A signature scheme from the finite fields isomorphism problem

Jeff Hoffstein; Joseph H. Silverman
Brown University
William Whyte; Zhenfei Zhang
OnBoard Security

MathCrypt
August 19, 2018

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	$4 + 2x + 4x^2 + 0x^3 + 4x^4$
⋮	⋮
3124	$4 + 4x + 4x^2 + 4x^3 + 4x^4$

X-Space

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

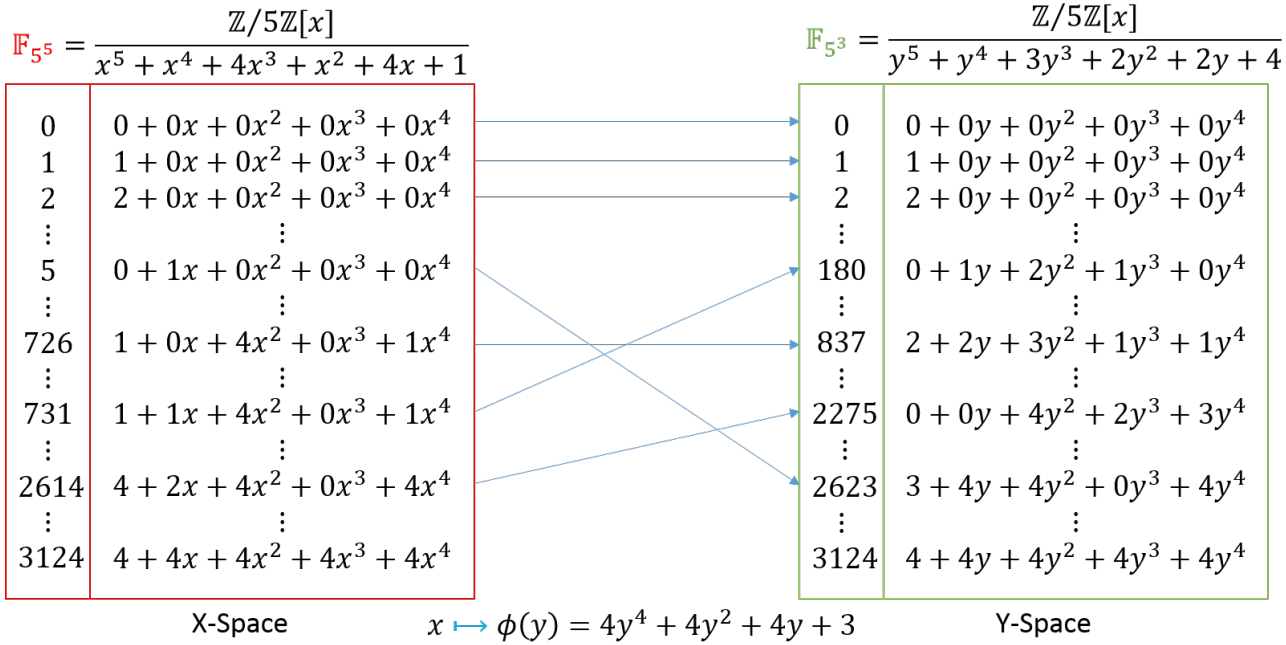
$$\mathbb{F}_{5^3} = \frac{\mathbb{Z}/5\mathbb{Z}[x]}{y^5 + y^4 + 3y^3 + 2y^2 + 2y + 4}$$

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	$3 + 4y + 4y^2 + 0y^3 + 4y^4$
⋮	⋮
3124	$4 + 4y + 4y^2 + 4y^3 + 4y^4$

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



- $\mathbb{F} = \mathbb{Z}/q\mathbb{Z}[x]/(f(x))$ 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

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

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

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

small

medium

large

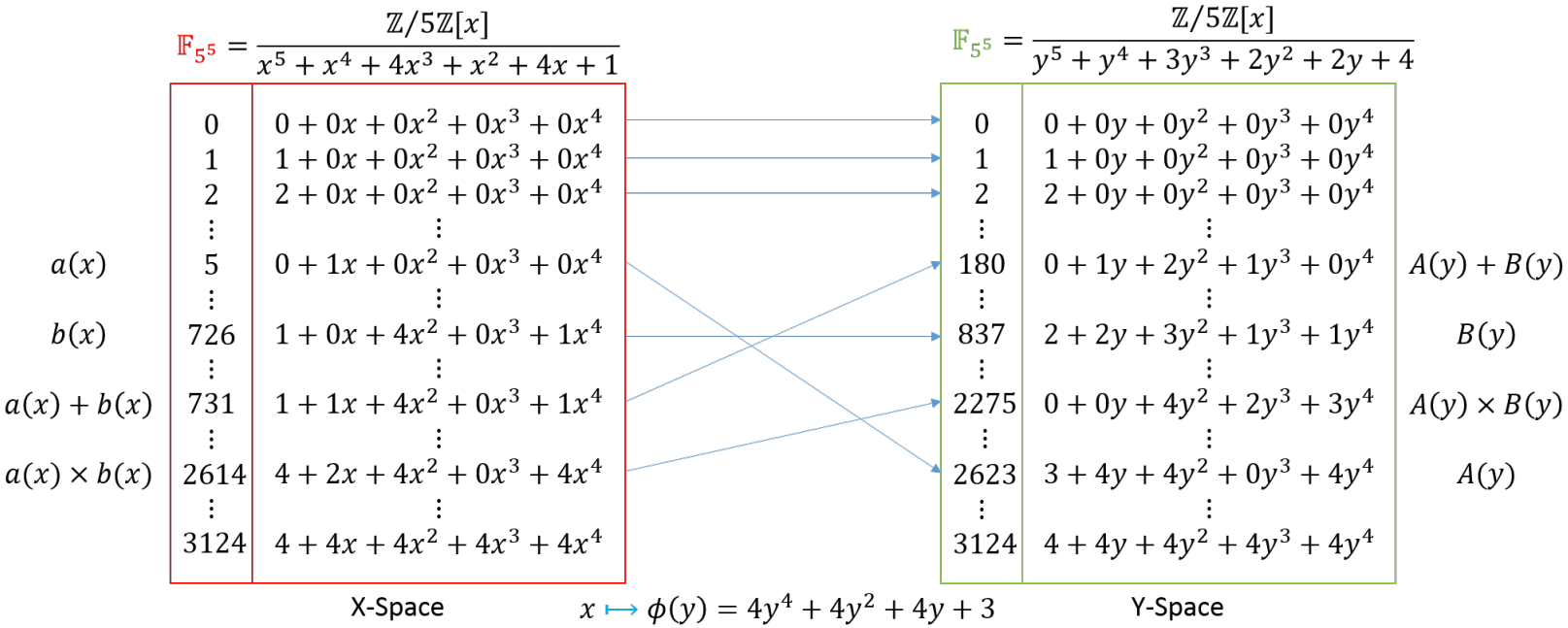
a4 x^4 + a3 x^3 + 2x^2 + 2x + 2 and its images										
62	687	1312	1937	2562		1622	520	2048	1071	2599
187	812	1437	2062	2687		2608	1506	534	2057	1080
312	937	1562	2187	2812		1119	2517	1540	568	2091
437	1062	1687	2312	2937		2100	1003	2526	1554	577
562	1187	1812	2437	3062		611	2014	1037	2560	1588
2 x^4 + 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 $a(x)$.

Also has a decision version of the problem.

Homomorphic mapping



- 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.

The Finite Field Isomorphism (FFI) Problems

Definition (FFI, CFFI, DFFI)

Finite Field Isomorphism Problems Let k be a positive integer. Let $\mathbb{X}, \mathbb{Y}$ be X-space and Y-space; ϕ be the isomorphism and χ_β be a β bounded distribution. Let $a_1(x), \ldots, a_k(x), b_1(x)$ be short polynomials, and $A_1(y), \ldots, A_k(y), B_1(y)$be the corresponding images. Also sample $B_2(y)$ uniformly.

Computational FFI problem: Given $A_1(y), \ldots, A_k(y)$, recover $f(x)$ and/or $a_1(x), \ldots, a_k(x)$.

Decisional FFI problem: Given $A_1(y), \ldots, A_k(y)$, B_1 and B_2, with one of B_1, B_2 an image of a short polynomial. Identify the image with a probability greater than $1/2$.

A few words on the hardness of the problem

Lemma

For large n, for any fixed $\boldsymbol{f}(x) \in \mathbb{F}_q[x]$, and any given degree $n-1$ polynomial $\phi(y) \in \mathbb{F}_q[y]$, there will exist, with probability approaching 1, a unique monic irreducible $\boldsymbol{F}(y) \in \mathbb{F}_q[y]$ such that the map $x \to \phi(y)$ induces an isomorphism between $\mathbb{F}_q[x]/(\boldsymbol{f}(x))$ and $\mathbb{F}_q[y]/(\boldsymbol{F}(y))$.

- We do not know the concrete hardness.
- This lemma suggests that the mapping SHOULD be random:
  - Fix $\boldsymbol{f}(x)$ there are $\approx q^n/n$ mappings;
  - For any $\boldsymbol{a}(x) \in \mathbb{X}$, it should have $\approx q^n/n$ images in different $\mathbb{Y}$s;
  - There is no reason that the mapping isn't random since $\boldsymbol{f}(x)$ and $\boldsymbol{F}(y)$ are both chosen at random.

The story so far

- With Yarkin Doroz, Jill Pipher and Berk Sunar, we proposed a fully homomorphic encryption scheme.
- It remains to be shown how to build signature scheme:
  - Both Fiat-Shamir and GPV doesn't seem to work for FFI.
  - But FFI does enable an additional feature: trapdoor hiding.

Trapdoor hiding

Lattice with a uSVPs

- $\boldsymbol{v} \in \mathcal{L}_{\mathbb{X}} \subset \mathbb{F}$ is a unique shortest vector of $\mathcal{L}_{\mathbb{X}}$;
- $\boldsymbol{V} \in \mathcal{L}_{\mathbb{Y}} \subset \mathbb{F}$ will be random, i.e., not a unique shortest vector of $\mathcal{L}_{\mathbb{Y}}$;
- There is no reason $\mathcal{L}_{\mathbb{Y}}$ has any unique shortest vector.

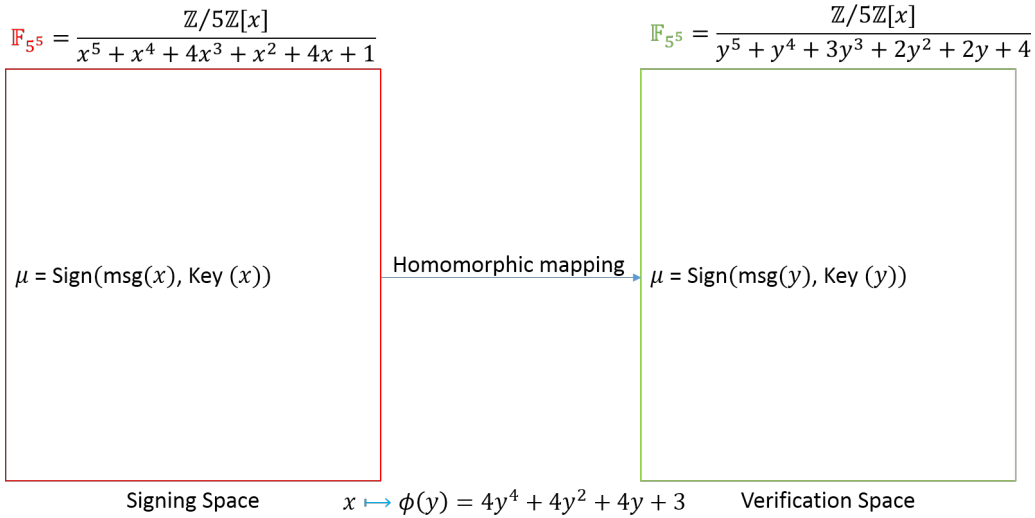
Trapdoor hiding

The NTRU setting

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

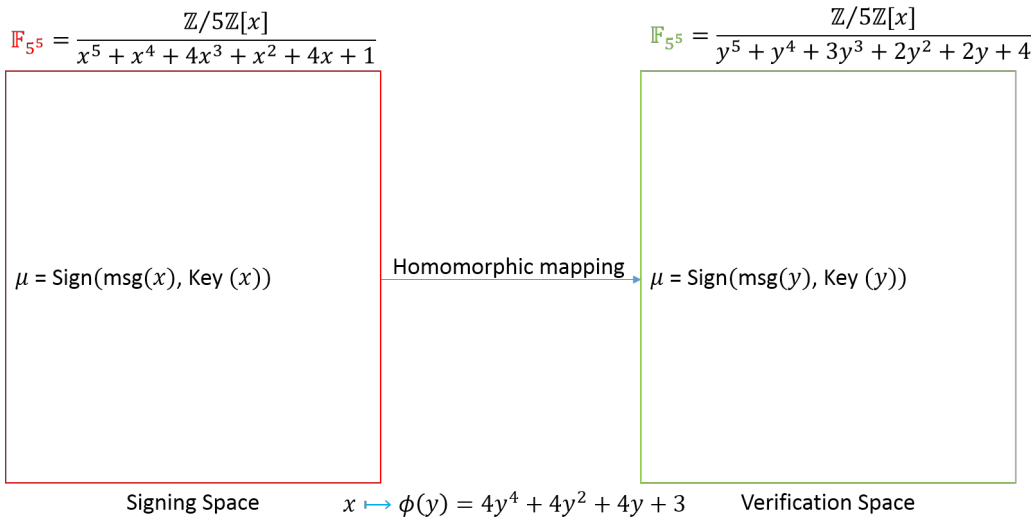
- $h(x) = a(x)/b(x) \mapsto H(y) = A(y)/B(y)$
- $L_{\boldsymbol{h}}$ is an NTRU lattice with unique short vectors $\langle a(x), b(x)\rangle$;
- $\langle A(y), B(y)\rangle$ are not short in $L_{\boldsymbol{H}}$, likely $L_{\boldsymbol{H}}$ does not have any unique short vectors.

Overview of the signature scheme



- 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.

"Improvement"



- Lattice attacks on the NTRU public keys are infeasible;
- smaller signatures
  - IF FFI is significantly harder than lattice problems.

Key Generation - I

Isomorphism

- Generate a finite field homomorphism $\{\boldsymbol{f}, \boldsymbol{F}, \boldsymbol{\psi}, \boldsymbol{\phi}\}$.

NTRU

- Choose a small integer p that is co-prime to q.
- Generate two sparse small polynomials $\boldsymbol{a}(x)$ and $\boldsymbol{b}(x)$.
- Compute $\boldsymbol{h}(x) \equiv \left(p\boldsymbol{a}(x)\right)^{-1}\boldsymbol{b}(x) \pmod{\boldsymbol{f}(x)} \in \mathbb{X}$.
- Compute $\boldsymbol{H}(y) \in \mathbb{Y}$, the image of $\boldsymbol{h}(x)$ in $\mathbb{Y}$.

Challenge

How do we prove to the verifier that a Y-space element has small image in $\mathbb{X}$-space.

We rely on a variant subset sum problem

- Publish a set of polynomials in $\mathbb{Y}$ that forms a basis of the vector space
- Images of short X-space elements can be written as short linear combinations of $\{\boldsymbol{C}_i(y)\}$.

Key Generation - II

An additional building block

- Choose an invertible n-by-n matrix U with small coefficients.
- Define $\boldsymbol{c}_1(x), \boldsymbol{c}_2(x), \cdots, \boldsymbol{c}_n(x) \in \mathbb{X}$ by the relation

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

- Compute the images $\boldsymbol{C}_1(y), \ldots, \boldsymbol{C}_n(y) \in \mathbb{Y}$.
- NOTE:

security

- There are many ways to decompose $(x, x^2, \ldots, x^n)^T$
- Under FFI, the attacker will not be able to tell the decomposition since $\boldsymbol{C}_1(y), \ldots, \boldsymbol{C}_n(y)$ appears to be uniform.

Key Generation - III

Final keys

- $pk := \{n, p, q, \boldsymbol{H}(y), \boldsymbol{C}_1(y), \ldots, \boldsymbol{C}_n(y)\}$
- $sk := \{\boldsymbol{f}, \psi, \phi, \boldsymbol{a}(x), \boldsymbol{b}(x), \boldsymbol{c}_1(x), \ldots, \boldsymbol{c}_n(x)\}$.

Signing

High level

- Find a lattice vector $(\boldsymbol{s}, \boldsymbol{t}) \in \mathcal{L}_{\boldsymbol{h}}$
- Express $(\boldsymbol{s}, \boldsymbol{t})$ with basis $\boldsymbol{c}_1(x), \ldots, \boldsymbol{c}_n(x)$:
  - $\boldsymbol{s}(x) = \sum_{i=1}^{n} \delta_i \boldsymbol{c}_i(x)$; $\boldsymbol{t}(x) = \sum_{i=1}^{n} \epsilon_i \boldsymbol{c}_i(x)$.
- $\mathit{Hash}(\mu, pk) \equiv (\boldsymbol{\delta}, \boldsymbol{\epsilon}) \bmod p$;
- Use rejection sampling to ensure $(\boldsymbol{\delta}, \boldsymbol{\epsilon})$ is uniform

Verification

- Build $\boldsymbol{S} := \sum_{i=1} \delta_i \boldsymbol{C}_i(y)$ and $\boldsymbol{T} := \sum_{i=1} \epsilon_i \boldsymbol{C}_i(y) \in \mathbb{Y}$;
- Check $(\boldsymbol{S}, \boldsymbol{T}) \in \mathcal{L}_{\boldsymbol{H}}$: $\boldsymbol{S}(y)\boldsymbol{H}(y) = \boldsymbol{T}(Y)$;
- Check $\mathit{Hash}(\mu, pk) \equiv (\boldsymbol{\delta}, \boldsymbol{\epsilon}) \bmod p$.

Limitations and future works

- Prove the hardness of FFI problem.
- Average-case/worse-case hardness.
- Understand concrete security w.r.t. practical parameters.
- Build a cleaner signature scheme.
  - Unforgibility depends only on FFI problem.

Thank you