

Altre alternative a RSA


Emmanuela Orsini

Torino 2011. Crittografia a chiave pubblica: oltre RSA

Università degli Studi di Pisa

13 Maggio 2011

Introduzione

- Computer quantistico: computer funzionante in base alle leggi della meccanica quantistica
- Algoritmo polinomiale per la fattorizzazione, su computer quantistici
 -  P.W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM J. Comput., pp. 1484 – 1509, 1997.
- **Post-quantum cryptography**: crittosistemi a chiave pubblica in grado di resistere agli attacchi dei quantum computers.




Introduzione

- Computer quantistico: computer funzionante in base alle leggi della meccanica quantistica
- Algoritmo polinomiale per la fattorizzazione, su computer quantistici
 - 📄 P.W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”, *SIAM J. Comput.*, pp. 1484 – 1509, 1997.
- **Post-quantum cryptography**: crittosistemi a chiave pubblica in grado di resistere agli attacchi dei quantum computers.
- ▶ Attualmente ci sono alcune famiglie di crittosistemi che potenzialmente potrebbero resistere a tali attacchi:



Outline

- 1 Crittografia con i polinomi
 - Hidden Field Equations (HFE)
- 2 Crittografia con codici correttori d'errore
 - McEleice-Niederreiter
- 3 Crittografia sui reticoli
 - NTRU

1. Crittografia con i polinomi

-  T. Matsumoto, H. Imai, "A class of asymmetric cryptosystems based on polynomials over finite rings", IEEE International Symposium on Information Theory, Abstract of Papers, pp.131-132, September 1983.
-  T. Matsumoto, H. Imai, "Algebraic Methods for Construction of Asymmetric Cryptosystems", AAECC-3, Grenoble, France, 15-19 of June 1985.
-  T. Matsumoto, H. Imai, "Public Quadratic Polynomial-tuples for efficient signature-verification and message-encryption", EUROCRYPT'88, Springer-Verlag 1998, pp. 419-453.

Crittografia basata sui polinomi

Supponiamo Alice  voglia trasmettere a Bob  il messaggio $m = (m_1, m_2, \dots, m_n) \in \mathbb{F}_q^n$.

- Bob costruisce un sistema di l polinomi in $\mathbb{F}_q[x_1, \dots, x_n]$ che **sa risolvere**:

$$\mathcal{A}' : \begin{cases} f_1(x_1, x_2, \dots, x_n) = 0 \\ f_2(x_1, x_2, \dots, x_n) = 0 \\ \vdots \\ f_l(x_1, x_2, \dots, x_n) = 0 \end{cases}$$

▷ Il sistema \mathcal{A}' può essere visto come un' applicazione

$$\begin{aligned} f : \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q^l \\ x = (x_1, \dots, x_n) &\longmapsto y = (f_1(x), \dots, f_l(x)) \end{aligned}$$

Crittografia basata sui polinomi

Schemi basati su *“un’oscura rappresentazione di polinomi”*.



T. Matsumoto, H. Imai, H. Harashima, H. Miyakawa “Asymmetric cryptosystems using obscure representations of enciphering functions”, Natl. Conf. Re. On Inf. Syst., IECE Japan, S8-5, 1983.

Bob sceglie due trasformazioni lineari affini \mathcal{S} e \mathcal{T} :

$$\mathcal{S} : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n \quad \mathcal{T} : \mathbb{F}_q^l \longrightarrow \mathbb{F}_q^l$$

- Chiave pubblica: $(\mathcal{A} = \mathcal{S} \circ \mathcal{A}' \circ \mathcal{T})$
- Chiave privata: $(\mathcal{S}, \mathcal{A}', \mathcal{T})$
- Cifratura:



$$\xrightarrow{\mathcal{A}(m)}$$



- Decifratura:

$$m = \mathcal{A}'^{-1} \circ \mathcal{A}'(m) = \mathcal{A}'^{-1} \circ \mathcal{S}^{-1} \circ \mathcal{A} \circ \mathcal{T}^{-1}(m)$$

Hidden Field Equations (HFE)



J. Patarin, "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of Asymmetric Algorithms", Eurocrypt'96, Springer Verlag, pp. 33-48.

Sia $\mathbb{K} = \mathbb{F}_q$, q primo o $q = p^\alpha$, allora \exists un (unico) campo finito $\mathbb{F}_{q^n} = \mathbb{K}[x]/p(x)$, con $p(x)$ polinomio di grado n irriducibile su \mathbb{K} .

$\mathbb{F}_{q^n} \simeq \mathbb{K}^n \implies$ ogni $a \in \mathbb{F}_{q^n}$ può essere rappresentato come una n -upla $(a_0, a_2, \dots, a_{n-1})$ di coefficienti di un polinomio in $\mathbb{K}[x]/p(x)$.

Rappresentazione multivariata e univariata

Ogni funzione $f : \mathbb{K}^n \longrightarrow \mathbb{K}^n$ può essere scritta come:

- un polinomio univariato
- n polinomi multivariati in n variabili su \mathbb{K}

Hidden Field Equations (HFE)

Grado univariato e multivariato

Esempio: $\mathbb{K} = \mathbb{F}_2$ e $n = 3$

$$b = f(a) = a + a^3 + a^5 =$$

$$(a_2x^2 + a_1x + a_0) + (a_2x^2 + a_1x + a_0)^3 + (a_2x^2 + a_1x + a_0)^5 \pmod{x^3 + x^2 + 1} =$$

$$(a_2 + a_2a_1 + a_2a_0 + a_1)x^2 + (a_2a_1 + a_1a_0 + a_2)x + (a_0 + a_2 + a_1a_0 + a_2a_0)$$

$$\begin{cases} b_2 = a_2 + a_2a_1 + a_2a_0 + a_1 \\ b_1 = a_2a_1 + a_1a_0 + a_2 \\ b_0 = a_0 + a_2 + a_1a_0 + a_2a_0 \end{cases}$$

- se $b = f(a) = a^{q^s}$, allora tutti i $b_i = f_i(a_1, \dots, a_n)$ sono \mathbb{K} -lineari
- se $f(a) = \sum a^{q^s + q^t}$, allora gli f_i sono quadratici

Hidden Field Equations

Si prende $f : \mathbb{K}^n \rightarrow \mathbb{K}^n$ (**mappa centrale**) del tipo:

$$f(x) = \sum_{q^{\phi_{i,j}} + q^{\theta_{i,j}} \leq d} \beta_{i,j} x^{q^{\phi_{i,j}} + q^{\theta_{i,j}}} + \sum_{q^{\xi_k} \leq d} \alpha_k x^{q^{\xi_k}} + c$$

di grado al più d , $\phi_{i,j}, \theta_{i,j}, \xi_k \in \mathbb{N}$.

Generazione della chiave pubblica

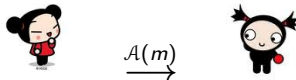
- Riscrivere come un sistema di n equazioni quadratiche:


$$\mathcal{A}' : \{f_i(x_1, \dots, x_n)\}_{i=1, \dots, n}$$

- scegliere due trasformazioni lineari affini \mathcal{S} e \mathcal{T} e considerare $(\mathcal{A} = \mathcal{S} \circ \mathcal{A}' \circ \mathcal{T})$ (**chiave pubblica**)

Hidden Field Equations

- Cifratura:



- Decifratura: Bob  deve invertire \mathcal{A}'^{-1} . Può sfruttare la conoscenza della chiave privata: poichè f è un polinomio univariato e di grado limitato d , può facilmente invertirlo (trovare una soluzione).



J. von zur Gathen, V. Shoup, "Computing Frobenius maps and factoring polynomials", Proceeding of the 24th Annual ACM Symposium in Theory of Computation, ACM Press, 1992.



P. van Oorschot, S. Vanstone, "A geometric approach to root finding in $GF(q^m)$ ", IEEE Trans. Info. Theory, 1989.

- ▷ È importante notare che f non è bigettiva, dunque possiamo trovare più di una soluzione a questa inversione (al più d).

Osservazioni ed attacchi ad HFE

Attacchi

- attacchi specifici a varianti di HFE



A. Kipnis, A. Shamir, "Cryptanalysis of the Oil and Vinegar signature scheme", in H. Krawczyk, editor *Advances in Cryptology, Crypto '98*, volume 1462 of LNCS, pages 257 – 266, Springer Verlag 1998.



H. Gilbert, M. Minier, "Cryptanalysis of SFLASH", in L. Knudsen, editot, *Advances in Cryptology, Eurocrypt '2002*, volume 2332 of LNCS, pages 288 – 298, Springer 2002.

- algoritmi per la risoluzione di sistemi multivariati di equazioni (\mathcal{A})



J.C. Faugère, A. Joux, " Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases", In Boneh Dan, editor, *Advances in Cryptology - CRYPTO 2003*, volume 2729 of Lecture Notes in Computer Science, pages 44-60, Springer Berlin / Heidelberg, 2003.

2. McEliece-Niederreiter



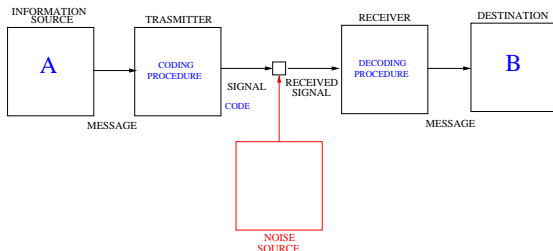
R.J. McEliece, "A public key cryptosystem based on algebraic coding theory", Technical report, Jet Propulsion Lab DSN Progress Report, 1978.



H. Niederreiter, "Knapsack-type cryptosystem and algebraic coding theory" *Problems of Control and Information Theory*, 15(2): 159 – 166, 1986.

Codici correttori d'errore

Schema di comunicazione



Codice lineare

Un **codice lineare** $[n, k]_q$ C su \mathbb{F}_q è un sottospazio di \mathbb{F}_q^n di dimensione k , $0 \leq k \leq n$. n è la **lunghezza** del codice, k la **dimensione**.

- Se C è un $[n, k]_q$, allora ogni matrice G $k \times n$, le cui righe sono una base per C come k -spazio vettoriale, è detta **matrice generatrice**.

$$v \in \mathbb{F}_q^k \implies vG \in C$$

Distanza di Hamming

Distanza di Hamming

$\forall v, w \in \mathbb{F}_q^n$, la **distanza di Hamming** $d_H(v, w)$ tra v e w è:

$$d(v, w) = \#\{i \mid v_i \neq w_i, 1 \leq i \leq n\}$$

- Hamming weight
- Sia C un $[n, k]_q$:

$$d_H(C) = \min\{d(a, b) \mid a, b \in C, a \neq b\}$$

Theorem

Sia C un $[n, k, d]_q$:

- C corregge fino a $t = \lfloor \frac{d-1}{2} \rfloor$ errori
- C trova $e = d - 1$ errori

- t è la **capacità di correzione** del codice

Matrici di parità e decodifica

Il codice C può essere definito tramite una matrice $(n - k) \times n$, detta **matrice di parità**.

$$\forall x \in \mathbb{F}_q^n, Hx^T = 0 \iff x \in C$$

Sia C un $[n, k, d]_q$ e siano $c, e, y \in \mathbb{F}_q^n$ rispettivamente la parola trasmessa, l'errore e il vettore ricevuto, allora $c + e = y$.

Dato y , applichiamo ad esso la matrice di parità H :

$$Hy^T = H(c + e)^T = He^T = s$$

Sindrome

Il vettore $s = Hy^T \in \mathbb{F}^{n-k}$ è detto **sindrome**.

Theorem

Se il numero degli errori è $\mu \leq t$, allora $\exists!$ errore corrispondente alla sindrome correggibile $s = He^T$.

Crittosistema di McEliece-Niederreiter: chiavi



● Chiave privata

- C codice lineare $[n, k, d]_q$ (con un algoritmo di decodifica efficiente) e una sua matrice di parità H
- S matrice $(n - k) \times (n - k)$ invertibile
- P matrice di permutazione $n \times n$



● Chiave pubblica

- $H_{pub}(= SHP)$

Osservazione: In McEliece C è un codice di Goppa binario. Originariamente Neiderreiter aveva proposto di usare un'altra classe di codici lineari, i codici GRS su \mathbb{F}_{2^m} , ma questa variante si è dimostrata debole.



V.M.Sidel'nikov, S.O. Shestakov "On cryptosystems based on generalized Reed Solomon codes", Discrete Mathematics, 1992. (in russo)

Cifratura e decifratura in McEliece-Niederreiter

● Cifratura

Sia $m \in \mathbb{F}_q^n$ di peso t , si calcola

$$c : m \mapsto s = H_{pub} m^T$$



$$s = H_{pub} m^T$$





● Decifratura






Bob riceve il crittogramma c che è $s = H_{pub} m^T = SHP m^T$

- calcola $S^{-1}s = HP m^T$
- $P m^T \in \mathbb{F}_q^n$ di peso t , dunque Bob può applicare un algoritmo di decodifica per C e trovare $P m^T$
- trova il messaggio m calcolando $m^T = P^{-1} P m^T$

McEliece-Niederreiter: osservazioni e sicurezza

- ▷ Dopo più di 30 anni il crittosistema di McEliece (nella sua forma originale) rimane sostanzialmente inviolato. La sua sicurezza si basa su due fattori:
 - problema della decodifica di codici lineari random (**NP-hard**)
-  E. Berlekamp, R. McEliece, H. van Tilborg “On the inherent intractability of certain coding problems”, IEEE Trans. on Inform. Theory, 24(3) : 384-386, 1978.
 - difficoltà nel recuperare la chiave privata, o almeno una equivalente.
- ▷ Sicuro contro attacchi quantistici
- Chiave pubblica molto grande
 - Per una sicurezza a 128-bit, prendendo un codice di Goppa binario $[2960, 2288]$ e $t = 56$, la dimensione della chiave pubblica è di **1534896** bits.
-  D.J. Bernstein, T. Lange, C. Peters, “Attacking and defending the McEliece Cryptosystem”, In PQCrypto, volume 5299 of LNCS, pp. 31-46, 2008.

3. Crittografia sui reticoli

-  M. Ajtai, "Generating hard instances of lattice problems", In Proc. of 28th STOC, pp. 99-108, ACM 1996.
-  M. Ajtai, C. Dwork, "A public-key cryptosystem with worst-case/ average-case equivalence", In Proc. of 29th STOC, pp. 284-293, ACM 1997.
-  O. Goldreich, S. Goldwasser, S. Halevi, "Public-key cryptosystem from lattice reductions problem", In Proc. of Crypto '97, volume 1294 of LNCS pp. 112-131, IACR, Springer-Verlag, 1997.
-  J. Hoffstein, J. Pipher, J.H. Silverman, "NTRU: a ring based public key cryptosystem", In Proc. of ANTSIII, volume 1423 pp. 267-288, Springer-Verlag 1997.
-  M. Caboara, F. Caruso, C. Traverso, "Lattice Polly Cracker cryptosystems", J. of Symb. Comput., 2010.

Lattices

Un **reticolo** in \mathbb{Z}^n (dunque un reticolo intero) è l'insieme di tutte le combinazioni lineari **interi** dei vettori della **base** (b_1, \dots, b_n) :

$$\mathcal{L} = \sum_{i=1}^n b_i \cdot \mathbb{Z} = \{Bx \mid x_i \in \mathbb{Z}, b_i \in \mathbb{Z}^n\}.$$

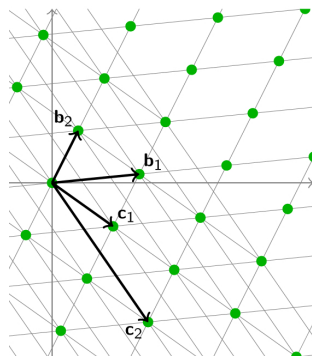
Lattices

Un **reticolo** in \mathbb{Z}^n (dunque un reticolo intero) è l'insieme di tutte le combinazioni lineari **interi** dei vettori della **base** (b_1, \dots, b_n) :

$$\mathcal{L} = \sum_{i=1}^n b_i \cdot \mathbb{Z} = \{Bx \mid x_i \in \mathbb{Z}, b_i \in \mathbb{Z}^n\}.$$

- ▷ $n =$ **dimensione**
- ▷ $B = [b_1, \dots, b_n] \in \mathbb{Z}^{n \times n}$
- ▷ Ogni reticolo ha molte basi

$$\mathcal{L} = \sum_{i=1}^n c_i \cdot \mathbb{Z}$$



Minimum Distance

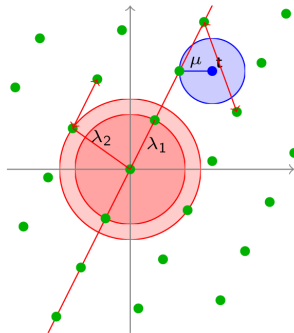
- **Distanza minima:**

$$\lambda_1 = \min_{x,y \in \mathcal{L}, x \neq y} \|x - y\|$$

$$\min_{x \in \mathcal{L}, x \neq 0} \|x\|$$

- **Distance function:**

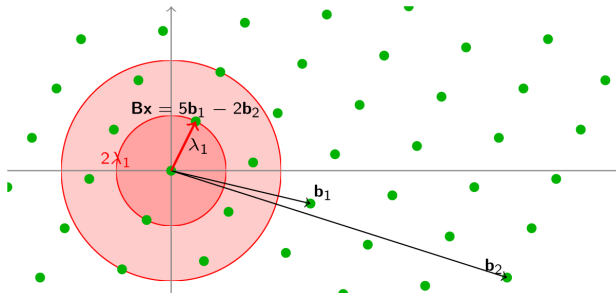
$$\mu(t, \mathcal{L}) = \min_{x \in \mathcal{L}} \|t - x\|$$



Lattice problems: SVP

Definition (SVP, Shortest Vector Problem)

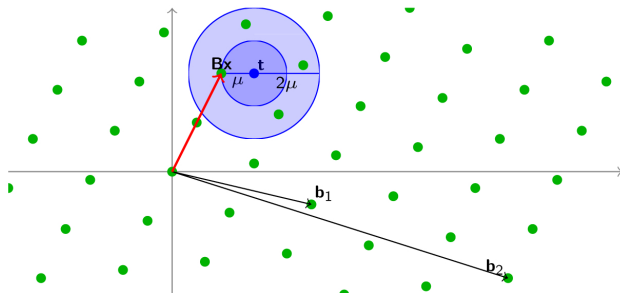
Data una base $B \in \mathbb{Z}^{n \times n}$ di \mathcal{L} , trovare il vettore non nullo del reticolo Bx (con $x \in \mathbb{Z}^n / \{0\}$) di lunghezza al più $\|Bx\| \leq \lambda_1$.



Lattice problems: CVP

Definition (CVP, Closest Vector Problem)

Data una base $B \in \mathbb{Z}^{m \times n}$ ed un vettore $t \in \mathbb{Z}^n$, trovare il vettore del reticolo Bx più vicino a t , i.e., cioè trovare un vettore intero $x \in \mathbb{Z}^n$ tale che $\|Bx - t\| \leq \mu$.



Problemi sui reticoli: SVP e CVP

- Le versioni esatte di questi problemi sono NP-hard.
- Algoritmi di riduzione classici (LLL, BKZ): gli algoritmi di riduzione producono “vettori relativamente corti” in tempo polinomiale.

Problemi sui reticoli: SVP e CVP

- Le versioni esatte di questi problemi sono NP-hard.
- Algoritmi di riduzione classici (LLL, BKZ): gli algoritmi di riduzione producono “vettori relativamente corti” in tempo polinomiale.



A. K. Lenstra, H. W. Jr. Lenstra, L. Lovász, “Factoring polynomials with rational coefficients, *Mathematische Annalen* 261 (4) : 515–534, 1982.

- Ridurre un reticolo vuol dire trovare una “buona base”, una base che permetta di approssimare problemi come lo SVP e il CVP, oppure di risolverli in modo esatto usando ulteriori procedimenti.

NTRU (Hoffstein, Pipher, Silverman (1998))

Notation and parameters

- $A = \mathbb{Z}[x]/(x^n - 1)$
- $p, q \in \mathbb{N}$ primi , $p \neq q$, p molto piccolo (2, 3)
- **Polinomi piccoli**: coefficienti piccoli (mod p), pochi monomi: peso Euclideo e di Hamming piccolo.
- **Polinomi moderati**: coefficienti piccoli (mod q),

Chiavi

Chiave privata



$f, g \in A$, f invertibile (mod q, p). f e g piccoli.

Chiave pubblica



$h = g/f \in A/(q)$

NTRU: cifratura e decifratura

Cifratura

Dato un messaggio $m \in A$ (polinomio piccolo), e un polinomio piccolo e random $r \in A$:

$$c = phr + m \pmod{q}$$



NTRU: cifratura e decifratura

Cifratura

Dato un messaggio $m \in A$ (polinomio piccolo), e un polinomio piccolo e random $r \in A$:

$$c = phr + m \pmod{q}$$



Decifratura

Si usa la seguente congruenza:

$$fc \equiv pgr + fm \pmod{q}$$

Se* $a = pgr + fm$ è un polinomio moderato, la congruenza è un'uguaglianza in $\mathbb{Z}[x]$. Dunque si riduce $a \pmod{p} \rightarrow \phi \equiv fm \pmod{p}$. A questo punto si divide per $f \pmod{p}$ e si ottiene m .

NTRU: cifratura e decifratura

Cifratura

Dato un messaggio $m \in A$ (polinomio piccolo), e un polinomio piccolo e random $r \in A$:

$$c = phr + m \pmod{q}$$



Decifratura

Si usa la seguente congruenza:

$$fc \equiv pgr + fm \pmod{q}$$

Se* $a = pgr + fm$ è un polinomio moderato, la congruenza è un'uguaglianza in $\mathbb{Z}[x]$. Dunque si riduce $a \pmod{p} \rightarrow \phi \equiv fm \pmod{p}$. A questo punto si divide per $f \pmod{p}$ e si ottiene m .

Osservazione:* bisogna stare attenti alla scelta dei parametri per garantire una corretta decifratura.

The Coppersmith-Shamir (or NTRU) lattice

NTRU può essere visto come un crittosistema sui reticoli:

- $A = \mathbb{Z}[x]/(x^n - 1) \cong \mathbb{Z}^n$ come gruppo abeliano;
- In A^2 , L_{CS} generato da $(q, 0)$ e $(h, 1)$ è un reticolo di rango pieno

$$L_{CS} = \begin{pmatrix} qI & 0 \\ H & I \end{pmatrix} = \begin{pmatrix} q & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & q & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & q & 0 & 0 & \dots & 0 \\ h_0 & h_1 & \dots & h_{N-1} & 1 & 0 & \dots & 0 \\ h_{N-1} & h_0 & \dots & h_{N-2} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ h_1 & h_2 & \dots & h_0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

The Coppersmith-Shamir (or NTRU) lattice

NTRU può essere visto come un crittosistema sui reticoli:

- $A = \mathbb{Z}[x]/(x^n - 1) \cong \mathbb{Z}^n$ come gruppo abeliano;
- In A^2 , L_{CS} generato da $(q, 0)$ e $(h, 1)$ è un reticolo di rango pieno

$$L_{CS} = \begin{pmatrix} qI & 0 \\ H & I \end{pmatrix} = \begin{pmatrix} q & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & q & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & q & 0 & 0 & \dots & 0 \\ h_0 & h_1 & \dots & h_{N-1} & 1 & 0 & \dots & 0 \\ h_{N-1} & h_0 & \dots & h_{N-2} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ h_1 & h_2 & \dots & h_0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

- ▷ **Key attacks:** $(g, f) \in L_{CS}$ ed è con molta probabilità lo SV
- ▷ **Message attack:** $[m, pr]$ è presumibilmente lo shortest residue of $[c, 0]$.

Crittosistema NTWO

 E. Orsini, C. Traverso, “Hybrid lattices and the NTWO cryptosystem”, preprint 2011.

- Generalizzazione in più variabili di NTRU:

$$A = \mathbb{Z}[x, y]/(x^n - 1, y^n - 1), \quad q, p \text{ primi}$$

- Chiave pubblica:

$$h = gf' + \alpha \quad \alpha \in A/q$$

- Chiave privata:

$$f, g, J = (\alpha, q) \subseteq A; \quad J \text{ ideale privato.}$$

The Lagrange-Coppersmith-Shamir lattice

- Reticoli ibridi

Un **reticolo ibrido** è un sottogruppo $L \subseteq \mathbb{Z}^n$ con metrica mista.

Grazie per l'attenzione!!