CISPA
HELMHOLTZ CENTER FOR
INFORMATION SECURITY

On the hardness of the Finite Field Isomorphism Problem

Dipayan Das, Antoine Joux

Hard Problems

- Cryptography relies on the assumptions of hard problems.

- Most assumptions in the literature of lattice-based cryptography are conjectured hard based on a transformation to a lattice problem.

- This talk: The approach is not always reliable (by counterexample).

Reminders from Finite field theory

- Finite field with q elements : F_q

- Finite field with q^n elements (n degree extension of F_q): F_{q^n}

- Isomorphic representations of F_{q^n} using irreducible polynomials over F_q

$$F_q[x]/f(x) \approx F_q[y]/F(y) \approx \ldots$$

- To find an explicit isomorphism, it is enough to know the roots of one polynomial in F_{q^n} in terms of the other representation

Finite Field Isomorphism (FFI) distribution

Private:	**Public:**
Uniform sparse ternary irreducible polynomial: $f(x) = x^n + g(x)$, $\deg(g) \leq \frac{n}{2}$	Uniform irreducible polynomial: $F(y)$
Pick an Isomorphism: ϕ	
Sample β- bounded linear combinations of powers of x: $a_i(x)$	$A_i(y) = \phi(a_i(x))$

"Good" representation in polynomial x −basis

"Bad" representation in polynomial y −basis

FFI problem [DHP+18,HSWZ20]

Given $F(y), A_1(y), A_2(y), \dots, A_k(y)$ **decide** if $A_i(y)$s come from FFI distribution **or** uniform distribution.

This is the Decisional FFI (DFFI) problem.

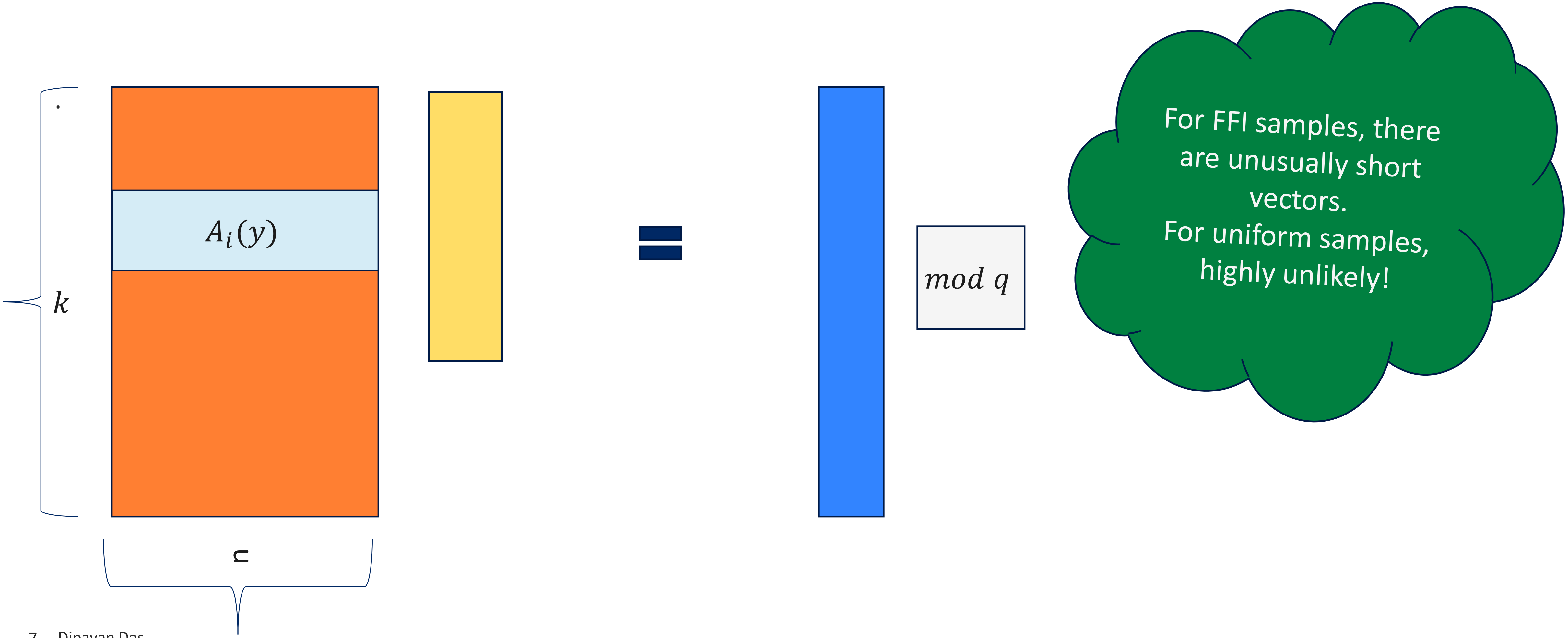
[DHP+18]: Y. Doröz, J. Hoffstein, J. Pipher, J. Silverman, B. Sunar, W. Whyte, and Z. Zhang. Fully homomorphic encryption from the finite field isomorphism problem. PKC'18.

[HSWZ20]: J. Hoffstein, J. Silverman, W. Whyte, Z. Zhang. A signature scheme from the finite field isomorphism problem. JoMC'20.

Toy example:

```
n=16
q=32771

f(x)=x^16 + x^7 + x^5 -x^3 - x^2 -x + 1

F(y)=y^16 + 4152*y^15 + 2594*y^14 + 26843*y^13 + 27498*y^12 + 31444*y^11
+ 15956*y^10 + 7616*y^9 + 30326*y^8 + 26729*y^7 + 8558*y^6 + 4785*y^5 +
27721*y^4 + 1198*y^3 + 14942*y^2 + 14544*y + 11277

\phi= 28228*y^15 + 13643*y^14 + 21168*y^13 + 4909*y^12 + 25475*y^11 +
21646*y^10 + 23297*y^9 + 19665*y^8 + 5019*y^7 + 1677*y^6 + 6823*y^5 +
15399*y^4 + 23882*y^3 + 242*y^2 + 18578*y + 31824

x-basis representataions
y-basis representations


x^14 + x^12 + x^10 + x^9 + x^8 -x^7 -x^6 -x^5 -x^4 -x^3 -x


28795*y^15 + 757*y^14 + 4649*y^13 + 30560*y^12 + 21773*y^11 + 19702*y^10
+ 14924*y^9 + 22488*y^8 + 29775*y^7 + 7212*y^6 + 5478*y^5 + 4488*y^4 +
9598*y^3 + 3290*y^2 + 19954*y + 25737


x^13 -x^12 + x^10 -x^9 + x^7 + x^5 -x^4 + x^3 -x^2 -x + 1


22173*y^15 + 15726*y^14 + 3731*y^13 + 2685*y^12 + 29516*y^11 + 30642*y^10
+ 9001*y^9 + 12333*y^8 + 8722*y^7 + 3340*y^6 + 28353*y^5 + 9853*y^4 +
32035*y^3 + 25337*y^2 + 19076*y + 29241


-x^15 + x^12 -x^11 -x^10 + x^8 -x^6 -x^5 -x^3 -x^2 -*x -1


25606*y^15 + 24744*y^14 + 20203*y^13 + 1563*y^12 + 10690*y^11 +
20096*y^10 + 22744*y^9 + 30083*y^8 + 16058*y^7 + 10331*y^6 + 30479*y^5 +
27544*y^4 + 19920*y^3 + 3869*y^2 + 6833*y + 2377
```

Previous attack on DFFI problem [DHP+18,HSWZ20]



FHE from FFI problem (oversimplified) [DHP+18]

Let $p = 2$

$m_a, m_b \in \{0,1\}$

- $\text{Enc}(m_a) = C_a = pC(y) + m_a$, $\text{Enc}(m_b) = C_b = pC'(y) + m_b$
- $\text{Dec}(C_a) = (pc(x) + m_a) \; mod \; p = m_a$
- $\text{Dec}(C_a + C_b) = (p\, c(x) + pc'(x) + m_a + m_b \,) mod \; p = m_a + m_b$
- $\text{Dec}(C_a . C_b) = (p^2\, c(x)c'(x) + p\, c(x)m_b + pc'(x)m_a + m_a . m_b) \; mod \; p = m_a . m_b$

Bounded Expansion factor

The sparse ternary choice of $f(x)$ bounds the noise growth after multiplications

Correctness: Choose q sufficiently large to avoid modular reductions in x-basis representations

Trace of finite field

Let $\alpha \in F_{q^n}$,

$$Tr(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}} \in F_q$$

- Trace is linear.
- Trace computation is polynomial time.
- Trace is invariant under representations.

Trace of polynomial x-basis

$$f(x) = x^n + \sigma_1 x^{n-1} + \cdots + \sigma_n \text{ where } \sigma_d = 0 \text{ for } 1 \leq d \leq \frac{n}{2} - 1$$

$$\sigma_d \in \{0, \pm 1\} \text{ for } \frac{n}{2} \leq d \leq n$$

Then

$$\left|Tr\left(x^d\right)\right| = n \; mod \; q \quad \text{for } d = 0$$

$$= 0 \; mod \; q \quad \text{for } \boxed{1 \leq d \leq \frac{n}{2} - 1}$$

$$\left.\begin{aligned} &= d \; mod \; q \text{ when } \sigma_d \neq 0 \\ &= 0 \; mod \; q \text{ when } \sigma_d = 0 \end{aligned}\right\} \boxed{\frac{n}{2} \leq d \leq n - 1}$$

Using Newton-Girard formula:

$$Tr\left(x^d\right) = (-1)^d d \sum_{r_i \in \mathbb{N}: r_1 + 2r_2 + \cdots + d r_d = d} \frac{(r_1 + r_2 + \cdots r_d - 1)!}{r_1! \, r_2! \ldots r_d!} \prod_{j=1}^{d} (-\sigma_j)^{r_j}$$

Trace of polynomial x-basis

$f(x) = x^n + \sigma_1 x^{n-1} + \cdots + \sigma_n$ where $\sigma_d = 0$ for $1 \leq d \leq \frac{n}{2} - 1$

$\sigma_d \in \{0, \pm 1\}$ for $\frac{n}{2} \leq d \leq n$

Then for $1 \leq d \leq \frac{n}{2} - 1$

- $\sigma_d = 0$

$Tr(x^d) = 0 \bmod q$

Using Newton-Girard formula:

$$Tr(x^d) = (-1)^d d \sum_{r_i \in \mathbb{N}: r_1 + 2r_2 + \cdots + d r_d = d} \frac{(r_1 + r_2 + \cdots r_d - 1)!}{r_1!\, r_2! \ldots r_d!} \prod_{j=1}^{d} (-\sigma_j)^{r_j}$$

Trace of polynomial x-basis

$$f(x) = x^n + \sigma_1 x^{n-1} + \cdots + \sigma_n \text{ where } \sigma_d = 0 \text{ for } 1 \leq d \leq \frac{n}{2} - 1$$

$$\sigma_d \in \{0, \pm 1\} \text{ for } \frac{n}{2} \leq d \leq n$$

Then for $\frac{\mathrm{n}}{2} \leq d \leq n-1$

- Only one solution for $r_i \colon r_1 + 2r_2 + \cdots + dr_d = d$

that contributes in the sum:

$(r_1 = 0, r_2 = 0, \ldots, r_d = 1)$

$$|Tr(x^d)| = d \; mod \; q \text{ when } \sigma_d \neq 0$$

$$= 0 \; mod \; q \text{ when } \sigma_d = 0$$

Using Newton-Girard formula:

$$Tr(x^d) = (-1)^d d \sum_{r_i \in \mathbb{N} : r_1 + 2r_2 + \cdots + dr_d = d} \frac{(r_1 + r_2 + \cdots r_d - 1)!}{r_1! \, r_2! \ldots r_d!} \prod_{j=1}^{d} (-\sigma_j)^{r_j}$$

Trace of FFI samples

Let $a_i(x)$ is a β −bounded linear combinations of polynomial x-basis.

Then $\left|Tr\left(a_i(x)\right)\right| = \left|Tr\left(A_i(y)\right)\right| \leq \beta n^2$

Polynomial-time attack on DFFI problem

- Let $q > 4\beta n^2$
- Let $A_1(y), A_2(y), \ldots, A_k(y)$ be the given samples.

Compute the trace of the samples.

Absolute value of traces $\leq \beta n^2$, output FFI distribution.

Otherwise, output uniform distribution.

Advantage of the attack: $1 - \frac{1}{2^k}$

Trace is uniformly distributed over F_q for uniform samples.

Polynomial-time semantic attack on the FHE

Let p is not a divisor of n

$C_a = pC(y) + m$, where $m \in \{0,1\}$

$Tr(C_a) = pTr(c(x)) + Tr(m)$ is small.

$$Tr(C_a) mod\, p = 0, \text{Return } m = 0$$
$$= 1, \text{Return } m = 1$$

Polynomial-time semantic attack on the FHE

Let p is a divisor of n

$C_a \; = pC(y) + m$, where $m \in \{0,1\}$

Pick any FFI sample C^* such that p is not a divisor of $Tr(C^*)$

$Tr(C_a . C^*) = pTr(c^*(x). c(x)) + m \, Tr(c^*(x))$ is still small.

The choice of $f(x)$ makes sure the coefficients of the product in x-basis are small.

$Tr(C_a C^*) mod \, p = 0$, Return $m = 0$
$= 1$, Return $m = 1$

The large modulus makes sure there is no modular reduction!

Questions??

Paper details: https://eprint.iacr.org/2022/998

QR Code: