Lattice based signatures and homomorphic encryption via finite field isomorphisms

Jeff Hoffstein; Jill Pipher; Joseph H. Silverman
Brown University
John M. Schanck; William Whyte; Zhenfei Zhang
Security Innovation

PQCRYPTO 2016
February 26,2016

The foundation for a new lattice related hard problem

Basic Fact: Any two finite fields of the same order are isomorphic.

Basic Question: How to use this to create new, efficient, hopefully quantum resistant cryptographic constructions?

Finite field isomorphism

$$\mathbb{F}_{5^5} = \frac{\mathbb{Z}/5\mathbb{Z}[x]}{x^5 + x^4 + 4x^3 + x^2 + 4x + 1}$$

0	$0 + 0x + 0x^2 + 0x^3 + 0x^4$
1	$1 + 0x + 0x^2 + 0x^3 + 0x^4$
2	$2 + 0x + 0x^2 + 0x^3 + 0x^4$
⋮	⋮
5	$0 + 1x + 0x^2 + 0x^3 + 0x^4$
⋮	⋮
726	$1 + 0x + 4x^2 + 0x^3 + 1x^4$
⋮	⋮
731	$1 + 1x + 4x^2 + 0x^3 + 1x^4$
⋮	⋮
2614	$4 + 2x + 4x^2 + 0x^3 + 4x^4$
⋮	⋮
3125	$4 + 4x + 4x^2 + 4x^3 + 4x^4$

X-Space

$$\mathbb{F}_{5^5} = \frac{\mathbb{Z}/5\mathbb{Z}[x]}{y^5 + y^4 + 3y^3 + 2y^2 + 2y + 4}$$

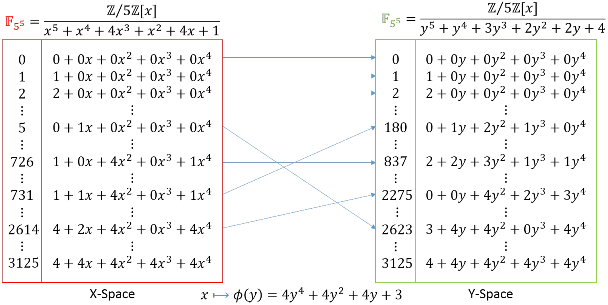
0	$0 + 0y + 0y^2 + 0y^3 + 0y^4$
1	$1 + 0y + 0y^2 + 0y^3 + 0y^4$
2	$2 + 0y + 0y^2 + 0y^3 + 0y^4$
⋮	⋮
180	$0 + 1y + 2y^2 + 1y^3 + 0y^4$
⋮	⋮
837	$2 + 2y + 3y^2 + 1y^3 + 1y^4$
⋮	⋮
2275	$0 + 0y + 4y^2 + 2y^3 + 3y^4$
⋮	⋮
2623	$3 + 4y + 4y^2 + 0y^3 + 4y^4$
⋮	⋮
3125	$4 + 4y + 4y^2 + 4y^3 + 4y^4$

Y-Space

$$x \longmapsto \phi(y) = 4y^4 + 4y^2 + 4y + 3$$

- $\mathbb{F} = \mathbb{Z}/q\mathbb{Z}[x]/(f(x))$ is a finite field $\mathbb{F}_{q^n}$ of order q^n.
- $f(x)$ and $F(y)$ define two copies of $\mathbb{F}_{q^n}$, and $\mathbb{Z}/q\mathbb{Z}[x]/(f(x)) \simeq \mathbb{Z}/q\mathbb{Z}[y]/(F(y))$ is a field isomorphism under a secret mapping $x \mapsto \phi(y)$.

Finite field isomorphism



$\mathbb{F}_{5^5} = \frac{\mathbb{Z}/5\mathbb{Z}[x]}{x^5+x^4+4x^3+x^2+4x+1}$

0	$0+0x+0x^2+0x^3+0x^4$
1	$1+0x+0x^2+0x^3+0x^4$
2	$2+0x+0x^2+0x^3+0x^4$
$\vdots$	$\vdots$
5	$0+1x+0x^2+0x^3+0x^4$
$\vdots$	$\vdots$
726	$1+0x+4x^2+0x^3+1x^4$
$\vdots$	$\vdots$
731	$1+1x+4x^2+0x^3+1x^4$
$\vdots$	$\vdots$
2614	$4+2x+4x^2+0x^3+4x^4$
$\vdots$	$\vdots$
3125	$4+4x+4x^2+4x^3+4x^4$

X-Space

$x \mapsto \phi(y) = 4y^4+4y^2+4y+3$

$\mathbb{F}_{5^5} = \frac{\mathbb{Z}/5\mathbb{Z}[x]}{y^5+y^4+3y^3+2y^2+2y+4}$

0	$0+0y+0y^2+0y^3+0y^4$
1	$1+0y+0y^2+0y^3+0y^4$
2	$2+0y+0y^2+0y^3+0y^4$
$\vdots$	$\vdots$
180	$0+1y+2y^2+1y^3+0y^4$
$\vdots$	$\vdots$
837	$2+2y+3y^2+1y^3+1y^4$
$\vdots$	$\vdots$
2275	$0+0y+4y^2+2y^3+3y^4$
$\vdots$	$\vdots$
2623	$3+4y+4y^2+0y^3+4y^4$
$\vdots$	$\vdots$
3125	$4+4y+4y^2+4y^3+4y^4$

Y-Space

- $\mathbb{F} = \mathbb{Z}/q\mathbb{Z}[x]/(f(x))$ is a finite field $\mathbb{F}_{q^n}$ of order q^n.
- $f(x)$ and $F(y)$ define two copies of $\mathbb{F}_{q^n}$, and $\mathbb{Z}/q\mathbb{Z}[x]/(f(x)) \simeq \mathbb{Z}/q\mathbb{Z}[y]/(F(y))$ is a field isomorphism under a secret mapping $x \mapsto \phi(y)$.

Finite field isomorphism

$\mathbb{F}_{5^5} = \dfrac{\mathbb{Z}/5\mathbb{Z}[x]}{x^5+x^4+4x^3+x^2+4x+1}$ X-Space

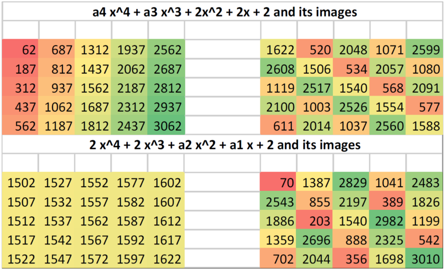
$x \mapsto \phi(y) = 4y^4+4y^2+4y+3$

$\mathbb{F}_{5^5} = \dfrac{\mathbb{Z}/5\mathbb{Z}[x]}{y^5+y^4+3y^3+2y^2+2y+4}$ Y-Space

🟥 small

🟧 medium

🟩 large



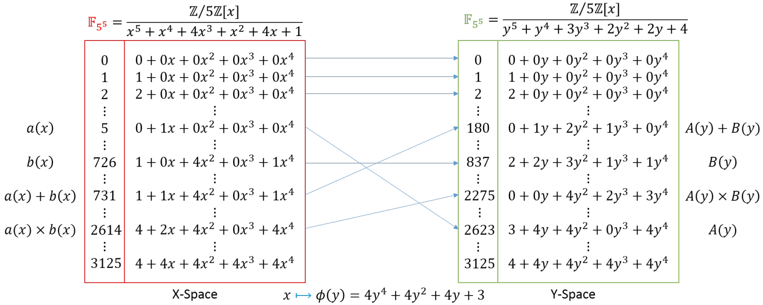
a4 x^4 + a3 x^3 + 2x^2 + 2x + 2 and its images										
62	687	1312	1937	2562		1622	520	2048	1071	2599
187	812	1437	2062	2687		2608	1506	534	2057	1080
312	937	1562	2187	2812		1119	2517	1540	568	2091
437	1062	1687	2312	2937		2100	1003	2526	1554	577
562	1187	1812	2437	3062		611	2014	1037	2560	1588
2 x^4 + 2 x^3 + a2 x^2 + a1 x + 2 and its images										
1502	1527	1552	1577	1602		70	1387	2829	1041	2483
1507	1532	1557	1582	1607		2543	855	2197	389	1826
1512	1537	1562	1587	1612		1886	203	1540	2982	1199
1517	1542	1567	1592	1617		1359	2696	888	2325	542
1522	1547	1572	1597	1622		702	2044	356	1698	3010

A hard problem based on this isomorphism

Given $F(y)$ and an element $A(y) \in \mathbb{F}_{q^n}$, with the promise that $a(x) \in \mathbb{F}_{q^n}$ is bounded, find $a(x)$.

There is also a decision version of this problem.

Homomorphic mapping



$\mathbb{F}_{5^5} = \dfrac{\mathbb{Z}/5\mathbb{Z}[x]}{x^5+x^4+4x^3+x^2+4x+1}$

	0	$0+0x+0x^2+0x^3+0x^4$
	1	$1+0x+0x^2+0x^3+0x^4$
	2	$2+0x+0x^2+0x^3+0x^4$
	⋮	⋮
$a(x)$	5	$0+1x+0x^2+0x^3+0x^4$
	⋮	⋮
$b(x)$	726	$1+0x+4x^2+0x^3+1x^4$
	⋮	⋮
$a(x)+b(x)$	731	$1+1x+4x^2+0x^3+1x^4$
	⋮	⋮
$a(x)\times b(x)$	2614	$4+2x+4x^2+0x^3+4x^4$
	⋮	⋮
	3125	$4+4x+4x^2+4x^3+4x^4$

X-Space

$x \longmapsto \phi(y) = 4y^4+4y^2+4y+3$

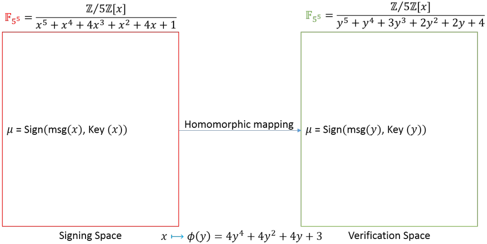
$\mathbb{F}_{5^5} = \dfrac{\mathbb{Z}/5\mathbb{Z}[x]}{y^5+y^4+3y^3+2y^2+2y+4}$

0	$0+0y+0y^2+0y^3+0y^4$	
1	$1+0y+0y^2+0y^3+0y^4$	
2	$2+0y+0y^2+0y^3+0y^4$	
⋮	⋮	
180	$0+1y+2y^2+1y^3+0y^4$	$A(y)+B(y)$
⋮	⋮	
837	$2+2y+3y^2+1y^3+1y^4$	$B(y)$
⋮	⋮	
2275	$0+0y+4y^2+2y^3+3y^4$	$A(y)\times B(y)$
⋮	⋮	
2623	$3+4y+4y^2+0y^3+4y^4$	$A(y)$
⋮	⋮	
3125	$4+4y+4y^2+4y^3+4y^4$	

Y-Space

- For short $a(x)$ and $b(x)$, $a(x)\times b(x)$ will also be short;
- $A(y)$, $B(y)$ and $A(y)\times B(y)$ should look random.

Signature scheme, omitting many details



$\mathbb{F}_{5^5} = \frac{\mathbb{Z}/5\mathbb{Z}[x]}{x^5 + x^4 + 4x^3 + x^2 + 4x + 1}$

$\mathbb{F}_{5^5} = \frac{\mathbb{Z}/5\mathbb{Z}[x]}{y^5 + y^4 + 3y^3 + 2y^2 + 2y + 4}$

μ = Sign(msg(x), Key (x))

Homomorphic mapping

μ = Sign(msg(y), Key (y))

Signing Space

$x \longmapsto \phi(y) = 4y^4 + 4y^2 + 4y + 3$

Verification Space

- Form an NTRU lattice in X-space and compute corresponding Y-space lattice.
- Compute a pqNTRUSign signature in X-space.
- Publish corresponding data in Y-space.
- Relationship still holds in Y-space due to homomorphism.
- Nothing on X-space is revealed.

Hardness

Isomorphism

The isomorphism between $\mathbb{Z}/q\mathbb{Z}[y]/(F(y))$, and $\mathbb{Z}/q\mathbb{Z}[x]/(f(x))$ does not respect the Archimedian property of size. The image of a short polynomial in x is a polynomial in y with coefficients "uniformly" distributed mod q.

Lattice strength

$$L_{\mathbf{h}} = \left\{(\mathbf{u},\mathbf{v}) \in \mathcal{R}_f^2 : \mathbf{v} \equiv \mathbf{h}\cdot\mathbf{u} \pmod q\right\} \qquad \subset \mathbb{F},$$
$$L_{\mathbf{H}} = \left\{(\mathbf{U},\mathbf{V}) \in \mathcal{R}_F^2 : \mathbf{V} \equiv \mathbf{H}\cdot\mathbf{U} \pmod q\right\} \qquad \subset \mathbb{F}.$$

- $h(x) = a(x)/b(x) \mapsto H(y) = A(y)/B(y)$
- $L_{\mathbf{h}}$ is an NTRU lattice with unique short vectors $\langle a(x), b(x)\rangle$;
- $\langle A(y), B(y)\rangle$ are not short in $L_{\mathbf{H}}$, likely $L_{\mathbf{H}}$ does not have any unique short vectors.

Thank you

1. A short summary of the hard problem

2. A detailed overview

3. An instantiation of pqNTRUSign over FF

The mathematical underpinning

Fix $n \approx 200$; (for example); fix a prime q on the order of a constant multiple of n; and fix a small prime p, relatively prime to q, such as 2 or 3, 5,7,11, or an irreducible polynomial of low degree with short coefficients.

Let $f(x)$ be a secret *short* monic polynomial of degree n, i.e., with small coefficients (for example chosen from $\{-1, 0, 1\}$), that is irreducible mod q.

Let $F(y)$ be a public monic polynomial of degree n with arbitrary coefficients, that is irreducible mod q.

Then

$$\mathbb{Z}/q\mathbb{Z}[x]/(f(x)) \simeq \mathbb{Z}/q\mathbb{Z}[y]/(F(y)),$$

as both are finite fields of order q^n.

The mathematical underpinning, part 2

The polynomials $f(x)$ and $F(y)$ are chosen independently and have *no* relation to each other.

Given knowledge of both, it is easy to construct a field isomorphism between $\mathbb{Z}/q\mathbb{Z}[x]/(f(x))$ and $Z/q\mathbb{Z}[y]/(F(y))$, and $F(y)$ is the image of $f(x)$ under this isomorphism.

This isomorphism is the secret key.

The mathematical underpinning, part 3

Homomorphism

Set $|f(x)|$ to be small, and $|F(y)|$ to be large. Instead of fields, consider the lattices

$$R_f = \mathbb{Z}[x]/(f(x)) \quad \text{and} \quad R_F = \mathbb{Z}[y]/(F(y)).$$

Fact: If $r_1(x), r_2(x) \in R_f$ are short, then $r_1(x)r_2(x) \in R_f$ will also be short, i.e $r_1(x)r_2(x)$ reduced modulo $f(x)$ will also be short.

This fact expresses generalizes the property that NTRU is based upon, in which $f(x)$ is the specific polynomial $x^n - 1$.

Constructing cryptosystems and signatures

Think of short polynomials $r_1(x), r_2(x), \cdots \in R_f$ as elements of the field $\mathbb{Z}/q\mathbb{Z}[x]/(f(x))$.

As long as the coefficients of a polynomial computation $P(r_1(x), r_2(x), \dots)$ do not exceed $q/2$ in absolute value, the value of the computation in $\mathbb{Z}/q\mathbb{Z}[x]/(f(x))$ can be lifted back to $\mathbb{Z}[x]/(f(x))$.

For any $r(x) \in \mathbb{Z}/q\mathbb{Z}[x]/(f(x))$, denote by $R(y)$ the isomorphic image of $r(x)$ in $\mathbb{Z}/q\mathbb{Z}[y]/(F(y))$.

Constructing cryptosystems and signatures, cont.

For homomorphic encryption or signature schemes, the input will be encoded as secret short polynomials in $\mathbb{Z}/q\mathbb{Z}[x]/(f(x))$.

These secret short polynomials will be mapped by the secret field isomorphism to public images $R(y)$ in $\mathbb{Z}/q\mathbb{Z}[y]/(F(y))$.

The main point: The isomorphism between $\mathbb{Z}/q\mathbb{Z}[y]/(F(y))$, and $\mathbb{Z}/q\mathbb{Z}[x]/(f(x))$ does not respect the Archimedian property of size. The image of a short polynomial in x is a polynomial in y with coefficients uniformly distributed mod q.

Depending on the details of the encryption or signature scheme, lattice attacks that work directly with the $R(y)$ may be possible.

Constructing cryptosystems and signatures, cont.

The idea behind signatures: set a problem involving the public information that is easily solvable using the short isomorphic images in the private field.

The idea behind homomorphic encryption: The cloud does computations on the public images $R(y)$. The possessor of the private isomorphism maps the answer back to $\mathbb{Z}/q\mathbb{Z}[x]/(f(x))$ and then lifts to $\mathbb{Z}[x]/(f(x))$. As long as the coefficients in the private space have not exceeded $q/2$ in absolute value this will give the correct answer.

Attacks, cont.

One approach to attacks of this sort is via lattice reduction. The object would be to search for a matrix which is a linear transformation of vector spaces that sends all known images of short vectors/polynomials to short polynomials.

There are many potential solutions to this, but with high probability there will a unique linear transformation that is also a field isomorphism.

Only a field isomorphism will be useful for decryption.

For example, the isomorphism will be given by an n by n matrix. Any of the $n!$ permutations of the rows of this matrix will give a linear transformation of vector spaces with the correct properties, but only one of these will be a field isomorphism.

Research on other potential attacks is ongoing.

Concluding point

Lattice reduction attacks force current homomorphic schemes and signature schemes to take n quite large.

Because of the fundamental *non-linearity* of this scheme, it appears to be possible to take n far smaller, in the low hundreds.

We believe that our scheme, exploiting nonlinearity via hidden isomorphisms, is a fundamentally new approach to *efficient* FHE and signature schemes that merits further research.

Signature details for one particular example

There are many possible methods of applying the basic notion of a secret isomorphism between two finite fields to create a signature scheme. In the following slides we will sketch one method which we call pqFF-Sign.

The fundamental idea underlying pqFF-Sign is to combine the transcript-secure signature scheme pq-NTRUSign (aka NTRUMls) with with the finite field isomorphic concept. Thus we first use the pq-NTRUSign signature scheme working in a finite field $\mathbb{F}_{q^n}$, but then we homomorphically map the signature to a different copy of the field $\mathbb{F}_{q^n}$. Verification is still possible due to the homomorphic property of the map, but various lattice attacks that were possible on pq-NTRUSign are blunted or eliminated due to the non-linear nature of the homomorphic encryption map.

1 A short summary of the hard problem

2 A detailed overview

3 An instantiation of pqNTRUSign over FF

Signature details:notation

n a dimension parameter.

q a prime (or prime power) greater than a constant times n.

p a small prime.

$\mathbf{f}(x) \in \mathbb{F}_q[x]$ a short irreducible monic polynomial of degree n.

$\mathbf{F}(y) \in \mathbb{F}_q[y]$ a random irreducible monic polynomial of degree n.

Signature details:notation, cont.

$\phi(y) \in \mathbb{F}_q[y]$. The map $x \mapsto \phi(y)$ induces an isomorphism $\mathbb{F}_q[x]/(\mathbf{f}(x)) \to \mathbb{F}_q[y]/(\mathbf{F}(y))$.

$\psi(x) \in \mathbb{F}_q[x]$ the map $y \mapsto \psi(x)$ induces the inverse isomorphism $\mathbb{F}_q[y]/(\mathbf{F}(y)) \to \mathbb{F}_q[x]/(\mathbf{f}(x))$.

$\mathbf{a}(x), \mathbf{b}(x) \in \mathbb{F}_q[x]$ short irreducible monic polynomials of degree n.

$\mathbf{h}(x) \in \mathbb{F}_q[x] \ \equiv \mathbf{b}(x) \cdot \big(p\mathbf{a}(x)\big)^{-1} \pmod{q}$.

$\mathbf{H}(y) \in \mathbb{F}_q[y] \ \equiv \mathbf{h}\big(\phi(y)\big) \pmod{q, \mathbf{F}(y)}$.

U is an n-by-n matrix, small entries, invertible mod q.

Signature details:notation, cont.

We will lift mod q polynomials to polynomials having integer coefficients in the range $(-\frac{1}{2}q, \frac{1}{2}q]$. Define rings and fields

$$\mathcal{R}_f = \frac{\mathbb{Z}[x]}{(\mathbf{f}(x))}, \quad \mathcal{R}_F = \frac{\mathbb{Z}[y]}{(\mathbf{F}(y))}, \quad \mathcal{R}_{f,q} = \frac{\mathbb{F}_q[x]}{(\mathbf{f}(x))}, \quad \mathcal{R}_{F,q} = \frac{\mathbb{F}_q[y]}{(\mathbf{F}(y))}.$$

And define lattices

$$L_{\mathbf{h}} = \left\{(\mathbf{u}, \mathbf{v}) \in \mathcal{R}_f^2 : \mathbf{v} \equiv \mathbf{h} \cdot \mathbf{u} \pmod{q}\right\},$$
$$L_{\mathbf{H}} = \left\{(\mathbf{U}, \mathbf{V}) \in \mathcal{R}_F^2 : \mathbf{V} \equiv \mathbf{H} \cdot \mathbf{U} \pmod{q}\right\}.$$

Signature details:notation, cont.

We use U to define polynomials $\mathbf{c}_1(x), \ldots, \mathbf{c}_n(x) \in \mathbb{F}_q[x]$ of degree less than n by

$$\begin{pmatrix} \mathbf{c}_1(x) \\ \mathbf{c}_2(x) \\ \vdots \\ \mathbf{c}_n(x) \end{pmatrix} \equiv U^{-1} \begin{pmatrix} x \\ x^2 \\ \vdots \\ x^n \end{pmatrix} \pmod{q, f(x)}.$$

For $1 \leq j \leq n$ we let

$$\mathbf{C}_j(y) = \mathbf{c}_j(\phi(y)) \in \mathcal{R}_{F,q}$$

be the corresponding polynomials in the y-field.

Security Assumption As U ranges over matrices with small coefficients that are invertible modulo q, the coefficients of U^{-1} mod q are uniformly distributed.

The big picture

The polynomials $\mathbf{c}_1(x), \mathbf{c}_2(x), \ldots, \mathbf{c}_n(x)$ form a basis for $\mathcal{R}_{f,q}$ and $\mathbf{C}_1(y), \mathbf{C}_2(y), \ldots, \mathbf{C}_n(y)$ form a basis for $\mathcal{R}_{F,q}$. Each $\mathbf{C}_j(y)$ is the image of the corresponding $\mathbf{c}_j(x)$ under the isomorphism that sends $x \mapsto \phi(y)$. This same isomorphism preserves the coefficients of linear combinations of the $\mathbf{c}_j(x)$, that is,

$$\sum \alpha_j \mathbf{c}_j(x) \mapsto \sum \alpha_j \mathbf{C}_j(y).$$

The big picture,cont

The key property that the scheme is based on is the fact that as

$$U \begin{pmatrix} \mathbf{c}_1(x) \\ \mathbf{c}_2(x) \\ \vdots \\ \mathbf{c}_n(x) \end{pmatrix} \equiv \begin{pmatrix} x \\ x^2 \\ \vdots \\ x^n \end{pmatrix} \pmod{q, f(x)},$$

and the coefficients of U are small, then each x^i, for $1 \leq i \leq n$ is expressible as a linear combination of the $\mathbf{c}_j(x)$ with small coefficients. From this it follows that any polynomial in x with small coefficients, of the form $\mathbf{t}(x) = \sum_{i=1}^{n} t_i x^i$, with the t_i small, can in turn be written as a polynomial in $\mathbf{c}_j(x)$ with small coefficients.

The big picture,cont

We will find it convenient to use polynomials reduced modulo $\mathbf{f}(x)$, which will necessarily have degree less than or equal to $n-1$, that is, of the form $\mathbf{r}(x) = \sum_{i=0}^{n-1} r_i x^i$, with the r_i short. Recall that $f(x) = x^n + f_{n-1}x^{n-1} + ... + f_1 x \pm 1$, where $f_i \in \{1, 0, -1\}$. Consequently

$$\pm 1 \equiv -f_1 x - ... - x^n \pmod{f(x)}.$$

and thus

$$\mathbf{r}(x) \equiv \sum_{i=1}^{n} r_i' x^i \equiv \pm r_0(-f_1 x - ... - x^n) + \sum_{i=1}^{n-1} r_i x^i \pmod{(f(x))},$$

where the r_i' are also short, is expressible as a short linear combination of the $\mathbf{c}_j(x)$.

The big picture, cont.

Most importantly, as the product of any two short polynomials in x remains short, such a product will also be writeable as a short linear combination of the $\mathbf{c}_j(x)$. The reverse does not hold: with high probability a random linear combination of $\mathbf{c}_j(x)$ with small coefficients will *not* equal a polynomial in x with small coefficients.

It is this property, that a product of short linear combinations of the $\mathbf{c}_j(x)$ that correspond to short polynomials in x can again be written as a short linear combination of the $\mathbf{c}_j(x)$, that allows the signer to solve a congruential lattice problem in $L_{\mathbf{h}}$ (just as in pq-NTRUSign) and then map the corresponding solution, with the same coefficients, back to $L_{\mathbf{H}}$.

What is the advantage over pq-NTRUSign?

There are two main security concerns that determine parameters in pq-NTRUSign. One is the problem of recovering the private key from the public NTRU key, and the other is the problem of forgery. Of these, the one that has the biggest impact on parameter size is the public key to private key problem. This is because, to make rejection sampling efficient, the q needs to be chosen large compared to n. This makes the lattice problem somewhat easier and forces an increase in the size of n.

What is the advantage over pq-NTRUSign, cont.?

In this context there appear at first to be two NTRU-type problems: Recovering $\mathbf{a}(x), \mathbf{b}(x)$ from $\mathbf{h}(x)$, and recovering the corresponding polynomials $\mathbf{A}(y), \mathbf{B}(y)$ from $\mathbf{H}(y)$.

The $\mathbf{h}(x)$ is private, and only revealed if the underlying isomorphism is discovered, in which case the scheme is considered broken. So this lattice problem does not arise.

What is the advantage over pq-NTRUSign, cont.?

On the other hand, the $\mathbf{H}(y)$ is public, but the corresponding problem of recovering $\mathbf{A}(y), \mathbf{B}(y)$ from $\mathbf{H}(y)$ is not a lattice reduction problem as $\mathbf{A}(y), \mathbf{B}(y)$ are generic polynomials with coefficients mod q, and not short. And as they are not short, recovery of them would not lead to any advantage.

There is a lattice attack to recover the matrix U from the $\mathbf{C}_j(y)$, which would suffice to break the scheme, but the dimension of the lattice required to accomplish this is on the order of than n^2.

For this reason, it appears that it will suffice to set parameters to avoid forgery attacks, which should allow for smaller signatures and better operating characteristics.

Signature details

Private Information: $\mathbf{f}(x), \mathbf{a}(x), \mathbf{b}(x), \mathbf{h}(x), \mathbf{c}_1(x), \ldots, \mathbf{c}_n(x)$ and U.

Public Information: $\mathbf{F}(y), \mathbf{H}(y)$ and $\mathbf{C}_1(y), \ldots, \mathbf{C}_n(y)$.

Digital Document Hash: A pair of mod p vectors $\overline{\boldsymbol{\delta}}, \overline{\boldsymbol{\epsilon}}$ obtained by applying a hash function to the document being signed:

$$\overline{\boldsymbol{\delta}} = \overline{\delta_1}, \ldots, \overline{\delta_n)} \in \left(-\tfrac{1}{2}p, \tfrac{1}{2}p\right]^n,$$

$$\overline{\boldsymbol{\epsilon}} = \overline{\epsilon}_1, \ldots, \overline{\epsilon_n} \in \left(-\tfrac{1}{2}p, \tfrac{1}{2}p\right]^n.$$

Signature: A pair of vectors

$$\boldsymbol{\delta} = (\delta_1, \ldots, \delta_n) \in \left(-\tfrac{1}{2}q, \tfrac{1}{2}q\right]^n$$

$$\boldsymbol{\epsilon} = (\epsilon_1, \ldots, \epsilon_n) \in \left(-\tfrac{1}{2}q, \tfrac{1}{2}q\right]^n.$$

Signature details, cont.

Verification: A signature on the document hash $(\bar{\boldsymbol{\delta}}, \bar{\boldsymbol{\epsilon}})$ is valid if it satisfies the following three conditions:

1. $\delta_i \equiv \bar{\delta}_i \pmod{p}$ and $\epsilon_i \equiv \bar{\epsilon}_i \pmod{p}$ for all $1 \leq i \leq n$.
2. $|\delta_i| \leq \frac{1}{2}q - B$ and $|\epsilon_i| \leq \frac{1}{2}q - B$ for all $1 \leq i \leq n$.
3. Let
$$\mathbf{S}(y) = \delta_1 \mathbf{C}_1(y) + \cdots + \delta_n \mathbf{C}_n(y),$$
and
$$\mathbf{T}(y) = \epsilon_1 \mathbf{C}_1(y) + \cdots + \epsilon_n \mathbf{C}_n(y).$$
Then $(\mathbf{S}, \mathbf{T}) \in L_{\mathbf{H}}$, i.e.,
$$\mathbf{T}(y) \equiv \mathbf{S}(y)\mathbf{H}(y) \pmod{q, \mathbf{F}(y)}.$$

Here B is a fixed small integer used to enable rejection sampling.

Signature Creation

Signatures are created as in pq-NTRUSign working in the ring $\mathcal{R}_f = \mathbb{Z}[x]/\big(\mathbf{f}(x)\big)$, with one change. Rather than creating polynomials with small coefficients relative to the standard basis $1, x, \ldots, x^{n-1}$, we instead create polynomials with small coefficients relative to the basis $\mathbf{c}_1(x), \ldots, \mathbf{c}_n(x)$.

Signature Creation details

Step 1: Choose δ_j at random mod q such that $q/2 < \delta_j \leq q/2$ and $\delta_j \equiv \overline{\delta_j} \pmod{p}$ and set

$$\mathbf{s}_0(x) = \sum_{j=1}^{n} \delta_j \mathbf{c}_j(x).$$

Step 2: Define $\mathbf{t}_0(x)$ by

$$\mathbf{t}_0(x) \equiv \mathbf{s}_0(x)\mathbf{h}(x) \pmod{q}$$

and write

$$\mathbf{t}_0(x) = \sum_{i=0}^{n-1} t_i x^i.$$

Then $(\mathbf{s}_0(x), \mathbf{t}_0(x)) \in L_{\mathbf{h}}$.

Signature Creation details, cont.

Step 3: Write

$$\mathbf{t}_0(x) = \sum_{j=1}^{n} \eta_j \mathbf{c}_j(x)$$

for some $\eta_1, \ldots, \eta_n$.
To accomplish this, as described previously, write

$$\mathbf{t}_0(x) = \sum_{i=0}^{n-1} t_i x^i \equiv \sum_{i=1}^{n} t_i' x^i \pmod{\mathbf{f}(x)}$$

as described previously, and set

$$(\eta_1, \ldots, \eta_n) \equiv (t_1', \ldots, t_n')U \quad (q),$$

and select representatives for the η_j in the interval $(-q/2/q/2]$.
The η_j will appear to be randomly and uniformly distributed mod q.

Signature Creation details , cont.

Step 4 : Construct $(\mathbf{u}(x), \mathbf{v}(x)) \in L_{\mathbf{h}}$ such that

$$\mathbf{u}(x) = \sum_{j=1}^{n} \delta_j^{(u)} \mathbf{c}_j(x) \quad \text{and} \quad \mathbf{v}(x) = \sum_{j=1}^{n} \delta_j^{(v)} \mathbf{c}_j(x),$$

with $\delta_j^{(u)}, \delta_j^{(v)}$ small, $\delta_j^{(u)} \equiv 0 \pmod p$, and $\delta_j^{(v)} + \eta_j \equiv \epsilon_j \pmod p$ for all j.

To construct the desired $(\mathbf{u}(x), \mathbf{v}(x))$, search for an appropriate $\mathbf{r}(x)$ which is short, and set

$$\mathbf{u}(x) = p\mathbf{r}(x)\mathbf{a}(x) \quad \text{and} \quad \mathbf{v}(x) = \mathbf{r}(x)\mathbf{v}(x).$$

Signature Creation details, cont.

Such an $\mathbf{r}(x)$ must satisfy

$$\mathbf{r}(x)\mathbf{b}(x) = \sum_{j=1}^{n} \delta_j^{(v)} \mathbf{c}_j(x),$$

with the $\delta_j^{(v)}$ small and $\delta_j^{(v)} + \eta_j \equiv \epsilon_j \pmod{p}$,

and also satisfy

$$p\mathbf{r}(x)\mathbf{a}(x) = \sum_{j=1}^{n} \delta_j^{(u)} \mathbf{c}_j(x),$$

with the $\delta_j^{(u)}$ small and $\delta_j^{(u)} \equiv 0 \pmod{p}$.

Signature Creation details, cont

As $\mathbf{r}(x), \mathbf{a}(x)$ are short, $\mathbf{r}(x)\mathbf{a}(x)$ is also short, and we may write

$$\mathbf{r}(x)\mathbf{a}(x) = \sum_{i=0}^{n-1} d_i x^i \in \mathcal{R}_f,$$

with the d_i small. Then the $\delta_j^{(u)}$ of

$$p\mathbf{r}(x)\mathbf{a}(x) = \sum_{j=1}^{n} \delta_j^{(u)} \mathbf{c}_j(x),$$

are given by

$$(\delta_1^{(u)}, \ldots, \delta_n^{(u)}) = p(d_0, \ldots, d_{n-1})U.$$

As all the d_i and entries of U are small there is no wraparound mod q and each $\delta_j^{(u)} \equiv 0 \pmod{p}$. Thus for whatever short $\mathbf{r}(x)$ we find, the $\delta_j^{(u)} \equiv 0 \pmod{p}$ condition will hold.

Signature Creation details, cont.

We turn now to finding $\mathbf{r}(x)$ short, such that

$$\mathbf{r}(x)\mathbf{b}(x) = \sum_{j=1}^{n} \delta_j^{(v)} \mathbf{c}_j(x),$$

with $\delta_j^{(v)}$ short and $\delta_j^{(v)} \equiv \overline{\epsilon_j} - \eta_j \pmod p$.

To accomplish this, write $\mathbf{b}(x) = \sum_i^{n-1} b_i x^i$, set

$$(b_{0,0}, b_{0,1}, \ldots, b_{0,n-1}) = (b_0, b_1, \ldots, b_{n-1}),$$

and define $(b_{i,0}, b_{i,1}, \ldots, b_{i,n-1})$ by

$$x^i \mathbf{b}(x) = b_{i,0} + b_{i,1}x + \cdots + b_{i,n-1}x^{n-1}.$$

Signature Creation details, cont.

Let B denote the matrix whose i, j entry is $b_{i,j}$, and let

$$\beta = BU.$$

Note that the entries $\beta_{i,j}$ of β are small because the $b_{i,j}$ and the entries of U are small.

For any

$$\mathbf{r}(x) = \sum_{i=0}^{n-1} r_i x^i \equiv \sum_{i=1}^{n} r_i' x^i \pmod{\mathbf{f}(x)}$$

we have

$$\mathbf{r}(x)\mathbf{b}(x) = (r_1', r_2', \ldots, r_n')\beta \begin{pmatrix} \mathbf{c}_1(x) \\ \mathbf{c}_2(x) \\ \vdots \\ \mathbf{c}_n(x) \end{pmatrix}.$$

Signature Creation details, cont.

To solve for $\mathbf{r}(x)$, first define

$$(\overline{r_1'}, \overline{r_2'}, \ldots, \overline{r_n'}) \equiv (\overline{\delta_1^{(v)}}, \overline{\delta_2^{(v)}}, \ldots, \overline{\delta_n^{(v)}})\beta^{-1} \pmod{p}$$

and lift each $\overline{r_j'}$ to $r_j' \in (-p/2, p/2]$.

Then define $\delta_j^{(v)}$ by

$$(\delta_1^{(v)}, \ldots, \delta_n^{(v)}) = (r_1', \ldots, r_n')\beta.$$

This accomplishes the goal

$$\mathbf{r}(x)\mathbf{b}(x) = \sum_{j=1}^{n} \delta_j^{(v)} \mathbf{c}_j(x),$$

with $\delta_j^{(v)} \equiv \overline{\delta_j^{(v)}} \pmod{p}$.

Rejection sampling

After accomplishing Step 4, we have found a short pair of vectors $(\mathbf{u}(x), \mathbf{v}(x)) \in L_{\mathbf{h}}$ with the appropriate congruential properties.

Having done so, set

$$\mathbf{s}(x) = \mathbf{s}_0(x) + \mathbf{u}(x) \quad \text{and} \quad \mathbf{t}(x) = \mathbf{t}_0(x) + \mathbf{v}(x).$$

Then

$$\mathbf{s}(x) = \sum_{j=1}^{n} (\delta_j + \delta_j^{(u)}) \mathbf{c}_j(x) \quad \text{and} \quad \mathbf{t}(x) = \sum_{j=1}^{n} (\eta_j + \delta_j^{(v)}) \mathbf{c}_j(x).$$

Rejection sampling, cont.

By our construction, $\delta_j + \delta_j^{(u)}$ and $\eta_j + \delta_j^{(v)}$ satisfy the required congruences mod p.

If, in addition, for an appropriate choice of $\mathcal{B}$, $|\delta_j + \delta_j^{(u)}| < q/2 - \mathcal{B}$, and $|\eta_j + \delta_j^{(v)}| < q/2 - \mathcal{B}$, then we accept the signature and release it. If not, we repeat the process.

An argument very similar to that in pq-NTRUSign shows that this guarantees an information free transcript.

Attacks

In signature and homomorphic encryption schemes based on this approach, the public key and private key are unrelated. In both cases, an attacker will have possession of a collection of images in $\mathbb{Z}/q\mathbb{Z}[y]/(F(y))$ of short polynomials in $\mathbb{Z}/q\mathbb{Z}[x]/(f(x))$.

To decrypt or forge, an attacker must find a field isomorphism that sends each encrypted piece of data, taking the form of a polynomial in y with coefficients uniformly distributed mod q, into a new field where all the coefficients are short.

With high probability, such a field will be unique.