Radboud University

Commutative algebra and symmetric cryptography

Robert Christian (Bobby) Subroto,
Radboud University (The Netherlands)
August 28, 2024

ESCADA

Introduction

- This presentation contains some work of my PhD research under ESCADA
- Main research goal: establishing deeper connections between commutative algebra and symmetric cryprography
- The results are based on three papers
- This presentation is split in three parts
- Each part corresponds to one of the three papers

Outline

Part I: Circulant rings and cyclic shifts

Part II: Semisimple circulant rings

Part III: General circulant rings

Part I: Circulant rings and cyclic shifts

Paper citation

Part I is based on the paper entitled:

An algebraic approach to circulant column parity mixers [Sub23]

Introducing circulant rings

- Let $\vec{m} := (m_1, \ldots, m_n) \in \mathbb{Z}^n_{>0}$, and let k be a field
- We define the circulant ring

$$\mathcal{C}_{\vec{m}/k} := k[X_1, \ldots, X_n]/(X_1^{m_1} - 1, \ldots, X_n^{m_n} - 1)$$

- Circulant rings are interesting both within mathematics and cryptography
  - **Mathematics:** commutative group algebras over finite abelian groups are algebraically isomorphic to circulant rings
  - **Cryptography:** circulant rings are used in constructing the mixing layer of some crypographic primitives like XOODOO (although not in this form)

Univariate circulant rings: cyclic shifts - Part 1

- Let $V_{m/k}$ be the m-dimensional vector space over a field k indexed from 0 to $m-1$
- For $v \in V_{m/k}$, we denote the i-th entry of v by v_i
- Cyclic shift by s: moves entry position i to $i+s$
- We denote this map by $\lll s : V_{m/k} \to V_{m/k},\ v \mapsto v^*$ where $v^*_i = (v_{i-s \bmod m})$

- $\mathcal{C}_{m/k}$ encapsulates also the effect of cyclic shifts
- We have the bijection

$$t_m : V_{m/k} \to \mathcal{C}_{m/k},\ v \to \sum_{0 \le i < m} v_i \cdot X^i$$

- We have the commutative diagram:

$$\begin{array}{ccc} V_{m/k} & \xrightarrow{\lll s} & V_{m/k} \\ \downarrow{\scriptstyle t_m} & & \downarrow{\scriptstyle t_m} \\ \mathcal{C}_{m/k} & \xrightarrow{\cdot X^s} & \mathcal{C}_{m/k} \end{array}$$

- This is equivalent to the theory of circulant matrices!

- Let $V_{(m_1,m_2)/k}$ be an $m_1 \times m_2$ plane with entries in k indexed by (i_1, i_2), where $0 \leq i_1 < m_1$ and $0 \leq i_2 < m_2$
- For an element $v \in V_{(m_1,m_2)/k}$, we denote the entry at position (i_1, i_2) by $v_{(i_1,i_2)}$
- Cyclic shift by (s_1, s_2): moves entry in position (i_1, i_2) to $(i_1 + s_1, i_2 + s_2)$
- We denote this map by

$$\lll (s_1, s_2) : V_{(m_1,m_2)/k} \to V_{(m_1,m_2)/k}, \ v \mapsto v^*$$

where $v^*_{(i_1,i_2)} = v_{(i_1 - s_1 \bmod m_1, i_2 - s_2 \bmod m_2)}$

- $\mathcal{C}_{(m_1,m_2)/k}$ encapsulates also the effect of cyclic shifts
- We have the bijection

$$t_{(m_1,m_2)} : V_{(m_1,m_2)/k} \to \mathcal{C}_{(m_1,m_2)/k}, \ v \to \sum_{(0,0)\leq(i,j)<(m_1,m_2)} v_{(i_1,i_2)} \cdot X_1^{i_1} X_2^{i_2}$$

- We have the commutative diagram:

$$\begin{array}{ccc} V_{(m_1,m_2)/k} & \xrightarrow{\lll(s_1,s_2)} & V_{(m_1,m_2)/k} \\ \downarrow{\scriptstyle t_{(m_1,m_2)}} & & \downarrow{\scriptstyle t_{(m_1,m_2)}} \\ \mathcal{C}_{(m_1,m_2)/k} & \xrightarrow{\cdot X_1^{s_1} X_2^{s_2}} & \mathcal{C}_{(m_1,m_2)/k} \end{array}$$

- For $\vec{m} := (m_1, \ldots, m_n)$, define $V_{\vec{m}/k}$ as the vector space over k indexed by $(i_1, \ldots, i_n)$ where $0 \leq i_j < m_j$ for all $1 \leq j \leq n$
- Shifts by $\vec{s} := (s_1, \ldots, s_n)$ on the indices are defined similarly as earlier, and denoted by $\lll \vec{s}$
- We have the bijection

$$t_{\vec{m}} : V_{\vec{m}/k} \to \mathcal{C}_{\vec{m}/k}, \ v \to \sum_{(0,,\ldots,0) \leq (i_1,\ldots,i_n) < \vec{m}} v_{(i_1,\ldots,i_n)} \cdot \prod_{j=1}^{n} X_j^{i_j}$$

- We have the commutative diagram:

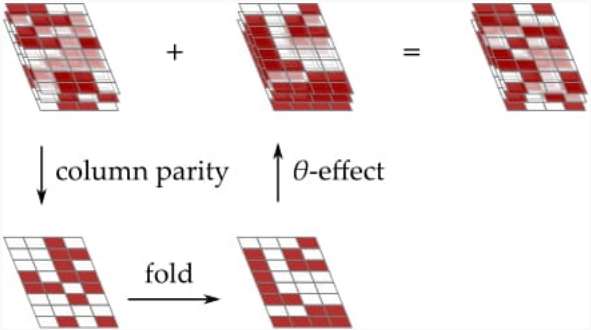
$$\begin{array}{ccc} V_{\vec{m}/k} & \xrightarrow{\lll \vec{s}} & V_{\vec{m}/k} \\ \downarrow{\scriptstyle t_{\vec{m}}} & & \downarrow{\scriptstyle t_{\vec{m}}} \\ \mathcal{C}_{\vec{m}/k} & \xrightarrow{\cdot \prod_{j=1}^{n} X_j^{s_j}} & \mathcal{C}_{\vec{m}/k} \end{array}$$

- Xoodoo is a cryptographic permutation, suitable for lightweight cryptography [DHAK18]
- We use the above insights to investigate the linear layer of Xoodoo from an alternative point of view
- The linear layer consists of a composition of 3 linear invertible maps

$$\rho_{\text{west}} \circ \theta \circ \rho_{\text{east}} : V^3_{(4,32)/\mathbb{F}_2} \to V^3_{(4,32)/\mathbb{F}_2}$$

- The construction of these maps relies heavily on cyclic shifts (next slide demonstrates θ)

$$P \leftarrow A_0 + A_1 + A_2$$
$$E \leftarrow P \lll (1,5) + P \lll (1,14)$$
$$A_y \leftarrow A_y + E, \qquad y \in \{0,1,2\}$$



- Consider the bijection $t^3_{(4,32)} : V^3_{(4,32)/\mathbb{F}_2} \to \mathcal{C}^3_{(4,32)/\mathbb{F}_2}$
- The maps $\rho_{\text{west}}, \theta, \rho_{\text{east}}$ induce corresponding maps

$$\rho^*_{\text{west}}, \theta^*, \rho^*_{\text{east}}, : \mathcal{C}^3_{(4,32)/\mathbb{F}_2} \to \mathcal{C}^3_{(4,32)/\mathbb{F}_2}$$

- Using a commutative diagram:

$$\begin{array}{ccc} V_{(4,32)/\mathbb{F}_2} & \xrightarrow{\rho_{\text{west}}, \theta, \rho_{\text{east}}} & V_{(4,32)/\mathbb{F}_2} \\ \downarrow t^3_{(4,32)} & & \downarrow t^3_{(4,32)} \\ \mathcal{C}_{(4,32)/\mathbb{F}_2} & \xrightarrow{\rho^*_{\text{west}}, \theta^*, \rho^*_{\text{east}}} & \mathcal{C}_{(4,32)/\mathbb{F}_2} \end{array}$$

- How do the maps $\rho^*_{\text{west}}, \theta^*, \rho^*_{\text{east}}$ look like?

Linear layer of Xoodoo - Module automorphism

- Because the cyclic shifts only happen on the level of planes, one can show that $\rho^*_{\text{west}}, \theta^*, \rho^*_{\text{east}}$ are linear under scaling over $\mathcal{C}_{(4,32)/\mathbb{F}_2}$
- Concretely, for $\mathbf{x}, \mathbf{y} \in \mathcal{C}^3_{(4,32)/\mathbb{F}_2}$ and $c \in \mathcal{C}_{(4,32)/\mathbb{F}_2}$:

$$\theta^*(\mathbf{x} + \mathbf{y}) = \theta^*(\mathbf{x}) + \theta^*(\mathbf{y})$$
$$\theta^*(c \cdot \mathbf{x}) = c \cdot \theta^*(\mathbf{x})$$

- Similarly for ρ^*_{east} and ρ^*_{west}
- In commutative algebra terms: these maps are $\mathcal{C}_{(4,32)/\mathbb{F}_2}$-module automorphisms over the free $\mathcal{C}_{(4,32)/\mathbb{F}_2}$-module of rank 3
- As a result, these maps have unique 3×3-matrix representations with entries in $\mathcal{C}_{(4,32)/\mathbb{F}_2}$!

- The linear maps has the following matrix representation:

$$\rho^*_{\text{west}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & X_1 & 0 \\ 0 & 0 & X_2^{11} \end{pmatrix} \quad \rho^*_{\text{east}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & X_2 & 0 \\ 0 & 0 & X_1^2 X_2^8 \end{pmatrix} \quad \theta^* = \begin{pmatrix} 1+f & f & f \\ f & 1+f & f \\ f & f & 1+f \end{pmatrix}$$

  where $f = X_1 X_2^5 + X_1 X_2^{14}$

- This approach establishes deeper connections between the behaviour of linear layer of XOODOO, and the algebraic structure of $\mathcal{C}_{(4,32)/\mathbb{F}_2}$
- An example: Using this approach, we managed to provide a mathematical explanation why the order of this linear layer is low (32), using the algebraic properties of $\mathcal{C}_{(4,32)/\mathbb{F}_2}$

Part II: Semisimple circulant rings

Paper citation

Part II is based on the paper entitled:

Wedderburn decomposition of commutative semisimple group algebras using the Combinatorial Nullstellensatz [Sub24]

Intuition: Prime number factorization

- **Prime factorization theorem:** every integer has a unique prime factorization
- Prime numbers are the building blocks for all integers
- Knowing the prime factorization of an integer m gives a lot of information about m
- Can the same ideas be applied to rings?
  - How does one compose rings?
  - What type of rings serve as the "prime numbers"?
  - Which rings admits such a decomposition/factorization?
- **Note:** We only consider commutative rings

(Semi)simple rings

- **Simple rings:** A ring R is simple if it does not contain any proper two-sided ideals
  - Simple rings are natural candidates to serve as fundamental building blocks
  - Simple commutative rings are fields
- **Semisimple rings:** A ring R is semisimple if there exists finitely many simple rings $R_1, \ldots, R_n$ such that

$$R \cong R_1 \oplus R_2 \oplus \ldots \oplus R_n$$

- **Krull-Remak-Schmidt:** Such a decomposition is unique up to isomorphism!
- If a semisimple ring R is commutative, then R is a direct sum of fields

- Are all circulant rings $\mathcal{C}_{\vec{m}/k}$, with $\vec{m} := (m_1, \ldots, m_n)$, always semisimple? NO!
- When is $\mathcal{C}_{\vec{m}/k}$ semisimple?

Maschke's Theorem

$\mathcal{C}_{\vec{m}/k}$ is semisimple if and only if $m_1, \ldots, m_n$ are all coprime to the characteristic of k.

Questions:

- What are the simple components of a semisimple circulant ring $\mathcal{C}_{\vec{m}/k}$?
- What about the case when $k = \mathbb{F}_q$?

Geometric group action

Define $k_{\vec{m}} := k(\mu_{m_1}, \ldots, \mu_{m_n})$, and define $\mathcal{V}(\mathfrak{a}_{\vec{m}}) := \mu_{m_1} \times \cdots \times \mu_{m_n} \subset \overline{k}^n$. For $\mathbf{x} := (x_1, \ldots, x_n) \in \mathcal{V}(\mathfrak{a}_{\vec{m}})$ and $\sigma \in \mathrm{Gal}(k_{\vec{m}}/k)$, define $\sigma(\mathbf{x}) := (\sigma(x_1), \ldots, \sigma(x_n))$. The **Geometric group action** is defined as the group action

$$\alpha_{\vec{m}/k} : \mathrm{Gal}(k_{\vec{m}}/k) \times \mathcal{V}(\mathfrak{a}_{\vec{m}}) \to \mathcal{V}(\mathfrak{a}_{\vec{m}}), \ (\sigma, \mathbf{x}) \mapsto \sigma(\mathbf{x}).$$

Semisimple decomposition over arbitrary fields

Let $\mathcal{C}_{\vec{m}/k}$ be semisimple, and let $S \subset \mathcal{V}(\mathfrak{a}_{\vec{m}})$ be a set of representatives of the orbits of $\alpha_{\vec{m}/k}$. Then we have the isomorphism

$$\mathcal{C}_{\vec{m}/k} \to \bigoplus_{\mathbf{x} \in S} k(\mathbf{x}), \ f \mapsto (f(\mathbf{x}))_{\mathbf{x} \in S}$$

Notation:

- For an integer m, Div_m is the set of all divisors of m, incuding 1 and m
- For $\vec{m} := (m_1, \ldots, m_n)$, we define $\mathrm{Div}_{\vec{m}} := \mathrm{Div}_{m_1} \times \ldots \times \mathrm{Div}_{m_n}$
- For $\vec{d} := (d_1, \ldots, d_n) \in \mathrm{Div}_{\vec{m}}$, we define the following expressions:
  - $\nu_{\vec{m}/\mathbb{F}_q}(\vec{d}) := \mathrm{lcm}_{1 \le i \le n}(\mathrm{ord}_{m_i/d_i}(q))$
  - $\eta_{\vec{m}/\mathbb{F}_q}(\vec{d}) := \frac{\prod_{i=1}^{n} \varphi(m_i)}{\nu_{\vec{m}/\mathbb{F}_q}(\vec{d})}$ (φ is Euler's totient function)

Semisimple decomposition over finite fields

Let $\mathcal{C}_{\vec{m}/\mathbb{F}_q}$ be semisimple, then its decomposition equals

$$\mathcal{C}_{\vec{m}/\mathbb{F}_q} \cong \bigoplus_{\vec{d} \in \mathrm{Div}_{\vec{m}}} \left(\mathbb{F}_{q^{\nu_{\vec{m}/\mathbb{F}_q}(\vec{d})}} \right)^{\eta_{\vec{m}/\mathbb{F}_q}(\vec{d})}$$

An example: $\mathcal{C}_{(5,5)/\mathbb{F}_2}$

- Consider: $\mathcal{C}_{(5,5)/\mathbb{F}_2} := \mathbb{F}_2[X_1, X_2]/(X_1^5 - 1, X_2^5 - 1)$
- $\mathrm{Div}_{(5,5)} = \{(1,1), (1,5), (5,1), (5,5)\}$
- For every $\vec{d} \in \mathrm{Div}_{(5,5)}$, compute $\nu_{\vec{m}/\mathbb{F}_q}(\vec{d})$ and $\eta_{\vec{m}/\mathbb{F}_q}(\vec{d})$:

$\vec{d}$	$\nu_{(5,5)/\mathbb{F}_2}(\vec{d})$	$\eta_{(5,5)/\mathbb{F}_2}(\vec{d})$
$(1,1)$	1	1
$(1,5)$	4	1
$(5,1)$	4	1
$(5,5)$	4	4

- $\mathcal{C}_{(5,5)/\mathbb{F}_2} \cong \mathbb{F}_2 \oplus \mathbb{F}_{2^4} \oplus \mathbb{F}_{2^4} \oplus (\mathbb{F}_{2^4})^4 = \mathbb{F}_2 \oplus (\mathbb{F}_{2^4})^6$

Part III: General circulant rings

Paper citation

Part III is based on the paper entitled:

The Krull-Remak-Schmidt decomposition of commutative group algebras

(citation TBA)

- Semisimple circulant rings can be decomposed in simple rings
- Can we do something similar for non-semisimple circulant rings?

(But we need a more general notion of simple rings....)

Indecomposable rings

- **Indecomposable ring:** A ring R is indecomposable if there does not exist other rings R_1 and R_2 such that $R = R_1 \oplus R_2$
- All simple rings are indecomposable
- Reverse statement not true: local rings are not simple, but indecomposable

Krull-Remak-Schmidt

Let R be an Artinian ring, hence also Noetherian. Then there exist indecomposable rings $R_1, \ldots, R_n$ such that

$$R \cong R_1 \oplus \ldots \oplus R_n.$$

This decomposition is unique up to isomorphism.

- Circulant rings are Artinian and Noetherian [Con63]

- When are circulant rings indecomposable?

Indecomposable circulant rings

A circulant ring $\mathcal{C}_{\vec{m}/k}$, with $\vec{m} := (m_1, \ldots, m_n)$, is indecomposable if and only if $m_1, \ldots, m_n$ are all powers of the characteristic of k

- Right-side implication is not too complicated to prove, however the reverse statement is not as immediate
- **Example:** $\mathcal{C}_{(4,32)/\mathbb{F}_2} := \mathbb{F}_2[X_1, X_2]/(X_1^4 - 1, X_2^{32} - 1)$ is indecomposable

Additional notation

- Let $m \in \mathbb{Z}_{>0}$ and p a prime number
  - $v_p(m) := \max\{j \in \mathbb{Z}_{\geq 0} : p^j \mid m\}$ (p-adic valuation)
  - $r_p(m) := m/p^{v_p(m)}$
- Let $\vec{m} := (m_1, \ldots, m_n) \in \mathbb{Z}^n_{>0}$ and p a prime number
  - $v_p(\vec{m}) := (v_p(m_1), \ldots, v_p(m_n)) \in \mathbb{Z}^n_{\geq 0}$
  - $r_p(\vec{m}) := (r_p(m_1), \ldots, r_p(m_n)) \in \mathbb{Z}^n_{\geq 0}$

Krull-Remak-Schmidt of circulant rings over arbitrary field

Let $\mathcal{C}_{\vec{m}/k}$ be any circulant ring over a field k with characteristic p, and let $S \subset \mathcal{V}(\mathfrak{a}_{r_p(\vec{m})})$ be a set of representatives of the orbits of $\alpha_{r_p(\vec{m})/k}$.

For p prime:

$$\mathcal{C}_{\vec{m}/k} \cong \bigoplus_{\mathbf{x} \in S} \left(k(\mathbf{x})[Y_1, \ldots, Y_n]/(Y_1^{p^{v_p(m_1)}} - 1, \ldots, Y_n^{p^{v_p(m_n)}} - 1) \right).$$

For $p = 0$:

$$\mathcal{C}_{\vec{m}/k} \cong \bigoplus_{\mathbf{x} \in S} k(\mathbf{x}).$$

Krull-Remak-Schmidt of circulant rings over finite fields

Let $\mathcal{C}_{\vec{m}/\mathbb{F}_q}$ be any circulant ring over $\mathbb{F}_q$ with characteristic p.

Define the expressions:

- $\nu_{\vec{m}/\mathbb{F}_q}(\vec{d}) := \mathrm{lcm}_{1\le i\le n}(\mathrm{ord}_{r_p(m_i)/d_i}(q))$
- $\eta_{\vec{m}/\mathbb{F}_q}(\vec{d}) := \frac{\prod_{i=1}^{n}\varphi(r_p(m_i))}{\nu_{\vec{m}/\mathbb{F}_q}(\vec{d})}$

Then we have the decomposition

$$\mathcal{C}_{\vec{m}/\mathbb{F}_q} \cong \bigoplus_{\vec{d}\in \mathrm{Div}_{r_p(\vec{m})}} \left(\mathbb{F}_{q^{\nu_{\vec{m}/\mathbb{F}_q}(\vec{d})}}[Y_1,\ldots,Y_n]/(Y_1^{p^{\nu_p(m_1)}}-1,\ldots,Y_n^{p^{\nu_p(m_n)}}-1)\right)^{\nu_{\vec{m}/\mathbb{F}_q}(\vec{d})}.$$

An example: $\mathcal{C}_{(5,5,2^l)/\mathbb{F}_2}$

- Consider $\mathcal{C}_{(5,5,2^l)/\mathbb{F}_2} := \mathbb{F}_2[X_1, X_2, X_3]/(X_1^5 - 1, X_2^5 - 1, X_3^{2^l} - 1)$ for some $l \in \mathbb{Z}_{>0}$
- This structure is used in KECCAK-f related to θ
- Observe: $\mathcal{C}_{r_2(5,5,2^l)/\mathbb{F}_2} = \mathcal{C}_{r_2(5,5,1)/\mathbb{F}_2} \cong \mathcal{C}_{r_2(5,5)/\mathbb{F}_2} \cong \mathbb{F}_2 \oplus (\mathbb{F}_{2^4})^6$
- The indecomposable components of $\mathcal{C}_{(5,5,2^l)/\mathbb{F}_2}$ are up to isomorphism:
  - $\mathbb{F}_2[Y_1, Y_2, Y_3]/(Y_1 - 1, Y_2 - 1, Y_3^{2^l} - 1) \cong \mathbb{F}_2[Y]/(Y^{2^l} - 1)$
  - $\mathbb{F}_{2^4}[Y_1, Y_2, Y_3]/(Y_1 - 1, Y_2 - 1, Y_3^{2^l} - 1) \cong \mathbb{F}_{2^4}[Y]/(Y^{2^l} - 1)$
- We get the decomposition

$$\mathcal{C}_{(5,5,2^l)/\mathbb{F}_2} \cong \left(\mathbb{F}_2[Y]/(Y^{2^l} - 1)\right) \oplus \left(\mathbb{F}_{2^4}[Y]/(Y^{2^l} - 1)\right)^6$$

Conclusion

Conclusion

- We presented an algebraic framework which is suitable for investigating circulant-like linear maps
- Can these insights be used to develop new cryptanalytic techniques?
- And maybe also design “better” linear layers based on these findings?

Thank you for your attention!

References i

Ian G Connell.
On the group ring.
Canadian Journal of Mathematics, 15:650–685, 1963.

Joan Daemen, Seth Hoffert, Gilles Van Assche, and Ronny Van Keer.
Xoodoo cookbook.
IACR Cryptol. ePrint Arch., page 767, 2018.

Robert Christian Subroto.
An algebraic approach to circulant column parity mixers.
IACR Cryptol. ePrint Arch., page 1124, 2023.


Robert Christian Subroto.
Wedderburn decomposition of commutative semisimple group algebras using the combinatorial nullstellensatz, 2024.