Radbound University

Column Parity Mixers & Module Theory

Robert Christian Subroto,
Radboud University (The Netherlands)
July 13, 2023

ESCADA

- Column Parity Mixers (CPMs) [Stoffelen & Daemen, 2018] are a special type of linear maps
- Used in cryptographic primitives like XOODOO and KECCAK
- They provide a good trade-off between implementation cost and mixing power, making them well suited for lightweight cryptography

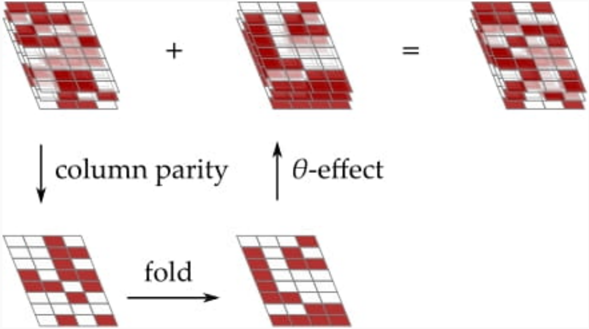
Example of a CPM: θ of Xoodoo

- Used in the linear layer of Xoodoo
- Linear map from $V = \mathbb{F}_2^{4 \cdot 32 \cdot 3} = \mathbb{F}_2^{384}$ to itself
- Described in terms of planes, lanes and the specified shifts of bits, as described in detail in the Xoodoo cookbook [Daemen et al., 2018]

$$P \leftarrow A_0 + A_1 + A_2$$

$$E \leftarrow P \lll (1,5) + P \lll (1,14)$$

$$A_y \leftarrow A_y + E, \qquad y \in \{0,1,2\}$$



Introduction & Motivation (Continued)

- CPMs in terms of linear algebra is complex and difficult for studying algebraic properties
- **Solution:** Study CPMs using module theory
- **Goals of presentation:**
  1. Re-introducing CPMs in terms of module theory
  2. Show some consequences/results of this new definition
  3. Show an interesting application of the linear layer of XOODOO

Outline

A New Approach to CPMs

Example: θ of Xoodoo

Application: Linear Layer of Xoodoo

A New Approach to CPMs

New Definition CPMs

- Let R be a commutative ring with unity, and let $z = (z_0, \dots, z_{m-1})^\intercal \in R^m$
- A **column parity mixer (CPM)** $\theta_z \colon R^m \to R^m$ is an R-linear map of the form

$$\theta_z = \begin{pmatrix} 1+z_0 & z_0 & z_0 & \cdots & z_0 \\ z_1 & 1+z_1 & z_1 & \cdots & z_1 \\ z_2 & z_2 & 1+z_2 & \cdots & z_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z_{m-1} & z_{m-1} & z_{m-1} & \cdots & 1+z_{m-1} \end{pmatrix}$$

- θ_z is uniquely determined by z, which we call the **parity folding matrix array**
- $z_0, \dots, z_{m-1}$ are the **parity folding matrices** of θ_z
- $\mathrm{CPM}_m(R)$: Set of all CPMs over R of dimension m

Properties CPMs

- **Characteristic polynomial** of θ_z:

$$p_{\theta_z}(\lambda) = \left(\left(1 + \sum_{i=0}^{m-1} z_i \right) - \lambda \right) \cdot (1 - \lambda)^{m-1}$$

- **Determinant** of θ_z:

$$\det(\theta_z) = 1 + \sum_{i=0}^{m-1} z_i$$

- θ_z is **invertible** if and only if $1 + \sum_{i=0}^{m-1} z_i$ is **invertible** in R
- The invertible CPMs form a group under matrix multiplication
- θ_z has an **eigenbasis** over R if and only if $\sum_{i=0}^{m-1} z_i$ is **invertible**

Example: θ of Xoodoo

Introducing Module Structure on the Planes

- The 4×32-planes can be modelled as the vector space $V := \mathbb{F}_2^4 \otimes_{\mathbb{F}_2} \mathbb{F}_2^{32}$
- Consider the ring $R := \mathbb{F}_2[X_1, X_2]/(X_1^4 - 1, X_2^{32} - 1)$
- Consider the map

$$\mu^*(X_1^a X_2^b, \mathrm{e}_i \otimes \mathrm{e}_j) = \mathrm{e}_{i-a \bmod 4} \otimes \mathrm{e}_{j-b \bmod 32}$$

  - **Monomials:** $X_1^a X_2^b \in R$ where $0 \leq a < 4$ and $0 \leq b \leq 32$
  - **Unit vectors:** $\mathrm{e}_i, \mathrm{e}_{i-a \bmod 4} \in \mathbb{F}_2^4$ and $\mathrm{e}_j, \mathrm{e}_{j-b \bmod 32} \in \mathbb{F}_2^{32}$ (indexing from 0)
- μ^* linearly extends to a map $\mu \colon R \times V \to V$
- (V, μ) is an R-module

Planes as Free Modules

- Consider the bijective map

$$\gamma\colon R \to V,\ X_1^a X_2^b \mapsto \mathrm{e}_a \otimes \mathrm{e}_b \quad \text{(linearly extends to all } R \text{ and } V\text{)}$$

- The module operation μ is equivalent with the product operation of R:

$$\begin{tikzcd} R \times R \arrow[r, "\cdot"] \arrow[d, "\mathrm{id}\times\gamma"] & R \arrow[d, "\gamma"] \\ R \times V \arrow[r, "\mu"] & V \end{tikzcd}$$

- (V, μ) is isomorphic to the 1-dimensional free module $(R, \cdot)$

θ as Module Endomorphism

- **Up to now**: θ is an $\mathbb{F}_2$-linear map from V^3 to V^3
- **Important observation:** θ is an (R, μ)-linear map
- **Indication:** The shift $\lll (a, b)$ is equivalent to the module action $\mu(X_1^a X_2^b, -)$
- We obtain the following commutative diagram of R-modules:

$$\begin{array}{ccc} R^3 & \xrightarrow{\theta_z} & R^3 \\ \downarrow{\scriptstyle \gamma^3} & & \downarrow{\scriptstyle \gamma^3} \\ V^3 & \xrightarrow{\theta} & V^3 \end{array}$$

- **Question:** What is the matrix representation of θ_z?

Matrix Representation of θ

- $\theta : V^3 \to V^3$ has matrix representation

$$\theta_z = \begin{pmatrix} 1+f & f & f \\ f & 1+f & f \\ f & f & 1+f \end{pmatrix}, \quad f = X_1 X_2^5 + X_1 X_2^{14}$$

- $\det(\theta_z) = 1 + 3 \cdot f = 1 + f$
- Simpler representation of θ $\to$ more convenient to study algebraically
- **Even better:** We can do something similar for the whole linear layer of Xoodoo

Application: Linear Layer of Xoodoo

Introducing The Linear Layer

- Linear layer of Xoodoo consists of the composition $\rho_{\text{west}} \circ \theta \circ \rho_{\text{east}}$
- **Problem:** It was observed experimentally that the order of the linear layer is low (only 32), which is a potential threat against invariant subspace attacks [Beierle et al., 2017]
- Using the original function description, it is hard to explain mathematically why the order of the linear layer is low
- However, this problem can be solved using the module-theoretic interpretation

Matrix Representation

- **Observation:** ρ_{west}, θ and ρ_{east} are all invertible (R, μ)-linear maps
- These maps can be modelled as endomorphisms over R^3
- The linear layer has the following matrix representation:

$$\rho_{\text{west}} \circ \theta \circ \rho_{\text{east}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & X_1 & 0 \\ 0 & 0 & X_2^{11} \end{pmatrix} \cdot \begin{pmatrix} 1+f & f & f \\ f & 1+f & f \\ f & f & 1+f \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & X_2 & 0 \\ 0 & 0 & X_1^2 X_2^8 \end{pmatrix}$$

- Using the module-theoretical approach, we can mathematically explain the low order from the algebraic structure of R

Mathematical Explanation (Sketch)

- **Note:** R is a local ring with maximal ideal $\mathfrak{m} := (X_1 - 1, X_2 - 1)$
- $q\colon R \to R/\mathfrak{m}$ induces the group homomorphism

$$\overline{q}\colon \mathrm{GL}_3(R) \to \mathrm{GL}_3(R/\mathfrak{m}), \text{ where } \overline{q}(A)_{i,j} = q(A_{i,j})$$

- **Observation:** If $M \in \ker(\overline{q})$, then $\mathrm{ord}(M) \mid 128$
- **Turns out:** $\rho_{\mathrm{west}}, \theta, \rho_{\mathrm{east}} \in \ker(\overline{q})$, which explains its low order

Conclusion

- We redefined CPMs as endomorphisms over free R-modules
- We showed that the linear layer of Xoodoo is an R-endomorphism of R^3, and we showed how this can be used to mathematically explain its low order
- **Possible follow-up topics:** Can this new interpretation of CPMs be used in designing new linear layers, or develop new cryptanalysis techniques?

Thank you for your attention!