Constructing Monogenic Fields of Cryptographic Size

Swechchha Adhikari, Daphne Plott

Brigham Young University
Department of Mathematics

July 6, 2026

Ring Learning with Errors

We want:

- $f(x)$ to be monic and irreducible over $\mathbb{Q}$
- $f(x)$ to generate a monogenic number field
- $\deg(f(x))$ to be large

Our Transformation

Our Transformation

Let f be any monic polynomial with integer coefficients. We generate a palindromic polynomial $F(x)$ as

$$F(x) = x^n f(\tfrac{1}{x} + c + x),$$

where $c \in \mathbb{Z}$ and $n = \deg(f)$.

Our Transformation

$$F(x) = x^n f(\tfrac{1}{x} + c + x)$$

Example

Let $c = 2$ and $f(x) = x^2 + 3x - 2$. We find

$$F(x) = x^2 \cdot f(\tfrac{1}{x} + 2 + x)$$

$$= x^4 + 7x^3 + 10x^2 + 7x + 1$$

Our Approach

If $F(x) = F_1(x)F_2(x)$, can we reverse the transformation on each of F_1 and F_2 to get f_1 and f_2 such that $f(x) = f_1(x)f_2(x)$?

Possible Factoring of $F(x)$

- $F(x)$ is irreducible
- $F(x) = p_1 \cdot p_2 \cdots p_n$
- $F(x) = g_1 \cdot g_2 \cdots g_m$
- $F(x) = p_1 \cdots p_n \cdot g_1 \cdots g_m$

Non-Palindromic Factors

Theorem (Cafure, Cesaretto)

If $F(x)$ is palindromic, and $g(x)$ is a factor of $F(x)$, then $g^{rev}(x)$ is also a factor of $F(x)$, where $g^{rev}(x) = x^m g(\frac{1}{x})$ and m is the degree of $g(x)$.

Example

If $g(x) = 3x^2 + x + 5$, then $g^{rev}(x) = 5x^2 + x + 3$.

Possible Factoring of $F(x)$

- $F(x)$ is irreducible
- $F(x) = p_1 \cdot p_2 \cdots p_n$
- $F(x) = g_1 \cdot g_1^{rev} \cdot g_2 \cdot g_2^{rev} \cdots g_m \cdot g_m^{rev}$
- $F(x) = p_1 \cdots p_n \cdot g_1 \cdot g_1^{rev} \cdots g_m \cdot g_m^{rev}$

Possible Factoring of $F(x)$

- $F(x)$ is irreducible
- $F(x) = p_1 \cdot p_2 \cdots p_n$
- $F(x) = g \cdot g^{rev}$

Constructing a Reverse Transformation

$$F(x) = \sum a_k x^k$$

Constructing a Reverse Transformation

$$F(x) = a_0 x^n + \sum a_k (x^{n+k} + x^{n-k})$$

Example

If $F(x) = x^4 + 7x^3 + 10x^2 + 7x + 1$, then we can rewrite it as

$$F(x) = 10x^2 + 7(x^3 + x) + 1(x^4 + 1)$$

Constructing a Reverse Transformation

$$F(x) = a_0 x^n + \sum a_k (x^{n+k} + x^{n-k})$$

Choose h_k such that:

$$x^n h_k(\tfrac{1}{x} + c + x) = x^{n+k} + x^{n-k}$$

Constructing a Reverse Transformation

$$F(x) = a_0 x^n + \sum a_k (x^{n+k} + x^{n-k})$$

$$F(x) = x^n (a_0 + \sum a_k h_k (\tfrac{1}{x} + c + x))$$

Constructing a Reverse Transformation

$$F(x) = a_0 x^n + \sum a_k (x^{n+k} + x^{n-k})$$

$$F(x) = x^n (a_0 + \sum a_k h_k (\tfrac{1}{x} + c + x))$$

$$f(x) = a_0 + \sum a_k h_k (x)$$

Irreducibility Criteria

Theorem (Adhikari, McKean, Plott, Torgersen)

Let $F(x) = x^n f(\frac{1}{x} + c + x)$, where n is the degree of $f(x)$. If $f(x)$ is irreducible, then $F(x)$ has no palindromic factors.

Corollary (Cafure, Cesaretto)

If $F(x)$ has no palindromic factors, then either:

1. $F(x) = gg^{rev}$
2. $F(x)$ is irreducible

Irreducibility Criteria

Corollary (Adhikari, McKean, Plott, Torgersen)

Given a palindromic $F(x)$ that is the result of the transformation $F(x) = x^n f(\frac{1}{x} + c + x)$ where $f(x)$ is irreducible,

1. If $|F(1)|$ or $|F(-1)|$ is not a perfect square, then $F(x)$ is irreducible.
2. If $F(1)$ and the middle coefficient of $F(x)$ have different signs, then F is irreducible.

Monogenic Criteria

Ring of Integers

Take irreducible $f = x^2 - 2 \implies \mathbb{Q}(\sqrt{2})$ is a (number) field!

$$\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}]$$

$\mathcal{O}_K =$ the set of all roots of monic polynomials over $\mathbb{Z}$

Monogenic Number Fields

$$\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}]$$

$$\mathcal{O}_{\mathbb{Q}(\sqrt{5},\sqrt{13})} = \mathbb{Z}\left[\tfrac{1+\sqrt{5}}{2}, \tfrac{1+\sqrt{13}}{2}\right]$$

Which *number field* is monogenic?

- $\mathcal{O}_K$ generated by a single element

Checking Monogenicity

Option 1:

- Compute the ring of integers
- Check if it's generated by a single element

Checking Monogenicity

Option 1:

- Compute the ring of integers
- Check if it's generated by a single element

Generally very difficult to check

Checking Monogenicity

Option 2:

- Compute $\frac{\operatorname{disc} f}{\operatorname{disc} K} = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2$
- If this ratio equals 1, $\mathbb{Z}[\alpha] = \mathcal{O}_K$

Discriminant of the Transformed Polynomial

Let $f = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$ be monic, then

$$\operatorname{disc}(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$$

Discriminant of the Transformed Polynomial

Let $f = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$ be monic, then

$$\operatorname{disc}(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$$

Roots of F?

Discriminant of the Transformed Polynomial

Roots of $F(x)$:

$$\frac{(\alpha - c) \pm \sqrt{(\alpha - c)^2 - 4}}{2}.$$

Discriminant of the Transformed Polynomial

Roots of $F(x)$:

$$\frac{(\alpha - c) \pm \sqrt{(\alpha - c)^2 - 4}}{2}.$$

Discriminant of $F(x)$:

Adhikari, McKean, Plott, Torgersen '26

$$\operatorname{disc}(F) \;=\; \operatorname{disc}(f)^2 \, f(c+2) \, f(c-2).$$

Discriminant of K

Recall:

$$\frac{\operatorname{disc} f}{\operatorname{disc} K} = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2$$

Discriminant of K

Recall:

$$\frac{\operatorname{disc} f}{\operatorname{disc} K} = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2$$

Discriminant of the number field K?

Discriminant of K

Recall:

$$\frac{\operatorname{disc} f}{\operatorname{disc} K} = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2$$

Discriminant of the number field K?

Generally very difficult to compute!

Conductor-Discriminant Formula

Conductor-Discriminant Formula

For any two number fields $A \subset B$, we have $\mathrm{disc}(A)^{[B:A]} | \mathrm{disc}(B)$.

Conductor-Discriminant Formula

Adhikari, McKean, Plott, Torgersen '26

If β is a root of F then $\alpha = \beta + \beta^{-1} + c$ is a root of f. This gives us $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\beta)$.

Conductor-Discriminant Formula

Fact: $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\beta)$

Conductor-Discriminant Formula

Fact: $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\beta)$

Conductor-Discriminant Formula

For any two number fields $A \subset B$, we have $\text{disc}(A)^{[B:A]} | \text{disc}(B)$.

$[\mathbb{Q}(\beta) : \mathbb{Q}(\alpha)] = 2$, so

$$\text{disc}(\mathbb{Q}(\alpha))^2 \mid \text{disc}(\mathbb{Q}(\beta))$$

Conductor-Discriminant Formula

Fact: $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\beta)$

Conductor-Discriminant Formula

For any two number fields $A \subset B$, we have $\mathrm{disc}(A)^{[B:A]} | \mathrm{disc}(B)$.

$[\mathbb{Q}(\beta) : \mathbb{Q}(\alpha)] = 2$, so

$$\mathrm{disc}(\mathbb{Q}(\alpha))^2 \mid \mathrm{disc}(\mathbb{Q}(\beta))$$

Assuming f is monogenic, $\mathrm{disc}(f) = \mathrm{disc}(\mathbb{Q}(\alpha))$, hence

$$\mathrm{disc}(f)^2 \mid \mathrm{disc}(\mathbb{Q}(\beta))$$

Discriminant Ratio

$$\frac{\operatorname{disc}(F)}{\operatorname{disc}(\mathbb{Q}(\beta))} = \frac{\operatorname{disc}(f)^2 f(c+2)f(c-2)}{\operatorname{disc}(f)^2 k}$$

$$= \frac{f(c+2)f(c-2)}{k}$$

$$= [\mathcal{O}_{\mathbb{Q}(\beta)} : \mathbb{Z}[\beta]]^2$$

$$\Rightarrow \quad f(c+2)f(c-2) = k \cdot [\mathcal{O}_{\mathbb{Q}(\beta)} : \mathbb{Z}[\beta]]^2$$

Square-Free Consequence

$$f(c+2)f(c-2) = k \cdot [\mathcal{O}_{\mathbb{Q}(\beta)} : \mathbb{Z}[\beta]]^2$$

$$f(c+2)f(c-2) \text{ square-free } \Rightarrow \text{ only square divisor } = 1$$

Square-Free Consequence

$$f(c+2)f(c-2) = k \cdot [\mathcal{O}_{\mathbb{Q}(\beta)} : \mathbb{Z}[\beta]]^2$$

$$f(c+2)f(c-2) \text{ square-free } \Rightarrow \text{ only square divisor } = 1$$

$$[\mathcal{O}_{\mathbb{Q}(\beta)} : \mathbb{Z}[\beta]] = 1$$

$$\mathcal{O}_{\mathbb{Q}(\beta)} = \mathbb{Z}[\beta]$$

A Sufficient Condition for Monogenicity

Adhikari, McKean, Plott, Torgersen (2026)

Let $f \in \mathbb{Z}[x]$ be monic and irreducible of degree $n \geq 2$, and define

$$F(x) = x^n f\left(x + \frac{1}{x} + c\right).$$

Assume that the number field $\mathbb{Q}[x]/(f)$ is monogenic. Then $\mathbb{Q}[x]/(F)$ is also monogenic provided that

$$f(c+2)\, f(c-2) \text{ is square-free.}$$

The End

Thank you!

Discriminant Simplification

$$\begin{aligned}\operatorname{disc}(F) &= \operatorname{disc}(f)^2 \cdot \prod_{i=1}^{n} \left((\alpha_i - c)^2 - 4\right) \\ &= \operatorname{disc}(f)^2 \cdot \prod_{i=1}^{n} (\alpha_i - c - 2)(\alpha_i - c + 2) \\ &= \operatorname{disc}(f)^2 \, f(c+2) \, f(c-2)\end{aligned}$$