Radboud University

An Algebraic Approach to Symmetric Linear Layers in Cryptographic Primitives

Robert Christian Subroto,
Radboud University (The Netherlands)
September 16, 2022

ESCADA

- The Subterranean 2.0 cipher suite is a lightweight cryptographic primitive which can be used for several types of authenticated encryption schemes [1]
- Its round function consists of the following composition:

$$\underline{\pi_s \circ \theta_s} \circ \iota \circ \chi : \mathbb{F}_2^{257} \rightarrow \mathbb{F}_2^{257}$$

- Both π_s and θ_s are linear maps, and are described as follows:
  - The i-th coordinate of $\theta_s(x)$ equals $x_i + x_{i+3 \bmod 257} + x_{i+8 \bmod 257}$
  - The i-th coordinate of $\pi_s(x)$ equals $x_{12i \bmod 257}$

[1] Daemen, J., Massolino, P.M.C., Mehrdad, A., Rotella, Y.: The subterranean 2.0 cipher suite. IACR Transactions on Symmetric Cryptology pp. 262–294 (2020)

- **Observation:** $\text{ord}(\pi_s \circ \theta_s) = 256$
- This is relatively low, which could be a potential weakness against **invariant subspace attacks** [2]
- **Goal:** Develop a mathematical framework to better understand and design linear maps π and θ which are "*similar*" to π_s and θ_s such that $\text{ord}(\pi \circ \theta)$ is high
- Concepts of abstract algebra prove to be very useful

[2] Beierle, C., Canteaut, A., Leander, G., Rotella, Y.: Proving resistance against invariant attacks: How to choose the round constants. In: Katz, J., Shacham, H. (eds.) Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II. Lecture Notes in Computer Science, vol. 10402, pp. 647–678. Springer (2017).

Outline

Circulant Matrices - Generalization of θ_s

Multiplicative Shuffles - Generalization of π_s

Composition

Two Upper Bounds

Circulant Matrices - Generalization of θ_s

Definition

- An $m \times m$-**circulant matrix** V over $\mathbb{F}$ is a matrix of the form

$$V = \begin{pmatrix} v_0 & v_{m-1} & \cdots & v_2 & v_1 \\ v_1 & v_0 & v_{m-1} & & v_2 \\ \vdots & v_1 & v_0 & \ddots & \vdots \\ v_{m-2} & & \ddots & \ddots & v_{m-1} \\ v_{m-1} & v_{m-2} & \cdots & v_1 & v_0 \end{pmatrix}$$

- V is **uniquely determined** by its first column vector $v = (v_0, ..., v_{m-1})^{\mathsf{T}}$
- For this reason: $V = \mathrm{circ}(v)$
- Set of $m \times m$-circulant matrices: $\mathcal{C}_{\mathbb{F},m}$ or $\mathcal{C}_m$
- Set of *invertible* $m \times m$-circulant matrices: $\mathcal{C}^*_{\mathbb{F},m}$ or $\mathcal{C}^*_m$

Ring of Circulant Matrices

- $\mathcal{C}_{\mathbb{F},m}$ is a ring with matrix addition and multiplication
- We have the isomorphism

$$\Phi : \mathcal{C}_{\mathbb{F},m} \to \mathbb{F}[X]/\langle X^m - 1\rangle, \;\; \text{circ}(v) \mapsto \sum_{i=0}^{m-1} v_i \cdot X^i \bmod \langle X^m - 1\rangle$$

- For algebraic purposes, it is easier to consider circulant matrices as polynomials in $\mathbb{F}[X]/\langle X^m - 1\rangle$
- **Notation:** Let μ_m be the m-roots of unity in $\overline{\mathbb{F}}$

Theorem

Let m be coprime to $\mathrm{char}(\mathbb{F})$.

- $f \in \mathbb{F}[X]$ is invertible modulo $\langle X^m - 1 \rangle$ if and only if $f(\zeta) \neq 0$ in $\overline{\mathbb{F}}$ for all $\zeta \in \mu_m$
- For invertible f, we have $\mathrm{ord}(f) = \mathrm{lcm}(\mathrm{ord}_{\overline{\mathbb{F}}}(f(\zeta)) : \zeta \in \mu_m)$

Proof (Sketch)

- Let $\mathbb{F}$ be algebraically closed
- By Chinese Remainder Theorem:

$$\mathbb{F}[X]/\langle X^m - 1 \rangle \to \bigoplus_{\zeta \in \mu_m} \mathbb{F}[X]/\langle X - \zeta \rangle \to \bigoplus_{\zeta \in \mu_m} \mathbb{F}, \ f \mapsto (f(\zeta))_{\zeta \in \mu_m}$$

- Hence the above statements are valid for $\mathbb{F}$ algebraically closed
- By the *Division Algorithm for Polynomials*, it is also valid for all $\mathbb{F}$ □

An Important Corollary

Theorem

Let m be coprime to $\mathrm{char}(\mathbb{F})$.

- $f \in \mathbb{F}[X]$ is invertible modulo $\langle X^m - 1 \rangle$ if and only if $f(\zeta) \neq 0$ in $\overline{\mathbb{F}}$ for all $\zeta \in \mu_m$
- For invertible f, we have $\mathrm{ord}(f) = \mathrm{lcm}(\mathrm{ord}_{\overline{\mathbb{F}}}(f(\zeta)) : \zeta \in \mu_m)$

Corollary

Let m be coprime to $\mathrm{char}(\mathbb{F})$.

- If $f \in \mathbb{F}[X]$ is invertible modulo $\langle X^m - 1 \rangle$, then $f(X^t) \in \mathbb{F}[X]$ is also invertible modulo $\langle X^m - 1 \rangle$ for all $t \in \mathbb{Z}_{>0}$
- For invertible f, we have that $\mathrm{ord}(f(X^t)) \mid \mathrm{ord}(f)$

Multiplicative Shuffles - Generalization of π_s

Definition (Multiplicative Shuffles)

Let $g \in (\mathbb{Z}/m\mathbb{Z})^*$. The **multiplicative shuffle with shuffling factor** g is defined as the map

$$\pi_g : \mathbb{F}^m \to \mathbb{F}^m, \quad x \mapsto x^*,$$

where $x^*_j = x_{gj \bmod m}$ for all $0 \leq j < m$.

- The set of multiplicative shuffles is denoted by MShuf_m

Example

- Take $m = 7$ and shuffling factor $g = 3$
- Let $x = (x_0, ..., x_6)^\mathsf{T} \in \mathbb{F}^7$
- Then $x_j^* = x_{gj \bmod m} = x_{3j \bmod 7}$

$$x = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} \xrightarrow{\pi_3} \begin{pmatrix} x_0 \\ x_3 \\ x_6 \\ x_2 \\ x_5 \\ x_1 \\ x_4 \end{pmatrix} = x^*$$

- π_g only shuffles the elements in the vector, depending on g

Multiplicative Order

- MShuf_m is a finite Abelian group
- We have the group isomorphism

$$(\mathbb{Z}/m\mathbb{Z})^* \to \mathsf{MShuf}_m, \;\; g \mapsto \pi_g$$

Lemma (Order of Multiplicative Shuffles)

By the above group isomorphism, we have

$$\mathsf{ord}(\pi_g) = \mathsf{ord}_m(g).$$

Composition

Assumptions

- Let $\mathbb{F} = \mathbb{F}_q$ with characteristic p
- Let $m > 0$ be coprime to p
- Consider $\pi_g \circ \theta$ where $\pi_g \in \mathsf{MShuf}_m$ and $\theta \in \mathcal{C}_m^*$
- Denote the group $\mathcal{G} = \langle \mathsf{MShuf}_m, \mathcal{C}_m^* \rangle$
- $\mathcal{G}$ is a multiplicative subgroup of $\mathsf{GL}_m(\mathbb{F}_q)$
- Requires understanding of the group structure $\mathcal{G}$ to find lower and upper bounds of $\mathrm{ord}(\pi_g \circ \theta)$

Properties of the group $\mathcal{G} = \langle \mathsf{MShuf}_m, \mathcal{C}_m^* \rangle$

- $\mathcal{C}_m^*$ is a normal subgroup of $\mathcal{G}$
- Every element in $\mathcal{G}$ can be uniquely written in the form $\pi_g \circ \theta$
- $\mathcal{G}/\mathcal{C}_m^* \cong \mathsf{MShuf}_m$
- For $\pi_g \circ \theta \in \mathcal{G}$, we have $\mathsf{ord}(\pi_g) \mid \mathsf{ord}(\pi_g \circ \theta)$

- **Note:** $\mathsf{ord}(\pi_g) = \mathsf{ord}_m(g)$
- **Hence:** $\mathsf{ord}_m(g) \mid \mathsf{ord}(\pi_g \circ \theta)$
- What is $(\pi_g \circ \theta)^{\mathsf{ord}_m(g)}$?

Circulant Resultant

- We represent circulant matrices by its polynomial form in $\mathbb{F}_q[X]/\langle X^m - 1\rangle$

Proposition

Consider the subgroup $\langle g\rangle$ of $(\mathbb{Z}/m\mathbb{Z})^*$. Then

$$(\pi_g \circ \theta)^{\mathrm{ord}_m(g)} = \prod_{\gamma \in \langle g\rangle} \theta(X^\gamma) \in \mathcal{C}_m^*$$

- Proof consists of standard algebra
- We define $\theta_g := \prod_{\gamma\in\langle g\rangle} \theta(X^\gamma)$
- θ_g is called the **circulant resultant**
- **Note:** $\mathrm{ord}(\pi_g \circ \theta) = \mathrm{ord}_m(g) \cdot \mathrm{ord}(\theta_g)$
- **Main goal:** to determine $\mathrm{ord}(\theta_g)$

Two Upper Bounds

Theorem (First Upper Bound)

$$\operatorname{ord}(\theta_g) \mid \operatorname{ord}(\theta)$$

Proof:

- By earlier corollary: $\operatorname{ord}(\theta(X^t)) \mid \operatorname{ord}(\theta)$ for all $t \in \mathbb{Z}_{>0}$

$$\theta_g^{\operatorname{ord}(\theta)} = \left(\prod_{\gamma \in \langle g \rangle} \theta(X^\gamma) \right)^{\operatorname{ord}(\theta)} = \prod_{\gamma \in \langle g \rangle} \theta(X^\gamma)^{\operatorname{ord}(\theta)} = \prod_{\gamma \in \langle g \rangle} 1 = 1$$

- Hence $\operatorname{ord}(\theta_g) \mid \operatorname{ord}(\theta)$ □

Prelude to the Second Upper Bound - Discrete Group Log (1/2)

- We need to introduce a concept called the **discrete group log**

Definition (Discrete Group Log)

Let G be a group, $g \in G$ and S a subgroup of G. The **discrete group log** of g over S denoted by $\mathrm{dlog}_S(g)$ is defined as

$$\mathrm{dlog}_S(g) := \min(t \in \mathbb{Z}_{>0} : g^t \in S)$$

Example:

- Let $G = (\mathbb{Z}/31\mathbb{Z})^*$, $g = 3$ and $S = \langle 6 \rangle = \{1, 5, 6, 25, 26, 30\}$
- Then: $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 27$, $3^4 \equiv 19$, $\underline{3^5 \equiv 26}$
- Hence $\mathrm{dlog}_{\langle 6 \rangle}(3) = 5$

Prelude to the Second Upper Bound - Discrete Group Log (2/2)

- Very often, G is a finite cyclic group
- For such groups G, we can determine $\text{dlog}_S(g)$ by using the following expression:

Proposition

Let G be a finite cyclic group, let $g \in G$ and let $S = \langle a \rangle$ for some $a \in G$. Then

$$\text{dlog}_{\langle a \rangle}(g) = \min \left(t \in \mathbb{Z}_{>0} : \frac{\text{ord}(g)}{\gcd(t, \text{ord}(g))} \mid \text{ord}(a) \right)$$

- The proof is based on the following property from group theory:

Proposition

Given a finite cyclic group G, for every divisor d of $|G|$, there exists a unique subgroup S_d of G such that $|S_d| = d$

Theorem (Second Upper Bound)

Let $\langle g \rangle$ be a subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$. Then

$$\mathrm{ord}(\theta_g) \mid q^{\mathrm{dlog}_{\langle g \rangle}(q)} - 1$$

Proof (Sketch):

- **Main idea:** find a (small) field extension $\mathbb{F}_{q^w}/\mathbb{F}_q$ such that $\theta_g(\zeta) \in \mathbb{F}_{q^w}$ for all $\zeta \in \mu_m$
- If we can find such $\mathbb{F}_{q^w}$, then $\mathrm{ord}(\theta_g) \mid q^w - 1$
- Using the product expression of θ_g and some Galois theory for finite fields, we find such a value $w = \mathrm{dlog}_{\langle g \rangle}(q)$
- From this, we conclude $\mathrm{ord}(\theta_g) \mid q^{\mathrm{dlog}_{\langle g \rangle}(q)} - 1$ □

Example (Subterranean 2.0)

- $m = 257$, $q = 2$ and $g = 12$
- **Note:** $2 \in \langle 12 \rangle < (\mathbb{Z}/257\mathbb{Z})^*$, hence $\mathrm{dlog}_{\langle 12 \rangle}(2) = 1$
- By Second Upper bound: $\mathrm{ord}(\theta_g) \mid 2^{\mathrm{dlog}_{\langle g \rangle}(2)} - 1 = 2^1 - 1 = 1$, hence $\mathrm{ord}(\theta_g) = 1$
- **Observe:**

$$\mathrm{ord}(\pi_s \circ \theta_s) = \mathrm{ord}(\pi_{12} \circ \theta_{12}) = \mathrm{ord}_{257}(12) \cdot \mathrm{ord}(\theta_{12}) = 256 \cdot 1 = 256$$

Conclusions

- These upper bounds help us to understand the behaviour of the linear layer
- One can use these upper bounds to find other examples with a higher order
- One can combine theory of **Mersenne prime numbers** together with the **second upper bound** to effectively construct compositions of a high order when restricting to the binary field $\mathbb{F} = \mathbb{F}_2$
- For $m = 367$, we managed to construct compositions where its order exceeds 10^{18}

Thank you for your attention!