO uo nImIOoE
oOo a'E' oIEotE ym nOobO agE eyqEI IO
sEoiy tE
kEqagE' IO oOo tI ayncIEqEI oEnnEoO
kEq...
oEnnEoO kEq uo nImIOoE

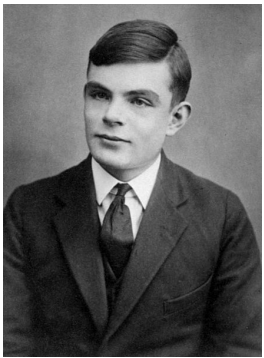
Crittanalisi dei cifrari di permutazione

Con un po' di pazienza, Edoardo riesce a decifrare il messaggio di Alice.

In generale, l'analisi delle frequenze e tecniche simili a quelle che abbiamo illustrato permettono di decrittare i cifrari di permutazione che sono perciò considerati insicuri.

Facciamo un passo avanti nel tempo...

La Seconda Guerra Mondiale e successivamente l'invenzione del computer hanno dato una spinta ulteriore alla crittografia e posto ulteriori sfide ed obiettivi.



Immagini da Wikipedia

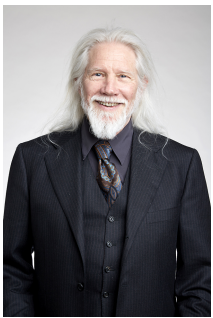
Part II

Crittografia a chiave pubblica (o asimmetrica)

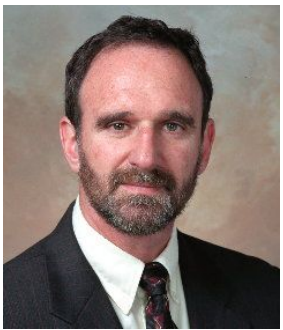
La crittografia a chiave pubblica

Domanda:

È possibile per Alice e Bob comunicare in maniera cifrata senza essersi prima messi d'accordo di persona su una chiave comune?



Whitfield Diffie

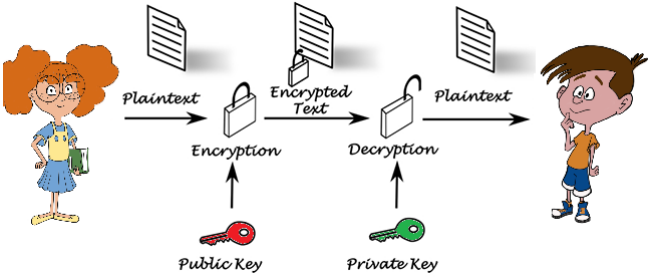


Martin Hellman

Immagini da Wikipedia

La crittografia a chiave pubblica

Diffie e Hellman in *New Directions in Cryptography* (1976) teorizzano la crittografia a chiave pubblica.



 = Chiave pubblica. Può essere condivisa.

 = Chiave segreta. Solo Bob la conosce.

Intermezzo: Aritmetica modulare

Fissiamo un numero intero $n > 0$ e consideriamo i numeri interi "modulo n", cioè identificando due numeri che danno lo stesso resto quando divisi per n.
Ad esempio per $n = 12$ abbiamo

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,$$

e poi

$$\begin{aligned} 12 &\equiv 0 \mod 12 \\ 13 &\equiv 1 \mod 12 \\ 14 &\equiv 2 \mod 12 \\ &\dots \end{aligned}$$

perchè $12 = 12 + 0$, $13 = 12 + 1$, $14 = 12 + 2$ e così via...

Intermezzo: Aritmetica modulare

Anche le operazioni di somma e prodotto si possono considerare modulo n:

$$(x \mod n) + (y \mod n) \equiv (x + y) \mod n$$
$$(x \mod n) \cdot (y \mod n) \equiv (x \cdot y) \mod n$$

Ad esempio ($n = 12$):

$$10 + 4 = 14 \equiv 2 \mod 12$$
$$7 \cdot 7 = 49 \equiv 1 \mod 12$$

Per $n = 2$ si ha l'aritmetica binaria:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Intermezzo: Aritmetica modulare

Sia p un numero primo. Un **generatore** $\bmod p$ è un intero $g \bmod p$ tale che g^m per $m = 0, 1, 2, 3 \ldots$ assume tutti i possibili valori $\neq 0 \bmod p$.

Teorema

Esiste sempre un generatore $\bmod p$, i.e., il gruppo $\mathbb{Z}_p^*$ è ciclico.

Esempio

2 è un generatore $\bmod 5$

$$2^0 = 1, \quad 2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8 \equiv 3$$

Diffie-Hellman Key Exchange

Alice e Bob scelgono un primo p e un generatore $g \mod p$.

Alice sceglie $a \in \mathbb{Z}$, calcola $A = g^a \mod p$ e lo manda a Bob.

$A \longleftrightarrow B$

Bob sceglie $b \in \mathbb{Z}$, calcola $B = g^b \mod p$ e lo manda ad Alice.

Alice e Bob sono entrambi in grado di calcolare il segreto condiviso (*shared key*)

$$K = g^{ab} = A^b = B^a$$

Diffie-Hellman Key Exchange

Alice e Bob scelgono un primo p e un generatore $g \mod p$.

Alice sceglie $a \in \mathbb{Z}$, calcola $A = g^a \mod p$ e lo manda a Bob.

$A \longleftrightarrow B$

Bob sceglie $b \in \mathbb{Z}$, calcola $B = g^b \mod p$ e lo manda ad Alice.

Alice e Bob sono entrambi in grado di calcolare il segreto condiviso (*shared key*)

$$K = g^{ab} = A^b = B^a$$

Edoardo conosce p, g, A, B. Può trovare K se sa calcolare i logaritmi in base g modulo p (**Problema del logaritmo discreto**).

Il crittosistema RSA

Lo scambio di chiavi di DH non è propriamente un crittosistema a chiave pubblica. Il primo crittosistema a chiave pubblica è il sistema RSA inventato da Ronald Rivest, Adi Shamir e Leonard Adleman nel 1977.

Immagine da
https://www.usc.edu

Intermezzo: Aritmetica modulare

Teorema di Eulero

Se $a \in \mathbb{Z}$ è coprimo con n allora

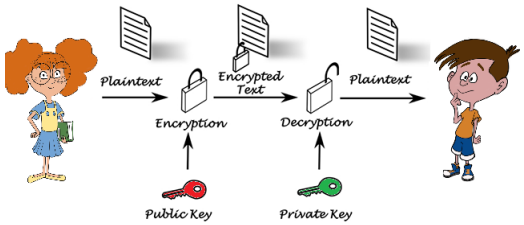
$$a^{\varphi(n)} \equiv 1 \bmod n$$

La funzione $\varphi(n) = \#\{x \in \mathbb{N} : \ x < n, \ \mathrm{MCD}(x, n) = 1\}$ è la funzione di Eulero che conta quanti numeri coprimi con n e minori di n ci sono. Ad esempio

$$\varphi(2) = 1, \ \varphi(3) = 2, \ \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2, \ldots$$
$$\varphi(p) = p - 1 \ \text{ se } p \ \text{ è primo}$$
$$\varphi(p \cdot q) = (p-1)(q-1) \ \text{ se } p, q \ \text{ sono primi distinti}$$

In generale è difficile calcolare $\varphi(n)$ se non si conosce la fattorizzazione di n.

Il crittosistema RSA



Fase 1: Bob costruisce le chiavi:

- Bob sceglie due numeri primi p, q molto grandi.
- Bob calcola $n = p \cdot q$ e $\varphi(n) = (p-1)(q-1)$.
- Bob sceglie un numero intero e (esponente pubblico) coprimo con $\varphi(n)$.
- Bob calcola un intero d (esponente privato) tale che $e \cdot d \equiv 1 \bmod \varphi(n)$.

Fase 2: Bob invia la chiave pubblica, n ed e, ad Alice, e mantiene per sè la chiave privata, p,q,$\varphi(n)$, d.

Il crittosistema RSA

Fase 3: Alice cifra ed invia il messaggio a Bob:

- Il messaggio in chiaro di Alice è un numero intero m.
- Alice calcola $c = m^e \bmod n$ che è il messaggio cifrato.
- Alice invia il messaggio cifrato c a Bob.

Fase 4: Bob decifra il messaggio:

- Bob riceve il messaggio cifrato c da Alice.
- Bob decifra il messaggio calcolando $c^d \bmod n$. Infatti

$$c^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{k\cdot\varphi(n)+1} \equiv \left(m^{\varphi(n)}\right)^k \cdot m \equiv 1 \cdot m \equiv m \bmod n$$

perchè $ed \equiv 1 \bmod \varphi(n)$ implica $ed = k \cdot \varphi(n) + 1$ con $k \in \mathbb{Z}$.

Crittanalisi di RSA

Edoardo intercetta:

- il messaggio cifrato c;
- la chiave pubblica n, e.

Ma non conosce $\varphi(n)$ e quindi non può calcolare l'esponente di decifratura d.[1]

Conoscere $\varphi(n)$ è equivalente a conoscere la fattorizzazione di $n = p \cdot q$.

- Per applicazioni, vengono scelti p, q molto grandi $p, q \sim 2^{1024}$.

[1] Ricordiamo che d è scelto in modo che $ed \equiv 1 \bmod \varphi(n)$.

Dove si usa la crittografia a chiave pubblica?

Algoritmi di crittografia asimmetrica usati:

- **RSA** (usato in SSL/TLS, online banking, ATM, …);
- **DSA** (firma digitale in SSL/TLS);
- Scambio di chiavi di **Diffie-Hellman** (usato in SSL/TLS, NFC, pagamenti digitali);
- **ECDH : Elliptic-curve Diffie–Hellman** (usato per crittografia end-to-end, Signal, WhatsApp, Facebook Messenger, Skype, …)
- **ECDSA: Elliptic-curve digital signature algorithm** (usato nei Bitcoin, Ethereum, …).

La crittografia a chiave pubblica è più lenta di quella a chiave segreta, quindi spesso si usa in combinazione.

Crittografia a chiave pubblica

Gli algoritmi a chiave pubblica più usati basano la loro sicurezza sulla difficoltà (computazionale) di due problemi matematici:

1. la scomposizione in fattori primi di un numero intero $N \gg 0$ (RSA);
2. il problema del logaritmo discreto in un gruppo G
   - $G = \mathbb{Z}_p^*$ $\longrightarrow$ DSA, Diffie-Hellman;
   - $G = E(\mathbb{F}_q)$ $\longrightarrow$ ECDH, ECDSA.

Con le dovute accortezze, questi problemi sono computazionalmente difficili (se N e $|G|$ sono sufficientemente grandi), anche avendo a disposizione un computer estremamente potente…

Crittografia a chiave pubblica

Gli algoritmi a chiave pubblica più usati basano la loro sicurezza sulla difficoltà (computazionale) di due problemi matematici:

1. la scomposizione in fattori primi di un numero intero $N \gg 0$ (RSA);
2. il problema del logaritmo discreto in un gruppo G
   - $G = \mathbb{Z}_p^*$ $\longrightarrow$ DSA, Diffie-Hellman;
   - $G = E(\mathbb{F}_q)$ $\longrightarrow$ ECDH, ECDSA.

Con le dovute accortezze, questi problemi sono computazionalmente difficili (se N e $|G|$ sono sufficientemente grandi), anche avendo a disposizione un computer estremamente potente…

…un computer normale…

Algoritmo di Shor

Nel 1994, Peter Shor ha ideato un algoritmo per computer quantistico che fattorizza un numero intero N e calcola il logaritmo discreto in un gruppo G in tempo polinomiale in $\log N$ (o $\log |G|$).

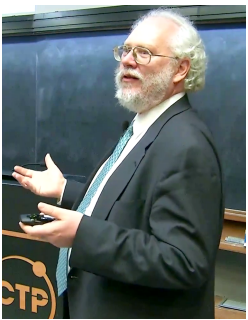
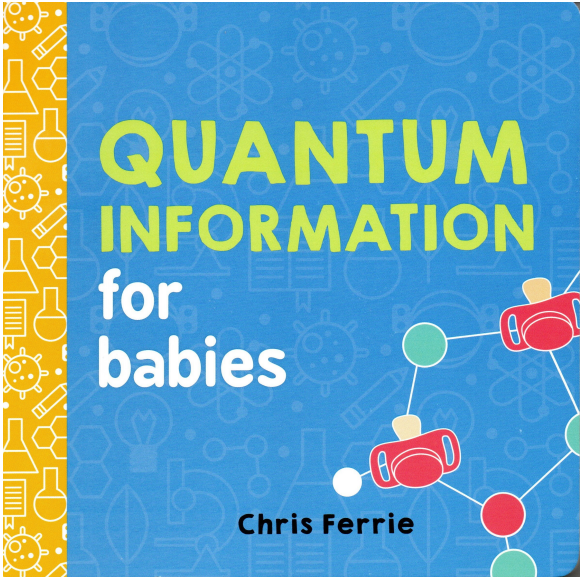


Immagine da Wikipedia

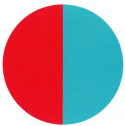
Part III

Crittografia post-quantum

Il computer quantistico



Il computer quantistico



We need 1 bit of information
to record the color of this ball.

An electron stores a
quantum bit of information.

Immagine da “Quantum information for babies” di C. Ferrie

Il computer quantistico è più potente?

Non necessariamente più potente, ma può fare alcune cose più velocemente

1. **Algoritmo di Shor (1994)**:
   - fattorizza gli interi su un computer quantistico,
   - dato un intero N, lo fattorizza in tempo polinomiale in $\log(N)$,
   - dato un gruppo G, calcola il logaritmo discreto in G in tempo polinomiale in $\log|G|$
   - su un computer classico, il tempo è esponenziale in N (o $|G|$).
2. **Algoritmo di Grover (1996)**:
   - effettua una ricerca in una lista non ordinata su un computer quantistico,
   - trova un'entrata in una lista di N elementi in tempo proporzionale a $\sqrt{N}$
   - su un computer classico, il tempo è proporzionale a N.

Bisogna preoccuparsi?

- La crittografia simmetrica (a chiave segreta) non è influenzata significativamente dal computer quantistico.
- I sistemi crittografici asimmetrici (a chiave pubblica) più usati al giorno d'oggi possono essere attaccati efficacemente con l'algoritmo di Shor: RSA, DSA, Diffie–Hellman, ECDH, ECDSA,…

Bisogna preoccuparsi?

- La crittografia simmetrica (a chiave segreta) non è influenzata significativamente dal computer quantistico.
- I sistemi crittografici asimmetrici (a chiave pubblica) più usati al giorno d'oggi possono essere attaccati efficacemente con l'algoritmo di Shor: RSA, DSA, Diffie–Hellman, ECDH, ECDSA,…

Ma il computer quantistico è fantascienza, no?

Computer quantistici: alcuni aggiornamenti

- 2011-2017: D-Wave sviluppa i primi computer quantistici usando l'annealing.
- 2019: Google annuncia Sycamore a **53 qubits**.
- 2020: IBM annuncia Q System One a **20 qubits** basato sulla superposition.
- 2020: L'Università di Scienze e Tecnologia della Cina (USTC) annuncia Jiuzhang a **76 qubits**.
- 2023: IBM sviluppa l'alveare quantistico Condor a **1121 qubits**.
- settembre 2025: Caltech assembla un array di 6100 qubits.
- marzo 2026: diversi articoli (Google, Oramics,...) stimano che ECC-256 e RSA-2028 possano essere rotti con < 500000 qubits.

Computer quantistici: alcuni aggiornamenti

- settembre 2025: Caltech assembla un array di 6100 qubits.
- marzo 2026: diversi articoli (Google, Oramics,...) stimano che ECC-256 e RSA-2028 possano essere rotti con < 500000 qubits.

Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits

Madelyn Cain[1,*,†], Qian Xu[1,2,*,‡], Robbie King[1], Lewis R. B. Picard[1], Harry Levine[1,3], Manuel Endres[1,2], John Preskill[1,2], Hsin-Yuan Huang[1,2], Dolev Bluvstein[1,2,§]
[1] *Oratomic, Pasadena, California 91125, USA*
[2] *California Institute of Technology, Pasadena, California 91125, USA*
[3] *Department of Physics, University of California, Berkeley, California 94720, USA*
[†] *mcain@oratomic.com,* [‡] *qxu@oratomic.com,* [§] *dbluvstein@oratomic.com*
[*] *These authors contributed equally*
(Dated: March 31, 2026)

Quantum computers have the potential to perform computational tasks beyond the reach of classical machines. A prominent example is Shor's algorithm for integer factorization and discrete logarithms, which is of both fundamental importance and practical relevance to cryptography. However, due to the high overhead of quantum error correction, optimized resource estimates for cryptographically relevant instances of Shor's algorithm require millions of physical qubits. Here, by leveraging advances in high-rate quantum error-correcting codes, efficient logical instruction sets, and circuit design, we show that Shor's algorithm can be executed at cryptographically relevant scales with as few as 10,000 reconfigurable atomic qubits. Increasing the number of physical qubits improves time efficiency by enabling greater parallelism; under plausible assumptions, the runtime for discrete logarithms on the P-256 elliptic curve could be just a few days for a system with 26,000 physical qubits, while the runtime for factoring RSA–2048 integers is one to two orders of magnitude longer. Recent neutral-atom experiments have demonstrated universal fault-tolerant operations below the error-correction threshold, computation on arrays of hundreds of qubits, and trapping arrays with more than 6,000 highly coherent qubits. Although substantial engineering challenges remain, our theoretical analysis indicates that an appropriately designed neutral-atom architecture could support quantum computation at cryptographically relevant scales. More broadly, these results highlight the capability of neutral atoms for fault-tolerant quantum computing with wide-ranging scientific and technological applications.

Post-quantum cryptography

Da tempo la comunità crittografica ha cercato delle soluzioni che possano resistere agli attacchi con un computer quantistico. L'idea generale è di costruire delle primitive crittografiche a partire da problemi dove un computer quantistico non sia più efficace di uno classico.

I principali candidati sono i seguenti:

- Lattice-based cryptography (basata sui reticoli)
- Code-based cryptography (basata sui codici correttori)
- Multivariate cryptography (basata sui polinomi)
- Isogeny-based cryptography (basata sulle isogenie tra curve ellittiche)
- Hash-based cryptography (basata sulle funzioni di hash)
- ⋮

La rivoluzione è già avviata!

Nel 2017, il NIST ha annunciato una competizione volta a stabilire i nuovi standard crittografici post-quantum per il futuro.

Il National Institute of Standards and Technology (NIST) è un'agenzia del dipartimento del commercio degli Stati Uniti. Il suo compito è la promozione dell'economia americana al fine di sviluppare standard, tecnologie e metodologie che favoriscano la produzione e il commercio.

Immagine da Wikipedia

NIST PQC requirements

Il NIST ha richiesto due tipi di protocolli crittografici:

1. **Key encapsulation mechanism (KEM).** Un protocollo che permette di trasmettere in maniera sicura una chiave di sessione attraverso un canale non sicuro.
2. **Digital Signature (DS).** Un protocollo che permette di autenticare l'autore di un documento elettronico e garantire la non-repudiation, analogo alla firma manuale di un documento.

Ciascun algoritmo deve essere proposto con cinque set di parametri corrispondenti a cinque livelli di sicurezza crescente.

NIST PQC 1st round candidates

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**

Immagine da NIST.gov

NIST PQC 1st round - Countries involved

263 researchers from 24 Countries

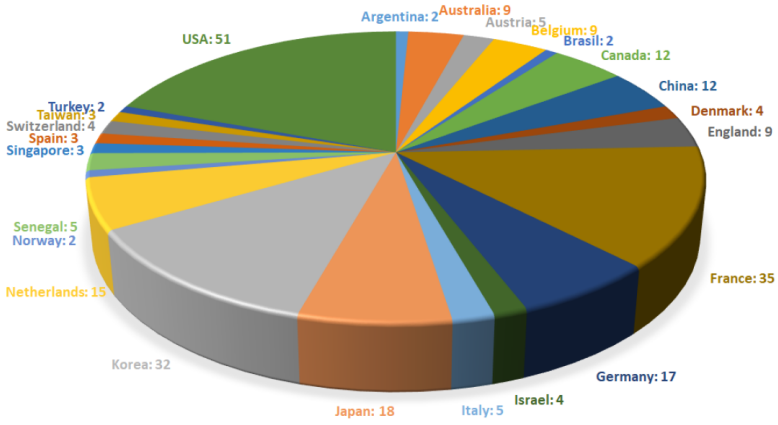


Immagine da Marco Baldi
(UniPM)

NIST PQC selection

Il processo di selezione del NIST è durato 6-7 anni attraverso 3+1 Round. Terminato definitivamente l'11 marzo 2025 con l'annuncio dell'ultimo algoritmo standardizzato (HQC).

Gli algoritmi selezionati per la *standardizzazione* sono

- **CRYSTALS-Kyber**: KEM basato sui reticoli.
- **CRYSTALS-Dilithium**: DS basata sui reticoli.
- **Falcon**: DS con firme corte basata sui reticoli.
- **SPHINCS+**: DS basata sulle funzioni di hash (consigliata come alternativa)
- **HQC**: KEM basato sui codici.

Not the end of the story ...

Vista la scarsa varietà (2 firme su 3 basate sui reticoli), il 6 settembre 2022 il NIST ha lanciato una nuova competizione per selezionare nuovi schemi di firma digitale (DS) post-quantum, preferibilmente non basati sui reticoli. Date limite per la submission: 1 giugno 2023.

Additional PQ digital signature candidates

Code-based
CROSS
Enhanced pqsigRM
FuLeeca
LESS
MEDS
Wave

Lattice-based
EagleSign
EHTv3 and EHTv4
HAETAE
HAWK
HuFu
Raccoon
SQUIRRELS

Multivariate-based
3WISE
DME-Sign
HPPC
MAYO
PROV
QR-UOV
SNOVA
TUOV
UOV
VOX

Hash-based
AIMer
Ascon-Sign
FAEST
SPHINCS-alpha

Isogeny-based
SQIsign

Others
Biscuit
MIRA
MiRitH
MQOM
PERK
RYDE
SDitH
ALTEQ
eMLE-Sig 2.0
KAZ-SIGN
Preon
Xifrat1-Sign.I

Additional PQ digital signature candidates: Round 2

Code-based
CROSS
LESS

Lattice-based
HAWK

Multivariate-based
MAYO
QR-UOV
SNOVA
UOV

Hash-based
FAEST

Isogeny-based
SQIsign

Others
MIRA+MiRitH=Mirath
MQOM
PERK
RYDE
SDitH

La transizione post-quantum è iniziata…

Milestone 1 Entro il 31 dicembre 2026	Milestone 2 Entro il 31 dicembre 2030	Obiettivo finale Entro il 31 dicembre 2035
1. Avviare la pianificazione della transizione PQC. 2. Coinvolgere sia stakeholder nazionali rilevanti (PA, industria, ricerca) che fornitori di terze parti(supply chain) 3. Sviluppare piani di implementazione e timeline nazionali. 4. Iniziare progetti pilota per casi d'uso ad alto e medio rischio. 5. Mappare le dipendenze crittografiche e valutare i rischi quantistici. 6. Definire e implementare sistemi di gestione degli asset crittografici e garantire la crypto-agilità 7. Costruire consapevolezza nazionale tramite programmi di comunicazione. 8. Iniziare a collaborare a livello europeo (NIS Cooperation Group, standardizzazione).	1. Completare la transizione PQC per i casi d'uso ad alto rischio. 2. Completare la pianificazione e i progetti pilota per i casi a rischio medio. 3. Rendere operativi aggiornamenti software e firmware quantum-safe di default. 4. Sostenere l'agilità crittografica e prevedere upgrade futuri. 5. Allocare risorse, evolvere normative e schemi di certificazione. 6. Rafforzare interoperabilità e cooperazione transfrontaliera. 7. Attivare centri di test e validazione in ambienti reali.	1. Completare la transizione per i casi ad alto e medio rischio. 2. Allinearsi con NIST, NCSC UK e altre roadmap globali. 3. Assicurare che ogni nuovo sistema immesso sul mercato sia aggiornabile a PQC.
Prodotti da consegnare 1. Roadmap nazionale PQC aggiornata e operativa. 2. Inventari crittografici e mappe di dipendenza (CBOM, SBOM). 3. Sistema di gestione degli asset crittografici (CBOM) operativo 4. Programma nazionale di consapevolezza e formazione (target C-level, IT, OT). 5. Progetti pilota documentati (TLS, VPN, firma digitale, aggiornamenti software, ecc.). 6. Partecipazione attiva a gruppi internazionali (NIS CG PQC, ETSI, NIST).	**Prodotti da consegnare** 1. Piani di migrazione per casi d'uso ad alto e medio rischio. 2. Bollettini di rischio e alert nazionali, basati su osservatori tecnici. 3. Schemi di certificazione aggiornati con algoritmi PQC (es. EUCC, SOG-IS). 4. Centri nazionali di test e interoperabilità (eventualmente in cooperazione UE).Report pubblici e raccomandazioni operative basate su sperimentazioni e benchmarking. 5. Programmi di finanziamento per l'adozione PQC (voucher, bandi, supporto a PMI).	**Prodotti da consegnare** 1. Aggiornamenti normativi a regolamenti, capitolati e requisiti crittografici. 2. Sistemi immessi sul mercato aggiornabili a PQC per default. 3. Interoperabilità assicurata a livello internazionale.

Immagine da ACN

Part IV

Multivariate cryptography

Multivariate Cryptography

La crittografia multivariata usa dei sistemi polinomiali per costruire primitive crittografiche post-quantum. La difficoltà si basa sul problema **PoSSo (Polynomial System Solving)**.

PoSSo Problem

Sia $\Bbbk$ un campo (finito), e siano $f_1, \ldots, f_m \in \Bbbk[x_1, \ldots, x_n]$ polinomi in n variabili a coefficienti in $\Bbbk$. Trovare $a = (a_1, \ldots, a_n) \in \Bbbk^n$ tale che

$$f_1(a) = f_2(a) = \cdots = f_m(a) = 0.$$

Multivariate Cryptography

La crittografia multivariata usa dei sistemi polinomiali per costruire primitive crittografiche post-quantum. La difficoltà si basa sul problema **PoSSo (Polynomial System Solving)**.

PoSSo Problem

Sia $\Bbbk$ un campo (finito), e siano $f_1, \ldots, f_m \in \Bbbk[x_1, \ldots, x_n]$ polinomi in n variabili a coefficienti in $\Bbbk$. Trovare $a = (a_1, \ldots, a_n) \in \Bbbk^n$ tale che

$$f_1(a) = f_2(a) = \cdots = f_m(a) = 0.$$

È un problema difficile?

PoSSo Problem

PoSSo : Trovare $a \in \mathbb{k}^n$ tale che $f_1(a) = f_2(a) = \cdots = f_m(a) = 0$.

- Se i polinomi $f_1, \ldots, f_m$ sono lineari ($\deg f_i = 1$), si può trovare facilmente una soluzione a usando l'eliminazione di Gauss.

PoSSo Problem

PoSSo : Trovare $a \in \mathbb{k}^n$ tale che $f_1(a) = f_2(a) = \cdots = f_m(a) = 0$.

- Se i polinomi $f_1, \ldots, f_m$ sono lineari ($\deg f_i = 1$), si può trovare facilmente una soluzione a usando l'eliminazione di Gauss.
- Se la cardinalità di $|\mathbb{k}^n|$ è piccola, si può facilmente trovare una soluzione a provando tutti gli elementi di $\mathbb{k}^n$ (forza bruta).

PoSSo Problem

PoSSo : Trovare $a \in \mathbb{k}^n$ tale che $f_1(a) = f_2(a) = \cdots = f_m(a) = 0$.

- Se i polinomi $f_1, \ldots, f_m$ sono lineari ($\deg f_i = 1$), si può trovare facilmente una soluzione a usando l'eliminazione di Gauss.
- Se la cardinalità di $|\mathbb{k}^n|$ è piccola, si può facilmente trovare una soluzione a provando tutti gli elementi di $\mathbb{k}^n$ (forza bruta).
- Se $n = 1$, i polinomi $f_1, \ldots, f_m$ sono univariati, si può trovare facilmente una soluzione a usando algoritmi di fattorizzazione (Berlekamp, ...).

PoSSo Problem

PoSSo : Trovare $a \in \mathbb{k}^n$ tale che $f_1(a) = f_2(a) = \cdots = f_m(a) = 0$.

- Se i polinomi $f_1, \ldots, f_m$ sono lineari ($\deg f_i = 1$), si può trovare facilmente una soluzione a usando l'eliminazione di Gauss.
- Se la cardinalità di $|\mathbb{k}^n|$ è piccola, si può facilmente trovare una soluzione a provando tutti gli elementi di $\mathbb{k}^n$ (forza bruta).
- Se $n = 1$, i polinomi $f_1, \ldots, f_m$ sono univariati, si può trovare facilmente una soluzione a usando algoritmi di fattorizzazione (Berlekamp, ...).
- Se $n > 1$, $\deg f_i > 1$, $|\mathbb{k}^n| \gg 0$, e i polinomi sono random, allora il problema è computazionalmente difficile, anche per il campo $\mathbb{k} = \mathbb{Z}_2$.

PoSSo Problem

PoSSo : Trovare $a \in \mathbb{k}^n$ tale che $f_1(a) = f_2(a) = \cdots = f_m(a) = 0$.

- Se i polinomi $f_1, \ldots, f_m$ sono lineari ($\deg f_i = 1$), si può trovare facilmente una soluzione a usando l'eliminazione di Gauss.
- Se la cardinalità di $|\mathbb{k}^n|$ è piccola, si può facilmente trovare una soluzione a provando tutti gli elementi di $\mathbb{k}^n$ (forza bruta).
- Se $n = 1$, i polinomi $f_1, \ldots, f_m$ sono univariati, si può trovare facilmente una soluzione a usando algoritmi di fattorizzazione (Berlekamp, ...).
- Se $n > 1$, $\deg f_i > 1$, $|\mathbb{k}^n| \gg 0$, e i polinomi sono random, allora il problema è computazionalmente difficile, anche per il campo $\mathbb{k} = \mathbb{Z}_2$.

Idea: Si può usare questo problema per fare della crittografia!

Multivariate Cryptography

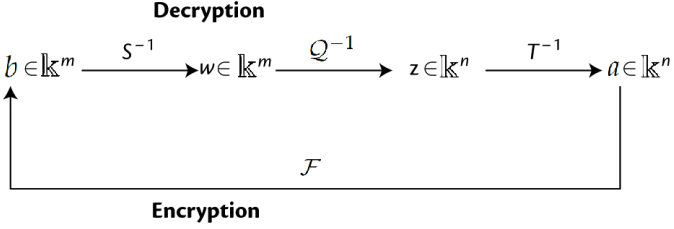
Uno schema crittografico multivariato consiste di:

- Un campo finito pubblico $\Bbbk = \mathbb{F}_q$.
- m polinomi privati (quadratici) $q_1, \ldots, q_m$ in n variabili che formano un'applicazione $\mathcal{Q} : \Bbbk^n \to \Bbbk^m$ che è *computazionalmente facile* da invertire.
- Due applicazioni lineari private e invertibili $S : \Bbbk^m \to \Bbbk^m$ e $T : \Bbbk^n \to \Bbbk^n$.
- L'applicazione pubblica $\mathcal{F} := S \circ \mathcal{Q} \circ T : \Bbbk^n \to \Bbbk^m$, composta da m polinomi $p_1, \ldots, p_m$ che sembrano random.

Multivariate Cryptography

Supponiamo che Bob abbia costruito il suo schema multivariato e abbia dato la chiave pubblica $\mathcal{F} = \{p_1, \ldots, p_m\}$ a Alice.

1. Alice vuole inviare il messaggio $a \in \mathbb{k}^n$ a Bob. Calcola $b = (p_1(a), \ldots, p_m(a)) \in \mathbb{k}^m$ e lo manda a Bob.
2. Bob riceve b e calcola $w = S^{-1}(b)$.
3. Bob risolve il sistema $q_i(x) - w_i = 0$ e trova una soluzione $z \in \mathbb{k}^n$.
4. Bob calcola $a = T^{-1}(z)$.



Multivariate Cryptography: osservazioni

1. E se la soluzione del sistema $q_i(x) - w_i = 0$ non è unica? Bob potrebbe trovare un valore diverso di a!

Multivariate Cryptography: osservazioni

1. E se la soluzione del sistema $q_i(x) - w_i = 0$ non è unica? Bob potrebbe trovare un valore diverso di a!
   - Se $n < m$, è probabile che il sistema abbia soltanto una soluzione.
   - Se $n > m$, ci sono più soluzioni. In questo caso è meglio usare lo schema come una firma digitale (DS). Non è un problema se ci sono più firme valide per lo stesso documento.

Multivariate Cryptography: osservazioni

1. E se la soluzione del sistema $q_i(x) - w_i = 0$ non è unica? Bob potrebbe trovare un valore diverso di a!
   - Se $n < m$, è probabile che il sistema abbia soltanto una soluzione.
   - Se $n > m$, ci sono più soluzioni. In questo caso è meglio usare lo schema come una firma digitale (DS). Non è un problema se ci sono più firme valide per lo stesso documento.
2. Come scegliere i polinomi (quadratici) $q_1, \ldots, q_m$ in modo che siano facili *computazionalmente* da invertire, cioè tali che sia facile trovare $a \in \mathbb{k}^n$ tale che $q_1(a) = q_2(a) = \cdots = q_m(a) = 0$?

Matsumoto–Imai (1988)

Uno dei primi schemi multivariati è stato proposto da Matsumoto e Imai (1988).

- Estensione di campi $\mathbb{F}_q \to \mathbb{F}_{q^n}$ di grado n (q potenza di 2).
- Isomorfismo di spazi vettoriali $\phi : \mathbb{F}_{q^n} \xrightarrow{\cong} (\mathbb{F}_q)^n$.
- Prendiamo $\overline{\mathcal{Q}}(x) = x^{1+q^\alpha}$, polinomio univariato in $\mathbb{F}_{q^n}$ con $\gcd(1+q^\alpha, q^n-1) = 1$. Allora

$$\mathcal{Q} = \phi \circ \overline{\mathcal{Q}} \circ \phi^{-1}$$

  restituisce un sistema di polinomi multivariati (quadratici) su $\mathbb{F}_q$.

Matsumoto–Imai (1988)

Uno dei primi schemi multivariati è stato proposto da Matsumoto e Imai (1988).

- Estensione di campi $\mathbb{F}_q \to \mathbb{F}_{q^n}$ di grado n (q potenza di 2).
- Isomorfismo di spazi vettoriali $\phi : \mathbb{F}_{q^n} \xrightarrow{\cong} (\mathbb{F}_q)^n$.
- Prendiamo $\overline{\mathcal{Q}}(x) = x^{1+q^\alpha}$, polinomio univariato in $\mathbb{F}_{q^n}$ con $\gcd(1+q^\alpha, q^n-1) = 1$. Allora

$$\mathcal{Q} = \phi \circ \overline{\mathcal{Q}} \circ \phi^{-1}$$

  restituisce un sistema di polinomi multivariati (quadratici) su $\mathbb{F}_q$.
- L'applicazione $\overline{\mathcal{Q}}$ è invertibile (e quindi anche $\mathcal{Q}$)

$$\overline{\mathcal{Q}}^{-1}(x) = x^h$$

  con $h(1+q^\alpha) = 1 \bmod q^n - 1$.

Weil restriction

Questa procedura è chiamata restrizione degli scalari di Weil.

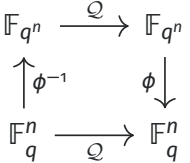
Esempio : $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ con $\alpha^2 = \alpha + 1$. Abbiamo $\mathbb{F}_4 \cong (\mathbb{F}_2)^2$ con base $\{1, \alpha\}$.

- $\overline{\mathcal{Q}}(x) = x^3 \in \mathbb{F}_4[x]$.
- Scriviamo $x = x_1 + \alpha x_2$ con due nuove variabili x_1 e x_2 su $\mathbb{F}_2$.
- Allora $\overline{\mathcal{Q}}(x)$ diviene

$$(x_1 + \alpha x_2)^3 = x_1^3 + \alpha x_1^2 x_2 + (1 + \alpha) x_1 x_2^2 + x_2^3$$

- Troviamo così il sistema su $\mathbb{F}_2$

$$\begin{cases} x_1^3 + x_1 x_2^2 + x_2^3 = 0 \\ x_1^2 x_2 + x_1 x_2^2 \end{cases}$$



Matsumoto–Imai (1988)

- Se q è una potenza di 2 e $\gcd(1+q^\alpha, q^n-1) = 1$, allora il polinomio univariato $\overline{\mathcal{Q}}(x) = x^{1+q^\alpha}$ è *invertibile*.
- Sia h un intero tale che $h(1+q^\alpha) = 1 \bmod q^n - 1$, allora $\overline{\mathcal{Q}}^{-1}(x) = x^h$.
- In effetti, abbiamo

$$\overline{\mathcal{Q}}^{-1}(\overline{\mathcal{Q}}(x)) = x^{h(1+q^\alpha)} = x^{1+k(q^n-1))} = x.$$

- Allora l'utilizzatore legittimo può trovare la soluzione del sistema $\mathcal{Q}$ componendo con l'isomorfismo ϕ e utilizzando $\overline{\mathcal{Q}}^{-1}$.

Matsumoto–Imai (1988)

- Se q è una potenza di 2 e $\gcd(1+q^\alpha, q^n-1) = 1$, allora il polinomio univariato $\overline{\mathcal{Q}}(x) = x^{1+q^\alpha}$ è *invertibile*.
- Sia h un intero tale che $h(1+q^\alpha) = 1 \bmod q^n - 1$, allora $\overline{\mathcal{Q}}^{-1}(x) = x^h$.
- In effetti, abbiamo

$$\overline{\mathcal{Q}}^{-1}(\overline{\mathcal{Q}}(x)) = x^{h(1+q^\alpha)} = x^{1+k(q^n-1))} = x.$$

- Allora l'utilizzatore legittimo può trovare la soluzione del sistema $\mathcal{Q}$ componendo con l'isomorfismo ϕ e utilizzando $\overline{\mathcal{Q}}^{-1}$.

Il crittosistema di Matsumoto–Imai è stato rotto da un attacco (attacco di linearizzazione), ma l'idea di usare un'estensione di campi per costruire sistemi polinomiali è stata usata in diversi schemi multivariati. Il più importante è **HFE (Hidden Field Equations)** (e le sue modifiche).

Oil and Vinegar (OV)

Lo schema Oil and Vinegar è stato proposto da Patarin (1997).

- $o, v \in \mathbb{Z} > 0$, $n = o + v$, $m = o$, $V = \{1, \ldots, v\}$, $O = \{v + 1, \ldots, n\}$.
- La funzione centrale è $\mathcal{Q} = \{f^{(1)}, \ldots, f^{(m)}\}$ con

$$f^{(i)} = \sum_{j,k \in V} \alpha_{jk}^{(i)} x_j x_k + \sum_{j \in V, k \in O} \beta_{jk}^{(i)} x_j x_k + \sum_{j \in V \cup O} \gamma_j^{(i)} x_j + \delta^{(i)}$$

  con $\alpha_{jk}^{(i)}, \beta_{jk}^{(i)}, \gamma_j^{(i)}, \delta^{(i)} \in \mathbb{F}_q$.
- Le $x_i : i \in V$ sono le variabili vinegar, mentre le $x_i : i \in O$ sono chiamate variabili oil.

Oil and Vinegar (OV)

Lo schema Oil and Vinegar è stato proposto da Patarin (1997).

- $o, v \in \mathbb{Z} > 0$, $n = o + v$, $m = o$, $V = \{1, \ldots, v\}$, $O = \{v+1, \ldots, n\}$.
- La funzione centrale è $\mathcal{Q} = \{f^{(1)}, \ldots, f^{(m)}\}$ con

$$f^{(i)} = \sum_{j,k \in V} \alpha_{jk}^{(i)} x_j x_k + \sum_{j \in V, k \in O} \beta_{jk}^{(i)} x_j x_k + \sum_{j \in V \cup O} \gamma_j^{(i)} x_j + \delta^{(i)}$$

  con $\alpha_{jk}^{(i)}, \beta_{jk}^{(i)}, \gamma_j^{(i)}, \delta^{(i)} \in \mathbb{F}_q$.
- Le $x_i : i \in V$ sono le variabili vinegar, mentre le $x_i : i \in O$ sono chiamate variabili oil.
- Non ci sono termini quadratici nelle sole variabili oil. Le variabili non sono completamente mischiate (come olio e aceto). Dopo l'applicazione della mappa lineare T, i polinomi pubblici diventano densi. La mappa esterna S non è usata. Si ha

$$\mathcal{F} = \mathcal{Q} \circ T.$$

Oil and Vinegar (OV)

Siccome $n = o + v > o = m$, lo schema è usato come firma digitale (DS).

1. Bob vuole firmare il messaggio $b \in \mathbb{F}_q^m$.

Oil and Vinegar (OV)

Siccome $n = o + v > o = m$, lo schema è usato come firma digitale (DS).

1. Bob vuole firmare il messaggio $b \in \mathbb{F}_q^m$.
2. Bob assegna dei valori casuali a $x_1, \ldots, x_v$, diciamo $c_1, \ldots, c_v$.

Oil and Vinegar (OV)

Siccome $n = o + v > o = m$, lo schema è usato come firma digitale (DS).

1. Bob vuole firmare il messaggio $b \in \mathbb{F}_q^m$.
2. Bob assegna dei valori casuali a $x_1, \ldots, x_v$, diciamo $c_1, \ldots, c_v$.
3. Bob cerca una soluzione del sistema lineare

$$f_i(c_1, \ldots, c_v, x_{v+1}, \ldots, x_n) = b_i \quad \forall i = 1, \ldots, m$$

Se il sistema non ha soluzione, assegna altri valori a $x_1, \ldots, x_v$.

Oil and Vinegar (OV)

Siccome $n = o + v > o = m$, lo schema è usato come firma digitale (DS).

1. Bob vuole firmare il messaggio $b \in \mathbb{F}_q^m$.
2. Bob assegna dei valori casuali a $x_1, \ldots, x_v$, diciamo $c_1, \ldots, c_v$.
3. Bob cerca una soluzione del sistema lineare

$$f_i(c_1, \ldots, c_v, x_{v+1}, \ldots, x_n) = b_i \quad \forall i = 1, \ldots, m$$

   Se il sistema non ha soluzione, assegna altri valori a $x_1, \ldots, x_v$.
4. Sia $c \in \mathbb{F}_q^n$, la soluzione trovata. Bob calcola $a = T^{-1}(c)$, che è la firma.

Oil and Vinegar (OV)

Siccome $n = o + v > o = m$, lo schema è usato come firma digitale (DS).

1. Bob vuole firmare il messaggio $b \in \mathbb{F}_q^m$.
2. Bob assegna dei valori casuali a $x_1, \ldots, x_v$, diciamo $c_1, \ldots, c_v$.
3. Bob cerca una soluzione del sistema lineare

$$f_i(c_1, \ldots, c_v, x_{v+1}, \ldots, x_n) = b_i \quad \forall i = 1, \ldots, m$$

   Se il sistema non ha soluzione, assegna altri valori a $x_1, \ldots, x_v$.
4. Sia $c \in \mathbb{F}_q^n$, la soluzione trovata. Bob calcola $a = T^{-1}(c)$, che è la firma.
5. Per verificare che la firma sia corretta, Alice deve semplicemente verificare che

$$\mathcal{F}(a) = b,$$

   dove $\mathcal{F}$ è la chiave pubblica.

Oil and Vinegar (OV): un esempio

- Scegliamo il campo $\mathbb{F}_5 = \mathbb{Z}_5$ e i parametri $o = v = 2$. Cioè $n = 4$ e $m = 2$.
- Siano x, y le variabili vinegar e z, w le variabili oil.
- I polinomi segreti $\mathcal{Q} = \{f_1, f_2\}$ di Bob sono

$$f_1 = 2x^2 + 2xy + 3xz + xw + 3y^2 + 3yz + 2yw,$$
$$f_2 = 4x^2 + 3xy + 2xz + 2xw + y^2 + yz + 4yw.$$

  Non hanno termini quadratici della forma z^2, zw, w^2.
- Bob sceglie la trasformazione lineare invertibile data dalla matrice

$$T = \begin{pmatrix} 2 & 2 & 3 & 3 \\ 2 & 4 & 4 & 0 \\ 1 & 1 & 4 & 2 \\ 1 & 1 & 2 & 0 \end{pmatrix}$$

Oil and Vinegar (OV): un esempio

I polinomi pubblici sono $\mathcal{F} = \mathcal{Q} \circ T$:

$$p_1 = x^2 + 4xy + 2xz + 2xw + 4yz + yw + z^2 + 4zw + w^2$$
$$p_2 = xz + 4y^2 + 4yz + 2yw + 2z^2 + 4zw + 3w^2.$$

Notiamo che nei polinomi della chiave pubblica compaiono monomi quadratici nelle variabili oil (z^2, zw, w^2), quindi apparentemente la chiave pubblica non ha più la stessa struttura della chiave privata.

Oil and Vinegar (OV): un esempio

I polinomi pubblici sono $\mathcal{F} = \mathcal{Q} \circ T$:

$$p_1 = x^2 + 4xy + 2xz + 2xw + 4yz + yw + z^2 + 4zw + w^2$$
$$p_2 = xz + 4y^2 + 4yz + 2yw + 2z^2 + 4zw + 3w^2.$$

Notiamo che nei polinomi della chiave pubblica compaiono monomi quadratici nelle variabili oil (z^2, zw, w^2), quindi apparentemente la chiave pubblica non ha più la stessa struttura della chiave privata.

1. Suppooniamo che Bob voglia firmare un documento $b = (3, 2)$ (*In pratica si firma l'hash di un documento*).
   Deve cercare $a \in \mathbb{F}_5^2$ tale che

$$(p_1(a), p_2(a)) = (3, 2).$$

Oil and Vinegar (OV): un esempio

2. Bob assegna dei valori casuali alle variabili vinegar, fissiamo $x = y = 1$.

Oil and Vinegar (OV): un esempio

2. Bob assegna dei valori casuali alle variabili vinegar, fissiamo $x = y = 1$.
3. Bob cerca una soluzione del sistema lineare

$$\begin{cases} f_1(1, 1, z, w) = 3 \\ f_2(1, 1, z, w) = 2 \end{cases} \Rightarrow \begin{cases} z + 3w + 2 = 3 \\ 3z + w + 3 = 2 \end{cases}$$

Il sistema ha una sola soluzione che è $z = 2$ e $w = 3$. Quindi Bob ottiene

$$c = (1, 1, 2, 3) \in \mathbb{F}_5^4.$$

Oil and Vinegar (OV): un esempio

2. Bob assegna dei valori casuali alle variabili vinegar, fissiamo $x = y = 1$.
3. Bob cerca una soluzione del sistema lineare

$$\begin{cases} f_1(1,1,z,w) = 3 \\ f_2(1,1,z,w) = 2 \end{cases} \Rightarrow \begin{cases} z + 3w + 2 = 3 \\ 3z + w + 3 = 2 \end{cases}$$

Il sistema ha una sola soluzione che è $z = 2$ e $w = 3$. Quindi Bob ottiene

$$c = (1,1,2,3) \in \mathbb{F}_5^4.$$

4. Bob calcola la firma

$$a = T^{-1}(c) = \begin{pmatrix} 2 & 2 & 3 & 3 \\ 2 & 4 & 4 & 0 \\ 1 & 1 & 4 & 2 \\ 1 & 1 & 2 & 0 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 \\ 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 4 \\ 3 \end{pmatrix}$$

Oil and Vinegar (OV): un esempio

5. Per verificare che la firma è corretta, Alice deve semplicemente verificare che $\mathcal{F}(a) = b$, cioè

$$p_1(0, 0, 4, 3) = 3, \quad p_2(0, 0, 4, 3) = 2.$$

Oil and Vinegar (OV)

- La proposta di Oil and Vinegar originale di Patarin aveva $v = o$ (il doppio di variabili rispetto alle equazioni). È stata rotta da Kipnis e Shamir.
- Scegliendo $v \approx 2o$, si ottiene l'Unbalanced Oil and Vinegar (UOV) che è considerato sicuro.
- Il problema di UOV è che la taglia delle chiavi è grande (bisogna memorizzare i coefficienti dei polinomi).
- Ci sono diverse varianti di UOV ancora in gara nel Round 2 di firme digitali del NIST: MAYO, QR-UOV, SNOVA, UOV.

Conclusioni

- La crittografia moderna si differenzia in crittografia simmetrica (a chiave segreta) e asimmetrica (a chiave pubblica).
- Gli schemi più usati a chiave pubblica (RSA, Diffie-Hellman,...) si basano sulla difficoltà computazionale di fattorizzare gli interi e del logaritmo discreto.
- Entrambi i problemi vengono risolti velocemente da un computer quantistico grazie all'algoritmo di Shor.
- Sono state sviluppate alternative (*post-quantum cryptography*) che si basano su problemi matematici differenti.
- Queste alternative stanno venendo selezionate e verranno presto messe in uso.

Conclusioni

- La crittografia moderna si differenzia in crittografia simmetrica (a chiave segreta) e asimmetrica (a chiave pubblica).
- Gli schemi più usati a chiave pubblica (RSA, Diffie-Hellman,...) si basano sulla difficoltà computazionale di fattorizzare gli interi e del logaritmo discreto.
- Entrambi i problemi vengono risolti velocemente da un computer quantistico grazie all'algoritmo di Shor.
- Sono state sviluppate alternative (*post-quantum cryptography*) che si basano su problemi matematici differenti.
- Queste alternative stanno venendo selezionate e verranno presto messe in uso.

La crittografia post-quantum è pensata per funzionare su computer *classici!*

Grazie!

Grazie!

Domande?

Bibliografia essenziale

Libri

1. D. Bernstein, J. Buchmann, et E. Dahmen
   Post-Quantum Cryptography
   Springer, 2009.
2. J. Hoffstein, J. Pipher, et J.H. Silverman
   An Introduction to Mathematical Cryptography
   Springer, 2014
3. D. Stinson et M.Paterson
   Cryptography, Theory and Practice, Fourth Edition
   Chapman & Hall CRC, 2019

Tesi di master

L'esempio di schema Oil and Vinegar è tratto da

4. S. Trebiani, *Breaking Rainbow: Analisi di Attacchi alla Crittografia Multivariata*, Università di Genova, 2024.

Università
di Genova