Estudi de l'esquema NTWE

Joan Carles Padilla

16 de Gener de 2024

Índex

Resum

El Procés d'estandardització NIST, encarregat de l'elaboració de normes i directrius de seguretat dels sistemes, va seleccionar quatre algorismes de criptografia post-quàntica basats en reticles on la seva seguretat es basa en la duresa dels problemes LWE i NTRU.

Les característiques principals son la seguretat i la eficiència en quant a la rapidesa per no alentir les comunicacions.

Els algorismes **LWE** i **NTRU**, han permès desenvolupar noves construccions de sistemes de clau asimètrica amb alts nivells de seguretat i per tant, de gran interès per la comunitat científica.

El sistema **NTWE** representa una d'aquestes noves construccions. En relació amb la seva seguretat, es pot estimar que el nivell es similar a la del problemes LWE i NTRU inclús amb un "*rank*" inferior.

L'objectiu d'aquest TFM es fer un anàlisi del sistema **NTWE** en quant a les ordres d'execució principals; generació de claus, encriptat i desencriptat. A nivell d'implementació, es fa un estudi de l'espai d'emmagatzematge de les claus i les millors combinacions per aconseguir un funcionament correcte així com anàlisi dels possibles atacs i nivells de seguretat.

Paraules clau; Criptografia, Reticles, LWE, NTRU, NTWE

1 Introducció

Aquest TFM desenvolupa els conceptes fonamentals de la criptografia post quàntica basada en reticles.

La primera part consisteix en una descripció dels Fonaments matemàtics necessaris per al coneixement dels problemes, seguit d'una descripció dels principis fonamental de la matemàtica reticular.

El següent capítol es centra en l'aplicació de la matemàtica reticular a la criptografia presentant els problemes més rellevants així com l'aplicació als problemes **LWE** i **NTRU** incloent una comparativa entre ells.

LWE es el problema basat en reticles anomenat *Problema d'aprenentatge amb Errors.* Aquest problema permet als criptosistemes on la seguretat es pot reduir a problemes de reticles, fer-ho sobre reticles generals.

NTRU Es el primer criptosistema basat en reticles i es basa en la dificultat per resoldre problemes de reticles dins d'un subgrup concret. A més, té un millor rendiment en comparació amb la criptografia clàssica, encara que la clau pública es més gran.

En base al coneixement del problemes LWE i NTRU, el capítol següent es centra en l'estudi del problema **NTWE**, basat en la seguretat i la duresa del problemes dels que depèn i tenint en compte el possibles atacs que pot tenir.

NTWE es una nova versió del criptosistema basat en el problema NTRU però menys estructurat i compacte, tot i que manté la flexibilitat de l'esquema basat en mòdul-LWE.

El capítol següent fa una implementació fent servir la programació phyton i l'anàlisi del programari amb pseudo codi que permet fer un estudi del càlcul del temps i recursos de memòria per al xifrat i desxifrat.

El programari NTWE es completament nou, ja que la proposta "NTWE - A Natural Combination of NTRU and LWE" d'en Joel Gärtner, no inclou cap prova pràctica ni disseny de programari per posar-ho en pràctica.

El programari es composa de la creació d'un parell de claus pública/privada i el xifrat i desxifrat d'un missatge.

Sobre aquest programari, es fan proves de les diferents mides de claus, test del temps de generació de claus i temps per xifrar i desxifrat un determinat text.

Al mateix tems, s'implementaran els problemes LWE i NTRU per fer una comparativa de mides de claus així com temps de xifrat i desxifrat per avaluar les millores i inconvenients amb respecte les propostes d'origen.

El capítol final conté les conclusions amb l'objectiu d'analitzar les possibles aplicacions del sistema NTWE, com per exemple, sistemes SCADA o l'Internet de les coses (IoT).

2 Fonaments

A continuació es descriuen els fonaments matemàtics bàsics necessaris per entendre el problemes LWE, NTRU i NTWE; grups, anells, cossos, espais vectorials i mòduls.

Seguidament, es fa una descripció bàsica per entendre els fonaments matemàtics dels reticles.

2.1 Fonaments matemàtics

2.1.1 Grups:

Un **Grup** es una estructura algebraica composta per un parell $(G, \cdot)$ on G es un conjunt no buit G i '$\cdot$' una operació interna definida a G que compleix les següents propietats:

- **Associativa**: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, per $\forall a, b, c \in G$

- **Element Neutre**: $\exists\ e \in G$ que acompleix $a \cdot e = e \cdot a = a\ \forall a \in G$

- **Element Oposat**: $\forall a \in G$, existeix una $a' \in G$ tal que $a \cdot a' = a' \cdot a = e$
L'element oposat a' també es diu **Simètric**

A més, es diu que G es **commutatiu o abelià** si, a més de les propietats anteriors, també acompleix la propietat commutativa:

$$a \cdot b = b \cdot a, \text{ per } \forall\ a,b \in G.$$

Un **Grup finit** es un conjunt G composat per un nombre finit d'elements.

2.1.2 Anells:

Un **anell** es defineix com un conjunt no buit amb dues operacions internes $(A, +, \cdot)$ anomenades *suma i producte* i relacionades entre si.

Els anells es defineixen com $A = (A, +, \cdot)$ i acompleixen les següents propietats:

- *(A, +)* es un grup **Abelià** respecte la suma.

- Propietat **associativa** del producte:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c), \forall \text{ a,b,c} \in \text{A}.$$

- Propietat **distributiva** del producte respecte la suma:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \forall a, b, c \in A,$$

$$(a + b) \cdot c = a \cdot c + b \cdot c, \forall a, b, c \in A.$$

Es diu que un anell es **unitari** o que té **l'element unitat** si acompleix la propietat de **l'element neutre per al producte**, es a dir:

$$\exists e \in A \text{ tal que } a \cdot e = e \cdot a = a, \forall a \in A$$

També es diu que l'anell es **commutatiu** si acompleix la **propietat commutativa del producte**, es a dir:

$$a \cdot b = b \cdot a, \forall a, b \in A$$

Un element a d'un anell $(A, +, \cdot)$ pot ser **invertible** si es simètric respecte de la operació multiplicació "$\cdot$", es a dir, si existeix un valor $b \in A$ que acompleix:

$$a \cdot b = b \cdot a = e \text{ (on } e \text{ es l'element neutre)}$$

Com exemple, un **Anell de Polinomis** es pot definir com una estructura d'anell amb les propietat indicades (grup abelià i propietats associativa i distributiva) i la propietat **commutativa**.

Matemàticament, un anell de polinomis s'expressa com:

$$A[x] = \{\textstyle\sum_{i=0}^{n} a_i x^i | n \in \mathbb{N} \cup \{0\}, a_i \in A, \forall i \in \{1, .., n\}\}$$

2.1.3 Cossos:

Es defineix un **cos** com un anell unitari $(A, +, \cdot)$ no buit amb dues operacions internes anomenades *suma i producte* definides a A.

Si l'anell $(A, +, \cdot)$ es commutatiu, es diu que el cos A també es commutatiu

amb element unitat i on tots els elements (excepte l'element nul) té el seu invers.

Els cossos han de complir les següents propietats:

- $(A, +)$ es un grup abelià (respecte la suma)

- $(A \setminus \{0\}, \cdot)$ es un grup abelià on el '0' es correspon amb l'element neutre de la suma.

- Propietat **distributiva** del producte respecte a la suma, es a dir:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \, \forall a, b, c \in K$$

2.1.4 Espais vectorials:

Un conjunt "V" es diu que té una estructura d'**Espai Vectorial** sobre un cos A si disposen de:

- Una operació interna 'Suma' + sobre V amb estructura de grup abelià; $(V, +)$

- Una operació externa 'Producte' $\cdot$ sobre V, es a dir: $K \times V \longrightarrow V$

El producte escalar ha de complir les propietats següents:

a) $(\alpha + \beta)v = \alpha v + \beta v$, $\forall \alpha, \beta \in K$, $\forall v \in V$.

b) $\alpha(v + w) = \alpha v + \alpha w$, $\forall \alpha \in K$, $\forall v, w \in V$.

c) $\alpha(\beta v) = (\alpha\beta)v$, $\forall \alpha, \beta \in K$, $\forall v \in V$.

d) $1 \cdot v = v$, $\forall v \in V$.

Tenint en compte que '1' es l'element neutre multiplicatiu de K.

Els elements de l'espai vectorial s'anomenen **vectors** i els elements del cos 'A' com **escalars**.

Per tant, els espais vectorials han de complir tant les operacions numèriques (escalars) com vectorials, es a dir; la suma i producte escalars i la suma i producte vectorials.

Una *Combinació Lineal* de vectors $v_1, v_2, .., V_n \in V$ es defineix com:

$$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n,$$

$$\text{on } \alpha_1 = \alpha_2 = ... = \alpha_n \in \mathbb{R}$$

El conjunt de vectors $v_1, v_2, .., v_n$ d'un Espai Vectorial "V"es **Linealment Independent** si la combinació lineal acompleix que:

$$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n = \mathbf{0}$$

$$\text{Únicament si } \alpha_1 = \alpha_2 = ... = \alpha_n = 0$$

Els Espais Vectorials es generen a partir de conjunts del tipus:

Generador: Es diu que X on $X \subseteq V$ es un espai generador de V si:

$$\forall v \in V,\ v \text{ es una combinació lineal dels elements de } X.$$

Base: B que acompleix $B \subseteq V$ es una base de V si es un conjunt linealment independent de V.

Una Base $B = v_1, ..., v_n$ es *Ortogonal* si s'acompleix que:

$$\forall v_i, v_j \in B, \text{ on } i \neq j, \text{ s'acompleix } < v_i, v_j >= 0$$

On $< v_i, v_j >$ equival al producte intern dels vectors.

2.1.5 Mòduls:

Un mòdul es una estructura algebraica fonamental.

Es diu que un Mòdul es a un anell el que un espai vectorial es a un cos. Per tant, un mòdul es un espai vectorial on el "**cos** de escalars"no es un cos, sinó un anell.

Tenint en compte que tot **cos** es també un **anell**, tot espai vectorial es un **mòdul**, però no a la inversa.

Un Mòdul M ha de complir les operacions de Suma i Producte per escalars de l'anell R.

$$M \times M \to M,\ (a,b) \longmapsto a+b;$$

$$R \times M \to M,\ (r,a) \longmapsto ra;$$

on $a,b,c \in M$ i $r,s \in R$.

Els mòduls han de contenir *l'element neutre*; $0 \in M$ per la suma i $1 \in R$ per al producte d'escalars.

Disposar *d'element oposat*; $-a \in M$ per la suma fent que $a+(-a)=0$

Es defineix R^n com un mòdul on els elements son vectors columna amb entrades a R.

La suma es defineix coordenada a coordenada i el producte es defineix multiplicant els escalars per totles les coordenades.

$$\begin{pmatrix} a_1 \\ . \\ . \\ . \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ . \\ . \\ . \\ b_n \end{pmatrix} = \begin{pmatrix} a_1+b_1 \\ . \\ . \\ . \\ a_n+b_n \end{pmatrix}, r \begin{pmatrix} a_1 \\ . \\ . \\ . \\ a_n \end{pmatrix} = \begin{pmatrix} ra_1 \\ . \\ . \\ . \\ ra_n \end{pmatrix}. \tag{1}$$

2.2 Fonaments Reticles

La introducció de la matemàtica basada en reticles a la criptografia post-quàntica té com objectiu principal la dificultat computacional dels problemes associats i el seu ús en la construcció de blocs per criptosistemes de clau pública, com LWE i NTRU.

La teoria de reticles també funciona com una eina bàsica per al criptoanàlisi de sistemes de clau pública, permetent analitzar possibles tipus d'atacs amb reticles a equacions polinòmiques, signatures digitals o variants de RSA.

Aquesta teoria, també es pot aplicar en la implementació eficient de sistemes de logaritme discret i com eina teòrica per l'anàlisi de seguretat de criptosistemes.

Matemàticament, un reticle Δ es defineix com un subgrup discret i additiu de $\mathbb{R}^n$, contingut dins $\mathbb{Z}^n$ i recobrint $\mathbb{R}^n$ ja que es considera un reticle enter i de rang complet.

Es diu que es *'Tancat'* respecte la suma, ja que per qualsevol suma o resta de dos valors que pertanyen al reticle Δ, el resultat també pertany al mateix reticle.

El reticle es defineix a partir de la seva 'Base' $\boldsymbol{B} \in \mathbb{R}^{(n+m)}$, composta per un conjunt de vectors ordenats, minimals i linealment independents de $\mathbb{K}^n$ de la forma $\mathbf{B} = \{b_1, ..., b_m\}$ quan $n \leq m$.

$$\Delta = \Delta(B) = \{B \cdot z | z \in \mathbb{Z}^m\} = B.\mathbb{Z}^m = \{\sum_{i=1}^{n} x_i.\mathbf{b}_i | x_i \in \mathbb{Z}\}$$

Es defineix el 'rang' o *'rank'* d'un reticle com el valor *'n'* i la *'dimensió'* d'un reticle com el valor *'m'*. Es a dir *dim(*Δ*)=m*

Quan $n = m$ es diu que el Reticle es de *rang màxim*.

La Base $\mathbf{B}$ d'un reticle Δ es una matriu $n \times m$ generada a partir dels vectors base b_i. Totes les files de les matriu Base son linealment independents.

Es defineix com *span* (o 'tram') d'un reticle *span*(Δ) a l'espai lineal 'travessat' (spanned) per als vectors d'aquest reticle.

El 'Determinant' d'un reticle $det(\Delta)$ correspon al volum n-dimensional del paral·lepíped fonamental d'un reticle depenent d'una base B.

El Paral·lepíped fonamental, $P(B)$ es genera a partir del 'tram' generat amb els vectors de la Base B.

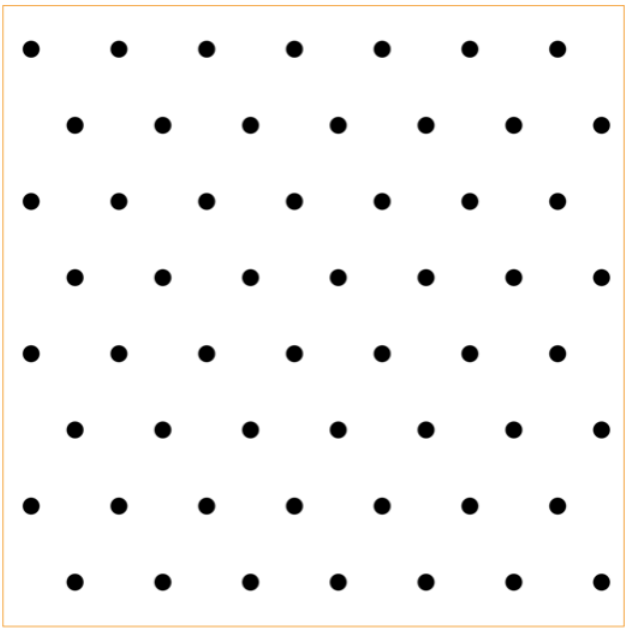
Simbòlicament, el determinant s'expressa com: $det(\Delta) := \sqrt{det(\boldsymbol{B}^T \boldsymbol{B})}$

En el cas que $n = m$, es diu que el determinant es de '*valor absolut*' i s'expressa com $det(\Delta) = |det(B)|$.

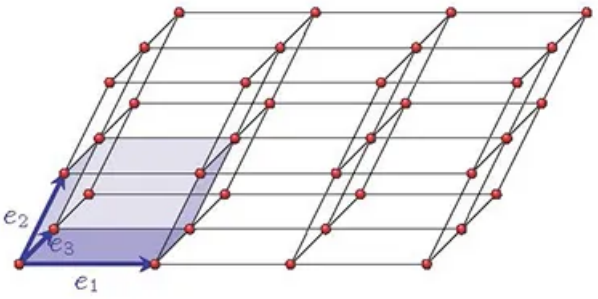
A nivell visual, un reticle es pot definir com una graella de punts dins d'un espai n-dimensional i amb una estructura periòdica.

Els reticles es generen a partir d'enters múltiples d'uns vectors base, per tant, un reticle poden tenir diferents bases.

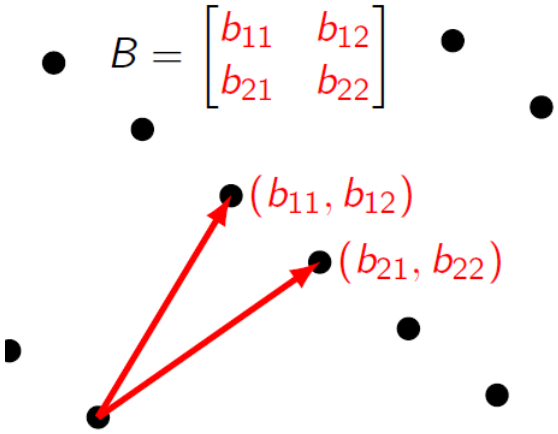
Els reticles es poden visualitzar en dos dimensions:



i també es poden representar en tres dimensions:



Els reticles també es poden representar com una matriu amb coeficients calculats a partir del vector Base B



Reticles q-aris:

Els reticles q-aris son de interès particular a la criptografia basada en reticles, ja que simplifiquen el principi de reticles mantenint les propietats associades a la seguretat i la complexitat computacional.

Sigui un reticle Δ en $\mathbb{R}^n$ i q un nombre enter primer. Degut a que els reticles son *tancats* respecte la suma, el vector $x \in \mathbb{Z}^n$ es troba al reticle q-ari si i només si $x \ mod \ q$ també es troba al Reticle.

Donats dos enters n, m, existeix una correspondència entre el codis lineals a $\mathbb{Z}_q^n$ i els reticles q-aris.

Donada una matriu $A \in \mathbb{Z}_q^{n \times m}$, amb $n \leq m$, es consideren dos reticles q-aris m-dimensionals de la forma:

$$\Delta_q^{\perp}(A) = \{y \in \mathbb{Z}^m : Ay = 0 \text{ mod q } \}$$

tal que $\mathbb{Z}_q^m \subseteq \Delta_q^{\perp}(A) \subseteq \mathbb{Z}^m$

Aquest primer es correspon al codi lineal amb matriu de verificació de paritat igual a $\boldsymbol{A}$ (mod q).

$$\Delta_q(A) = \{y \in \mathbb{Z}^m : y = A^T s \text{ mod q per un valor } s \in \mathbb{Z}^n$$

El segon es correspon al codi lineal generat per dues files de $\boldsymbol{A}$ (mod q).

Donat un reticle Δ, el reticle *dual* es defineix de la forma:

$$(\Delta_q^{\perp}(A))^* = \tfrac{1}{q}\Delta_q(A)$$

3 Problemes relacionats amb la Criptografia basada en Reticles:

El problemes següents es consideren computacionalment complexos, ja sigui de manera clàssica o quàntica.
Aquests problemes tenen com avantatge que totes les claus son difícils de trencar, ja sigui amb el cas més simple, com al més complicat, fent que la criptografia basada en reticles sigui difícil de trencar independentment de les possibles claus seleccionades.

No s'ha demostrat que hi hagin algoritmes quàntics capaços de resoldre aquests problemes amb l'ajuda d'un ordinador quàntic.

Els problemes es basen en la distribució gaussiana discreta i el problema de mostreig gaussià discret.

3.1 Problema vector més curt - (SVP)

La base d'aquest problema consisteix en trobar el vector més curt no nul definit com $\lambda(\mathbf{B})$, en base a un reticle Δ i la seva matriu base $\boldsymbol{B}$.

Es defineix com λ_1 la distancia mínima d'un reticle Δ equivalent a la longitud més curta d'un vector del reticle.

$$\lambda_1 = \min_{b \in \lambda(B)} ||b||$$

La versió 'Completa' del problema consisteix en trobar el vector v més curt, no nul, que pertany al reticle Δ creat a partir d'una base $\boldsymbol{B}$.

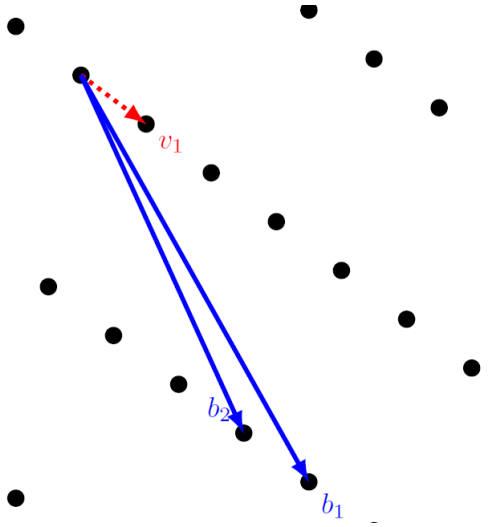
El càlcul consisteix en fer complir que la «norma» d'aquest vector sigui igual a la distancia mínima definida.

$$||v|| = \lambda_1(\Lambda)$$

Aquest càlcul es pot realitzar a partir del «teorema de Minkowski» on es pot calcular que existeix un vector $x \in \lambda_1(\Delta)$ on la 'norma' d'aquest vector

més curt es menor o igual a l'arrel quadrada de n pel determinant del reticle elevat a $1/n$.

Per contra, l'execució d'aquest algorisme es lent, ja que fa servir un temps exponencial per trobar la solució exacta.



Existeixen altres version simplificades, com SVP_γ o GapSVP_γ que consisteixen en afegir un paràmetre γ per trobar el vector v més curt (no nul).

Aquestes versions son més ràpides, pel fet que l'algorisme es basa en trobar una solució aproximada, fent servir menys temps exponencial.

3.2 Problema vector més proper - CVP

El problema CVP es basa en trobar el vector més proper a l'origen, per així obtenir el vector, no nul, més curt dins del reticle.

Per una base B, un reticle $\Delta(B)$ i un vector $w \in \mathbb{R}^n$; el problema consisteix en trobar el vector $v \in \Delta(B)$ més proper a w.

Donat un nombre real $r \in \mathbb{R}$, es tracta de decidir si la distancia entre el vector w i el reticle $\Delta(B)$ es més petit o igual o més gran que el nombre real r.

S'entén per distancia com: $dist(w, \Delta(\mathbb{B})) = min_{v \in \Delta(\mathbb{B})} ||w - v||$.

Cal trobar el nombre $r \in \mathbb{R}$ que acompleixi que $r = dist(w, \Delta(B))$.

Per fer-ho, cal trobar el vector "v" $\in \Delta(B)$ on la distancia sigui: $dist(w, v) \leq dist(w, \Delta(\mathbb{B}))$

Com al cas anterior, també existeixen versions aproximades CVP_γ i $GapCVP_\gamma$ on també s'afegeix un factor $\gamma = \gamma(n) > 1$ per fer un càlcul aproximat del problema.

- CVP_γ: Donada una base $\mathbf{B}$, el problema consisteix en trobar un vector v diferent de zero ($v \in \Delta$) que acompleixi: $||v|| \leq \gamma \cdot \lambda_1(\Delta)$

- $GapCVP_\gamma$: Donada la base $\mathbf{B}$ i un nombre real d, decidir entre:

$$\lambda_1(\Delta) \leq d \text{ o } \lambda_1(\Delta) > \lambda \cdot d.$$

Es pot comprobar que $GapCVP_\gamma$ té millor solució a mesura que el valor λ creix.

3.3 LWE: Learning With Errors (Regev, 2005)

"Learning With Errors" (LWE) es un criptosistema basat en reticles i relacionat amb la reducció quàntica del problema SVP (vector més curt) en el pitjor cas.

El problema **LWE** es basa en trobar un vector $\mathbf{s} \in \mathbb{Z}_q^n$ que acompleixi la fórmula $\mathbf{As + e = b}$ (mod q) on:

1. - sigui $q \in \mathbb{N}$ un valor primer.
2. - $n, m \in \mathbb{Z}$ que acompleixin $m > n$.
3. - Matriu $\mathbf{A} \in \mathbb{Z}_q^{mxn}$ aleatòria uniforme de mida mxn.
4. - Vector $\mathbf{e} \in \mathbb{Z}_q^m$: error donat de manera independent per la distribució de probabilitat X^m a $\mathbb{Z}_q^m$ amb mitjana 0 i desviació estàndard σ.
5. - $\mathbf{b} \in \mathbb{Z}_q^m$: Matriu resultant

El resultat del problema s'expressa com el parell (**A,b**)

3.3.1 Recerca LWE:

La recerca $LWE_{s,x}$ té com objectiu principal trobar un vector $\mathbf{s} \in \mathbb{Z}_q^n$, tal que, donats '$m$' vectors de $\mathbb{Z}_q^n$, $\overrightarrow{a_i}$ que corresponen a la matriu 'A', escollits de manera uniforme i independent així com 'm' escalars de $\mathbb{Z}_q, b_i$ que acompleixin la fórmula escalar: $b_i = As + e_i \ mod \ q$, on :

1. - A es una matriu $\in \mathbb{Z}_q^{mxn}$ composta per 'm' vectors a_i
2. - b es un vector $\in \mathbb{Z}^m$
3. - e vector error, donat per la distribució X^m i amb probabilitat $\mathbb{Z}_q^m$ amb amplitud α_q que es correspon amb un vector petit.

El problema **LWE** tindrà com resultat un parell (A, b)

$f : \Delta_q^n \cdot \mathbb{Z}^m \to \mathbb{Z}_q^m$

$(s, e) \rightarrow b^t = s^t A + e$

Representat gràficament, el punt dins del reticle es desplaça lleugerament del punt del reticle més proper.

El problema consisteix en trobar aquest punt més proper del reticle, que coincideix amb el valor 's' i que es correspon amb el punt dins de la circumferència i amb la «clau privada».

Sense l'error afegit, el problema es pot resoldre fàcilment fent servir la eliminació gaussiana.

3.3.2 Versions:

1.- **Ring-LWE**: Es basa en un anell R_q on totes les variables son polinomis d'un anell.

El parell (A, b) ve donar per:

1. - $A \in \mathbb{R}_q$
2. - $b = As + e \ mod \ q \ R$ amb:
   - $s \in R_q$
   - e obtingut de la distribució de probabilitat $X \ mod \ q$.

2.- **Mòdul-LWE**: El problema NTWE considera aquesta versió del problema, basada en el problema Ring-LWE.

Equilibri entre LWE estàndard i Ring LWE; estructura més reduïda comparat amb Ring-LWE però major escalabilitat.

Per missatges de mida fixa, el rendiment es similar als esquemes que es basen en Ring-LWE.

El problema Mòdul LWE es soluciona amb algorismes de reducció de Reticles sobre un o dos tipus de reticles diferents, que es corresponen amb el atacs a reticles Primari i Dual.

A la instancia Mòdul-LWE, s'utilitzen h mostres aplicades a les fórmules similars adaptades a Reticles, on:

- $\overline{A} \in R^{hn \times kn}$

- $\overline{b} = \overline{A}\overline{s} + \overline{e} \in R_q^h$

  on $\overline{e}$ son mostres de l'error de distribució Ψ

A la versió normal del problema, els elements $\overline{s}$ també es corresponen a mostres de Ψ

Avantatges de algorismes LWE: La seva eficiència en quant a la velocitat, mida de la clau i text de xifrat.

Desavantatges: Atacs eficient per la estructura addicional i que les compensacions entre seguretat i eficiència son escalables només de manera aproximada.

3.3.3 Propietats de LWE:

LWE disposa de dues propietats que, amb un algorisme que pot resoldre el problema de recerca LWE amb probabilitat 'p' d'encertar, es pot traslladar el secret 's' a un vector $t \in \mathbb{Z}_q^n$ per obtenir noves mostres.

A continuació, aplicant l'algorisme podem comprovar si la solució es correcta. En cas que no es trobi, es reitera el procés fins trobar la solució correcta, tenint en compte la probabilitat 'p'.

Les propietat son:

1. Facilitat per comprovar si un vector $s' \in \mathbb{Z}_q^n$ es correspon amb la solució.

Cal comprovar si $(b - s' \cdot A)$ dona una valor petit dins de $(-q/4, q/4)$

Aleshores, si $s \neq s'$, implica que $(b - s' \cdot A = s–s', A + e)$ s'estén de manera correcta a $\mathbb{Z}_q$, fent que alguns components de $(b - s' \cdot A)$ siguin grans (si es troben a l'interval $(-q/2, -q/4) \cup (q/4, q/2)$) i altres petits (si es troben a l'interval $-q/4, q/4)$

2. La mateixa solució LWE es pot obtenir traslladant el secret 's' a qualsevol $t \in \mathbb{Z}_q^n$, fent la translació.

3.3.4 Dificultat del problema LWE

La dificultat per resoldre el problema LWE es basa en la duresa «Hardness» d'aquest problema, i al mateix temps, en la dificultat per mostrejar la distribució gaussiana discreta o **DGS** (Discrete Gaussian Sampling).

El problema **DGS** es basa en trobar una mostra de la Distribució Gaussiana Discreta ($D_{\Delta,r}$) d'un reticle Δ de dimensió n i un valor real r on:

- Donat un enter $p \geq 2$ i un real $\alpha \in (0, 1)$.

- $r \geq \sqrt{2n} \cdot \eta_\epsilon(\Delta)/\alpha$

- $\alpha p > 2\sqrt{n}$

Existeix un algorisme quàntic eficient per resoldre la fórmula $DGS_{\sqrt{(2n \cdot \eta_\epsilon)}(\Delta)/\alpha}$ que utilitza l'oracle per resoldre LWE_{p,Ψ_α} per retornar una mostra de $D_{\Delta,r}$

Aquest problema es redueix als problemes SVP_γ i $GapSVP\gamma$ vists anteriorment, per tant, garanteix el 'hardness' quàntic.

3.3.5 Criptosistema de clau pública amb LWE

Es basa en el criptosistema de clau pública de Regev que fa servir la teoria de reticles i el problema LWE per xifrar i desxifrar informació de manera segura.

El sistema té en compte les següents variables:

- n : Paràmetre de seguretat del sistema.
- $q \geq 2$: Nombre primer entre n^2 y $2n^2$
- $m = (1 + \epsilon)$ *(1+n)log* q per $\epsilon > 0$ arbitrari.
- $\mathbb{A}$ matriu $\in \mathbb{Z}_q^{nxm}$ uniformement aleatòria sobre $\mathbb{Z}_q$
- Ψ_α : Distribució de l'error 'e', a "$\alpha < 1/n$ *logn*

Clau Privada

Es un vector $s \in \mathbb{Z}_q^n$ escollit aleatòriament uniforme.

Clau pública

Es calcula a partir de la clau privada fent: $b^t = s^t A + e^t$, on 'e' s'escull segons la distribució Ψ_α.

Per **xifrar** una missatge, es pren un valor secret efímer $x \in 0, 1$ per al xifrat de bit i es fa el càlcul següent:

$u = Ax$

$u' = b^t x + \lfloor bitq/2 \rfloor$

Per **desxifrar** el missatge rebut, es calcula la formula següent:

$s^t u = s^t Ax = (b^t – e)x = u' – ex$

i s'analitza la diferència: $d = u' – s^t$ on $u = ex + \lfloor bitq/2 \rfloor \ mod\ q$, que s'expressa dins l'interval $[-(q-1)/2, (q-1)/2]$

Si el **resultat** es troba entre: $-q/4 <= d <= q/4$, el bit encriptat era un '0'

En cas contrari, el resultat es un '1'.

3.4 NTRU

Aquest Criptosistema de clau pública basat en anell de polinomis va ser el primer que es va realitzar basant-se en la teoria de Reticles.

Referencia: Els autors son Hoffstein, Pipher i Silverman al 1998.

També es la primera construcció criptogràfica que fa servir «anells de polinomis», dins del que es coneix com «Reticles algebraicament estructurats».

La seva fortalesa es basa en la facilitat per resoldre el problema d'aquest reticle estructurat de manera eficient.

No es pot aplicar cap reducció coneguda a les versions del NTRU, per tant, no es pot trencar la seguretat semàntica del criptosistema.

Hi ha una variant del criptosistema NTRU basat en la dificultat de resolució de problemes de reticles dins d'un subgrup concret que inclouen el reticles de NTRU. L'inconvenient es la mida de la clau pública (Més gran que amb RSA)

NTRU es parametritza mitjançant un anell polinomial $R = \mathbb{Z}[X]/(f(X))$ *mod* q.

on:

1. $f(X) = (X^n - 1)$ on n es un valor primer
2. $f(X) = (X^n + 1)$ on n es una potencia de 2
3. Anell quocient $R_q = R/qR$, sent un valor imparell alt.
4. i sent q un valor enter, normalment en potencia de 2.

Procés de Generació de Claus:

Per generar la clau pública $h \in R$, es fan servir les variables $f, g \in R$ dos polinomis petits amb coeficients $\{-1, 0, 1\}$ on la major part dels valors son zero i una quantitat fixa petita diferent de zero.

La formula es la següent:

$$h \cdot f = 3g \ mod \ q$$

Que en notificació matemàtica, es pot expressar com:

$$h = 3g/f \ mod \ q \text{ a } \mathbb{Z}[x]/(x^n - 1)$$

La clau privada f i f_3 compleix que $f \cdot f_3 = 1 \ mod \ 3$

La clau s s'escull per que sigui invertible amb modul q i amb 2.

Procés de Xifratge:

Donada la clau pública $h \in R$ i el missatge $m \in R$ amb coeficients $\{-1, 0, 1\}$:

El càlcul consisteix en multiplicar h per un factor de cegat $r \in R$ amb coeficients $\{-1, 0, 1\}$ on la majoria dels valors son zero que codifica el missatge en coeficients mòdul q per obtenir el missatge xifrat c de la forma:

$$c = h \cdot r + m \ mod \ q$$

Per al Desxifratge:

Es realitza el càlcul inicial següent, multiplicant el missatge encriptat $c \in R_q$ per la variable f per obtenir:

$$a = f \cdot c = f \cdot (r \cdot h + m) = r \cdot 3g + f \cdot m \ mod \ q$$

Si tenim en compte que $h \cdot f = 3g \ mod \ q$ i es mouen tots els coeficients de a a valors entre $[-q/2, q/2]$.

Això funciona ja que tots els valors son suficientment petits, i per tant, es pot confirmar que $a = r \cdot 3g + f \cdot m$ a R, fent que es pugui recuperar el missatge de la forma:

$$m = a \cdot f_3 \ mod \ 3$$

Tenint en compte que $f \cdot f_3 = 1 \ mod \ 3$

3.4.1 Semblances i diferències entre LWE - NTRU:

Semblances:

La seguretat de la parametrització d'un criptosistema NTWE es basa en la seguretat dels criptosistemes NTRU i LWE.

El resultat d'aquesta parametrització es més eficient i compacta que el criptosistemes en els quals es basa, tot i que més complicat.

Diferències:

- Mides de les claus generades per la proposta NTWE.

Als problemes NTRU i LWE, la longitud de les claus públiques es calcula de manera diferent.

Així, si mentre a LWE la longitud depèn de manera lineal del rang del mòdul, amb NTRU la clau pública creix al quadrat del rang del mòdul, fent que, per exemple, sigui més gran que amb RSA, el que no el fa convenient per la encriptació amb clau pública.

En conseqüència, la clau pública de NTWE dependrà de la versió que es faci servir, variant entre 800, 1152 i 1536 bytes.

El càlcul es deriva d'una 'llavor' de 256 bits (32 bytes) que es considera suficient per representar la matriu de clau pública.

• Temps de generació de claus:

NTWE fa servir el mateix procediment que LWE per la generació de claus, això implica que es fa servir una llavor matriu, el que fa que la operació sigui més llarga que amb NTRU, on la clau es un element d'anell simple.

• Estudi del temps de generació de claus amb NTWE i el nombre de vegades que es fa servir la mateixa clau pública dintre d'un marge acceptable.

El temps que utilitza NTWE es similar al del sistema NTRU, ja que permet el càlcul invers de: f_q^-1

• Temps per xifrar i desxifrar un missatge.

NTWE es basa en l'esquema LWE de Linder-Peikert per l'encriptat i en NTRU per al desencriptat.

La comparació dels temps de xifrat i desxifrat es una tasca complicada, ja que depèn de l'algoritme utilitzat per les convolucions cícliques i negatives.

Al projecte es faran servir les tècniques general de multiplicació NTT (Number Theoretic Transform), encara que NTRU no el consideri.

4 El problema NTWE

Aquest TFM es basa en descriure el problema NTWE i en la creació d'un nou criptosistema basat en Reticles que combina els problemes NTRU i LWE de manera natural però mantenint una duresa "hardness"pròpia.

En aquest aspecte, la duresa o seguretat del criptosistema NTWE es pot considerar superior a la dels problemes LWE i NTRU, donant com resultat que el rendiment es comparable amb els esquemes basats en reticles.

El problema NTWE, en matèria de 'rank' "k", es pot considerar tant dur com el rank "k+1"del problema mòdul-LWE. A més, una versió més estructurada de NTWE es tan dur com el rank "k+1"del problema NTRU.

A més, com es veurà a la part d'implementació, el criptosistema basat en NTWE es una versió més compacta i estructurada del problema mòdul-NTRU i amb la flexibilitat de l'esquema basat en mòdul-LWE.

El problema NTWE es basa en les següents parts:

Distribució NTWE

Es considera una distribució de instancies del problema quan el vector secret s i l'element secret f es mostren a la distribució d'error.

Una mostra de la distribució NTWE $W(\bar{s}, f, \Psi)$ on Ψ es una distribució de R_q es dona per:

$$(\bar{a}, b = (\bar{a} \cdot \bar{s} + e)f^{-1}) \in R_q^k \times R_q$$

on:

q es un valor primer, k un enter i n un valor potencia de 2.

$R = \mathbb{Z}[X]/(X^n + 1)$

Ψ una distribució sobre R_q

$\bar{a} \leftarrow U(R_q^k)$

$e \leftarrow \Psi$

Es considera una distribució mitjana de casos del problema de instancies on el vector secret $\bar{s}$ i l'element secret f corresponen a mostres de la distribució d'error Ψ.

Decisió problema NTWE

La decisió DTNWE(Ψ, h) es dona a partir d'una distribució desconeguda D que pot ser tant aleatòriament uniforme com una distribució $W(\bar{s}, f, \Psi)$. El problema es basa en determinar quin es el cas on donat un màxim de h mostres d'una distribució desconeguda.

Recerca problema NTWE Si Ψ es una distribució sobre R_q i h es un enter, la instancia de recerca consisteix en recuperar $\bar{s}X^i$ i fX^i per una donada i quan es donen al menys h mostres de la distribució $W(\bar{s}, f, \Psi)$.

4.1 Comparació Mòdul LWE i NTWE

El criptosistema basat en NTWE es més resistent al atacs "Reticle dual"que el sistema basat en mòdul LWE.

Els atacs habituals al sistema mòdul LWE son de tipus "Reticle primari" i "reticle dual", sent el dual el més eficient a atacs a reticles.

En quant a la probabilitat d'errors de desxifratge, NTWE es més eficient que el mòdul LWE si es fa servir valors inversos no trivials de les funcions.

4.2 Comparació Mòdul NTRU i NTWE

El criptosistema basat en NTWE es més compacte que el problema basat en mòdul-NTRU i igual de sobre carregat.

La similitud amb el problema NTRU es que una instància del problema NTWE es de la forma:

$$h = g \cdot f^{-}1, \text{ on } g \leftarrow \Psi_1 \text{ i } f \leftarrow \Psi_2$$

En canvi, no es fa servir la igualtat de distribucions gaussianes $\Psi_1 = \Psi_2$ sinó que Ψ_1 s'utilitza una distribució basada en mòdul LWE i, per tant, les

mostres de la distribució son difícils de diferenciar entre valors uniformement aleatoris.

La clau pública dels problemes NTWE i NTRU es una mostra de les distribucions basades en una instancia del problema NTRU.

4.3 Atacs als sistema NTWE

Degut a la similitud de NTWE amb els problemes NTRU i LWE, l'estudi dels possibles atacs es centralitza en analitzar els seus possibles atacs més comuns; atacs Primar i Dual. De totes formes, no es descarta que puguin haver altres més eficients no considerats.

Igualment, es considera que qualsevol millora als atacs del problema NTWE també suposaràn una millora en el coneixement dels problemes dels que deriva.

A continuació es descriuen el possibles atacs; primari i dual, que es poden fer al problema LWE, que també son vàlids per al problema NTWE.

4.3.1 Atacs Primaris

Els atacs primaris al problema NTWE fan servir la mateixa construcció de reticle que per als atacs al problema LWE.

L'atac primari al problema LWE comença per la recerca del vector més curt al reticle generat i fa servir dues matrius $A \in \mathbb{Z}^{hn \times kn}$ i $B \in \mathbb{Z}^{hn \times n}$

Encara que pugui semblar que el reticle NTWE es similar al reticle donat per una instancia mòdul LWE amb *rank k*, realment, hi han diferències; Encara que tinguin la mateixa forma i determinant, el reticle mòdul LWE rank k té vectors objectius més curts que als reticles NTWE. Això demostra que la "duresa"del *rank k* del problema NTWE es més comparable al *rank k+1* del problema mòdul LWE.

Es pot considerar que el problema NTWE es més estructurat que la versió *rank k+1* del problema mòdul LWE ja que el reticle del mòdul NTWE es una

dimensió més petita que la corresponent al reticle *rank k+1* del mòdul LWE, i la matriu $\tilde{A}$ no es genera de la mateixa manera, ja que no pren mostres uniformes del problemes de reticles.

En conclusió, l'atac primari contra el problema *rank k* NTWE i contra el *rank k+1* mòdul LWE requereix aproximadament la mateixa càrrega.

A més, el reticle NTWE conté diversos vectors curts que abasten un espai n dimensional del sub-reticle que semblen ser la raó dels atacs contra paràmetres d'un NTRU sobrecarregat i diferent de NTWE.

4.3.2 Atacs Duals

Encara que es possible fer atacs de tipus dual al problema NTWE, no sembla més eficient que l'atac primari contra algunes parametritzacions del sistema.

Per tant, es té en compte per al càlcul de la duresa "concrete hardness" a instancies específiques de NTWE.

L'atac dual a NTWE es realitza de forma similar al que es fa amb el problema LWE, fent servir un vector curt al reticle.

$$L^{\perp} = \{(x, y) : xA = y \ mod \ q \ \}$$

Si un atac dual es produeix, el problema consisteix en que no es pugui resoldre el valor $L^{\perp}$ donats uns certs valors (x, y)

En relació al problema NTWE i als NTRU i LWE, no es fàcil comparar l'atac primari amb el dual.

Tan sols es pot demostrat que l'atac de reticles dobles al problema NTWE es menys eficient que l'atac primari, excepte per certes eleccions de paràmetres.

4.4 Seguretat

La seguretat del criptosistema NTWE es basa en al fortalesa del problema NTWE i del mòdul LWE. La fortalesa del problema NTWE es basa en no fer distingible la clau púbica dins d'una aleatorietat uniforme.

L'emmascarament complet del missatge encriptat també es similar al criptosistema basat en NTRU, on la clau es genera de forma pseudo-aleatòria mentre que la seguretat del text xifrat recau en la fortalesa de la varien del problema ring-LWE.

5 Implementació

Aquest TFM inclou una part pràctica realitzada amb programació Python amb l'objectiu de dissenyar un programari que permeti la generació de claus, encriptació d'un missatge aleatori i posteriorment el seu desencriptat fent servir les instruccions proposades per Joel Gärtner al document "**NTWE - A Natural Combination of NTRU and LWE**".

El programari definitiu es una combinació de diversos subprogrames on s'han fet servir diferents tipus d'arrays, des de funcions polinòmiques fins a llistes senzilles de valors.

Finalment, la versió entregada no inclou programació amb l'ús del paquet genèric "Numpy". Tot i que es molt completa i permet fer càlculs científics computacionals de manera molt més simple, he preferit generar els "arrays" amb dimensions variables de forma senzilla, tant per matrius com anells de polinomis.

D'aquesta forma es simplifiquen els càlculs que es poden fer entre ells.

Igualment, per omplir les dades dels arrays, he fet servir diferents versions on es combina les distribucions únicament aleatòries (random) amb distribucions gausianes uniformes.

El valors també s'han modificat per treballar amb valors enters (sobretot en la distribució de l'error) i no únicament naturals.

En quant al disseny del programari; m'he basat en programari Python ja disponible a GitHub i l'he modificat per adaptar-ho a les especificacions de NTWE.

Respecte a "**Mòdul-LWE**", m'he basat en varis programaris amb codi "*LWE*"

i "*Ring-LWE*" amb l'objectiu principal de dissenyar el procediment de Generació de Claus.

NTRU es un programa "de codi obert" amb dos algorismes principals anomenats *NTRUencrypt* i *NTRUdecrypt*.

Els propietaris Hoffstein, Pipher i Silverman han realitzat una implementació d'aquests algorismes i també estan disponibles GitHub.

L'algorisme NTRU es fa servir principalment a les fases de Encriptació i Desencriptat.

La diferencia principal de l'algorisme **NTWE** respecte NTRU i Mòdul-LWE son:

1. Modificació dels algorismes originals afegint opcions que afegeixen més seguretat sense modificar la eficiència computacional.
2. Combinació dels dos algorisme segons el procés.
3. Modificació de les distribucions utilitzades als polinomis (sobretot NTRU)
4. Modificació dels valors, en quant a mida i contingut.

A continuació es detallen els procediments per la generació de claus que permeten encriptar i desencriptar missatges.

Es considera el cas on R es un anell d'enters en un camp ciclotrònic de potencia dos i $p = 2$

Generació de claus

Al seu document, en Joel indica que per la implementació de l'encriptat, fa servir la versió "Normal-form decision Module-LWE", on fa servir un valor valor primer 'q', un anell de enters 'R' per un camp numèric 'K' i una distribució sobre R_q simbolitzada com Ψ.

L'objectiu consisteix en distingir mostres des de $A_{\overline{s},\Psi}$ uniformement aleatòries a $R_q^k \times R_q$, quan $\overline{s}$ es un vector amb element mostrejats des de Ψ.

1. Donada una matriu $\overline{A} \leftarrow U(R_q)^{h \times k}$ mostrada a partir d'un generador pseudo-aleatori
2. $\overline{s} \leftarrow \Psi_{gen}^{k}$
3. $\overline{e} \leftarrow \Psi_{gen}^{h}$
4. $f \leftarrow \Psi_f$

Es calcula $b = (\overline{A} \cdot \overline{s} + \overline{e}) \cdot f^{-1} \in R_q^h$, on f_p^{-1} es l'invers de f a R_p

El càlcul retorna: Clau pública: $pk = (\overline{A}, \overline{b})$, on $\overline{A}$ es un matriu generada de forma pseudo-aleatòria i $\overline{b}$ un vector.

Clau Privada: $sk = (\overline{s}, f, f_p^{-1}))$

La dificultat en quant a la programació d'aquest procediment, es basa en fer treballar conjuntament l'algorisme LWE basat en Lindner-Peikert però afegint la inversa d'una distribució gaussiana f.

Aquest algorisme es més simple que l'algorisme de Regev, però manté el mateix nivell de seguretat.

Per la creació de f, es fa servir la fórmula indicada $f = p \cdot f' + 1$, on $f' \leftarrow \Psi_{gen}$. Com càlcul, per la generació del polinomi f, es fa servir una distribució uniforme de valors.

Encriptat

Un cop generades les claus, es procedeix a encriptar el missatge a partir de la clau pública "pk" i les variables addicionals.

Sent:

1. $\overline{s}' \leftarrow \Psi_{enc}^{h}$
2. $e' \leftarrow \Psi_{enc}$
3. $\overline{e}'' \leftarrow \Psi_{enc}^{k}$

Es calcula el valor de retorn ct com, $ct = (c_1, \overline{c}_2) \in R_q \times R_q^k$, on els valors c_1 i $\overline{c}_2$ es calculen com:

$$c_1 = \overline{s}' \cdot \overline{b} + e' + \lfloor mq/p \rfloor$$

$$\overline{c}_2 = \overline{s}' \cdot \overline{A} + \overline{e}''$$

Per fer el procés d'encriptació, faig servir el mètode bit a bit amb valors "0" i "1" escollits de manera aleatòria.

En aquest procés, NTRU no es considera adequat per la encriptació, degut a la mida de la seva clau pública (creix en potencia de 2 respecte al rang del mòdul).

Per tant, aquest procés d'encriptació es basa principalment en les variables i la fórmula utilitzada a *Mòdul-LWE* per encriptar valors amb la diferència principal que es modifiquen les fórmules per al càlcul de les variables encriptades c_1 i c_2.

Per encriptar el missatge generat de forma aleatòria, es calcula per separat $\overline{c}_1$ que correspon a la part b a partir de les mostres finals de "Mòdul-LWE" més $\lfloor mq/p \rfloor$.

$\overline{c}_2$ es calcula també a partir d'un part de b sobre k de les mostres agafades sobre "Mòdul-LWE".

La part $\overline{\mathbf{a}}$ del mòdul-LWE s'escull agafant mostres de la matriu $\overline{\mathbf{A}}$ per la clau pública.

La part final de $\overline{\mathbf{a}}$ per les mostres de mòdul-LWE també serveix per generar la part $\overline{\mathbf{b}}$ de la clau pública.

La clau pública resultant, a diferencia del problema "mòdul-LWE' on el resultat es la concatenació d'un vector i un valor fixe, al problema "NTWE" c_1 i c_2 son dos vector.

Les proves realitzades confirmen que el missatge encriptat difereix completament de l'original, tant en mida com en contingut.

Desencriptat

Per desencriptar el missatge rebut, calen la combinació c_1 i c_2 i la clau privada "sk" generada a la fase de generació de claus.

1. Es realitza el càlcul de v com:

   $v = c_1 \cdot f - \overline{c}_2 \cdot \overline{s}\ mod\ q$

   v s'interpreta com l'element a R amb coeficients a $\lfloor 0, q)$

2. i es calcula u com un valors dins de R_q:

   $u = \lfloor v \cdot p/q \rceil$ interpretat com un element a R_p

3. Es resultat final es el càlcul:

   $v f_p^{-1} \in R_p$

Aconseguir un correcte desencriptat del missatge original correspon al punt amb major complexitat de la programació d'aquest algorisme criptogràfic "NTWE".

El motiu principal està relacionat amb el fet de fer servir la funció f^{-1} durant l'encriptat i posteriorment f i f_p per desencriptar juntament amb la modificació de les fórmules c_1 i C_2 respecte a l'algorisme "mòdul-LWE" estàndard per generar el missatge desencriptat definitiu.

Es té present que el resultat final ha de ser un valor enter entre $\{0, 1\}$ i que s'ha de correspondre amb el mateix valor utilitzat durant el procés d'encriptació.

La diferència principal en comparació amb l'algorisme "Mòdul-NTWE" es basa en com aconseguir aquest resultat final.

L'algorisme "Mòdul-LWE" original rep un vector u i un valor fixe v.

Mitjançant la formula i arrodonint el valor final a mòdul 2, s'aconsegueix en resultat esperat (valors $\{0, 1\}$)

5.1 Paràmetres i proves

valors de p diferents de 2 La modificació del paràmetre p amb valors diferents de"2", no suposa un retard addicional en la creació de les claus pública i privada.

En canvi, sí que suposa un retard considerable en el càlcul de la funció inversa f^{-1}.

A mesura que aquest valor augmenta, el temps per fer el càlcul invers s'incrementa considerablement.

Cal valorar valors de menys de 4 xifres per tenir un temps de càlcul raonable.

Marges d'error 'e'

El mes senzill es fer servir l'error como valor 0. Aquesta opció, encara que es la més vulnerable, permet verificar el correcte funcionament del programari.

Els valors d'error més utilitzats, han sigut entre 0 i 1,

Càlcul matriu inversa 'f^{-1}'

El valor primer q afecta directament al càlcul de la funció f i sobretot del seu invers f^{-1}.

Un valor molt gran (a partir de 10 nombres), el càlcul de la inversa va gairebé inviable l'execució d'aquest algorisme.

Inclús, provant diferents mètodes de càlcul de l'invers, aquest procediment s'esdevé molt llarg.

Mides de les claus La mida de les claus privada i pública utilitzada als diferents algorismes es un factor important a considerar en quant a la mida dels arxius que poden generar.

En la comparativa feta entre el tres sistemes, el que surt pitjor parat en quant a la mida es l'algorisme NTRU i més concretament en relació a la mida de l'arxiu que conté la clau pública, ja que la mida de l'arxiu corresponent creix exponencialment a mesura que augmenta el rang.

Com algorisme intermedi es troba NTWE. La clau pública es més gran a la de "mòdul-LWE", degut a que conté més informació del valor encriptat.

A nivell de clau privada, tots tres sistemes tenen en comú que la mida en fixa; sent NTRU l'algorisme amb l'arxiu corresponent més gran, seguit de

NTWE, degut a que conté tres valors $(s, fif_p^{-1}$.

Mòdul-LWE es la solució amb la mida de les dues claus més petita. Tot i així, cal tenir present que la mida no es fixa, sinó que depèn dels paràmetres des configuració, especialment en relació al valor que representa la mida dels vectors i matrius.

5.2 Eficiència

Comparat amb Mòdul-LWE

Es pot comprovar que, comparant el rank $k + 1$ de l'algorisme basat en Mòdul-LWE amb el de NTWE, no es necessari que les dades de la matriu **A** siguin uniformement aleatòries. La manera de verificar-ho, es modificant el programari a la part de generació de la Matriu **A** limitant el valor mínim i màxim.

D'aquesta manera, es pot jugar una mica amb la uniformitat de la matriu i verificar que el resultat, comparat amb la programació Mòdul-LWE (pujant el valor rank), es similar en quan a resultat i temps d'execució.

Comparat amb NTRU

La comparació amb NTRU, gràcies a la programació disponible, es fàcil fer una comparació.

L'avantatge principal de NTRU es la seva velocitat de generació de claus, encriptació i desencriptat.

Es pot dir, que sense tenir en compte el càlcul de f^{-1}, el temps d'execució es similar en tots dos sistemes.

El punt negatiu del sistema NTRU es la mida de la clau pública, que el fa inviable per l'ús en sistemes criptogràfics asimètrics.

Gestió dels temps d'execució

El programari inclou tot un seguit de línies de codi dedicades al càlcul dels temps parcials; generació de claus, temps d'encriptat i temps per desencrip-

tar.

Aquests càlculs ens permeten analitzar i comparar el temps a mesura que es modifiquen les variables del sistema.

La conclusió general, comparat amb el sistemes NTRU i Mòdul-LWE es que el temps computacional es molt similar en tots tres casos.

Val a dir que aquest càlcul depèn de les capacitats computacionals de l'equip on s'executin, especialment a microprocessador amb capacitats d'execució limitades i poc espai de memòria.

Es demostra que NTWE té una bona combinació de tamany de claus, temps d'execució i capacitat de memòria per instalar-se en aquests tipus de dispositius.

6 Conclusions

Un cop realitzats els test d'implementació, parametrització i comparació de programari, la conclusió principal es que el criptosistema basat en **NTWE** pot ser tan eficient a nivell de duresa com els esquemes en els quals es basa; mòdul-LWE i NTRU.

L'avantatge principal de NTWE es el seu baix nivell de computació. Això fa que sigui un solució ideal per sistemes on es requereixen molta flexibilitat en els càlculs computacionals i en l'ús de memòria.

Com únic inconvenient a millorar, es pot considerar que el càlcul de la funció inversa f^{-1} es eficient per valors enter q petits.

El temps de computació es fa mes llarg a mesura que el valor q creix.

Es possible que amb un algorisme més eficient, sigui possible rebaixar aquest temps.

Les posibles utilitats de l'algorisme **NTWE** poden ser:

1. - NTWE amb SCADA: ús del problema NTWE podria ser com algorisme criptogràfic per l'autentificació i integritat de les dades en les comunicacions segures de sistemes de control SCADA (Supervisory Control and Data Acquisition).

   SCADA es un sistema de control molt utilitzat per controlar i monitoritzar processos industrials autònoms. El protocols de comunicacions SCADA també s'han adaptat a les tecnologies TCP/IP i per tant, també s'han fet vulnerables a possibles ciberatacs.

   Gràcies a la "lleugeresa" de problema NTWE, les operacions criptogràfiques poden arribar a ser 30 vegades més ràpides que amb altres sistemes com RSA o ECC gràcies a la reducció en els càlculs computacionals i en la ocupació de memòria necessària.

   Les Signatures Digitals son un tipus d'encriptació de clau pública utilitzada per identificar un usuari i prevenir la falsificació de les dades

enviades.

2. - NTWE amb 5G: La cinquena generació de LTE (Long Term Evolution) presenta un canvi fonamental en la criptografia.

   Si les generacions anteriors basaven la seva seguretat en la criptografia simètrica, els estàndards 3GPP per 5G consideren la opció "Quantum ready"per als seus estàndards post-quàntics.

   Les xarxes 5G estan dissenyades per ser compatibles amb micro serveis amb el seu certificat de clau pública propi per autenticar, autoritzar i assegurar les transaccions.

   Les claus públiques poder permetre la transmissió de noms d'usuari i contrasenyes per Autenticar els dispositius 5G a les xarxes.

   L'avantage de l'ús del problema NTWE a les xarxes 5G implica una reducció de la mida de les clau públiques i la facilitat per xifrar i desxifrar el valors que permeten simplificar el protocol d'autentificació AKA (Authenticated Key Agreement).

3. - NTWE amb IoT: Altre possible ús i molt relacionat amb les xarxes 5G es l'adaptació als equips IoT (Interest of Things). Degut a la limitació de recursos computacionals, els criptosistemes amb alt nivell de seguretat i baix nivell computacional, la solució NTWE compleix els requeriments. Els equips IoT estan dissenyats per la comunicació a baix nivell sense intervenció humana. Per això, requereixen baixes capacitats computacionals i potencials però mantenint nivells alts de seguretat en les comunicacions.

   NTWE pot ser la opció ideal quan es fan servir claus de mides petites per permetre que els processos de xifrat i desxifrat sigui més ràpid. Per això cal que una parametrització específica que permet la seguretat contra atacs basats en l'algorisme de reducció basat en reticles anomenat L·LLL"(Lenstra-Lenstra-Lovász).

4. - NTWE amb HTTPS: La seguretat i privacitat a internet també s'han d'adaptar a les noves tecnologies.

Actualment, les comunicacions SSL/TLS (Secure Socket Layer / Transport Layer Security) fan servir estàndards basats en algorismes simètrics o asimètrics per donar un nivell de seguretat als protocols d'aplicació.

Actualment, el principals protocols asimètrics son RSA (Rivest Shamir Adleman), DSA (Digital Signature Algorith) o variants de corba el·líptica ECDSA.

Com certificat simètric, el més utilitzat es AES (Advanced Encryption Standard).

Aquests protocols poden ser vulnerables per sistemes post-quàntics. En aquest aspecte, la solució **NTWE** por ser una solució ja que pot tenir claus privades amb mides similars a RSA, amb millores significatives en quant al processos computacionals.

La clau per que NTWE sigui més eficient que altres versions encara a nivell experimental de sistema post-quàntics.

Referències

[1] NTWE A Natural Combination of NTRU and LWE - Joel Gärtner.

[2] Mathematic of Public Key Cryptography. Version 2.0 - Steven D Galbraith

[3] Isogènies, codis i reticles en criptografia postquàntica - Ramsès Fernàndez-València

[4] An Introduction to Mathematical Cryptography - Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman.

[5] A Decade of Lattice Cryptography - Chris Peikert.

[6] Better Key Sizes LWE - Lindner & Peikert

[7] Verfiying Solutions to LWE with Implication for Concrete Security - Palash Sarkar and Subhdip Singha.

[8] Post-Quantum cryptography from the learning with errors problem - Douglas Stebila