Generalization of AES-Based Ciphers

Liljana Babinkostova[1], Joshua Keller[2], Bridget Schreiner[3], Jeffrey Schreiner-McGraw[4], and Kevin Stubbs[5]

[1]Boise State University, [2]Worcester Polytechnic Institute, [3]Wellesley College, [4]Willamette University, [5]University of Maryland – College Park

Introduction

In today's world, with over 5 million gigabytes of data being produced every ten minutes, data protection is more important than ever. The Advanced Encryption Standard (AES), established in 2001 by the U.S. National Institute of Standards and Technology, is used in many applications. We generalize the AES to more abstract mathematical structures and provide a characterization that will be useful for future ciphers based on AES.

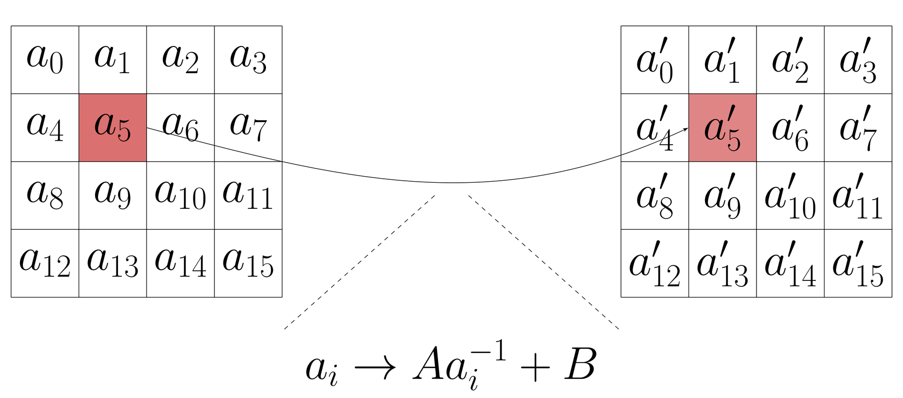
Objectives

- Generalize AES to ciphers over arbitrary finite fields.
- Provide conditions under which the group generated by the set of encryption functions of an AES-based ciphers is the alternating group $A_{\mathcal{M}}$ or the symmetric group $S_{\mathcal{M}}$.
- Construct a new class of ciphers based on the construction given in [1].

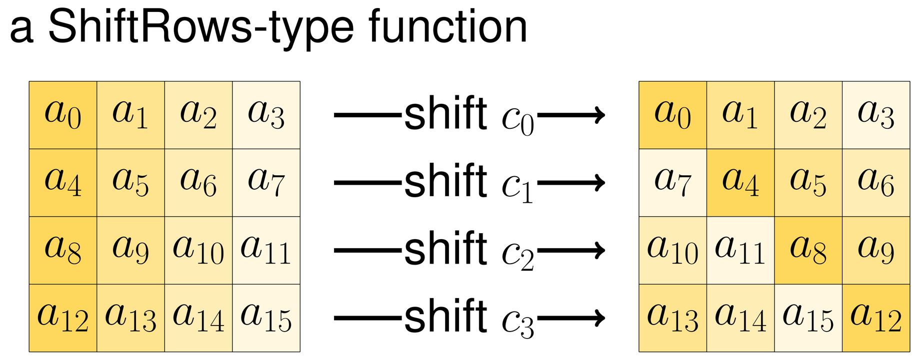
AES-Based Ciphers

Definition. An **AES-Based Cipher** is an encryption function, $T[k]$ which can be written as the composition $T[k] = \sigma_k \circ \rho \circ \pi \circ \lambda$ or $T[k] = \sigma_k \circ \pi \circ \rho \circ \lambda$, where:

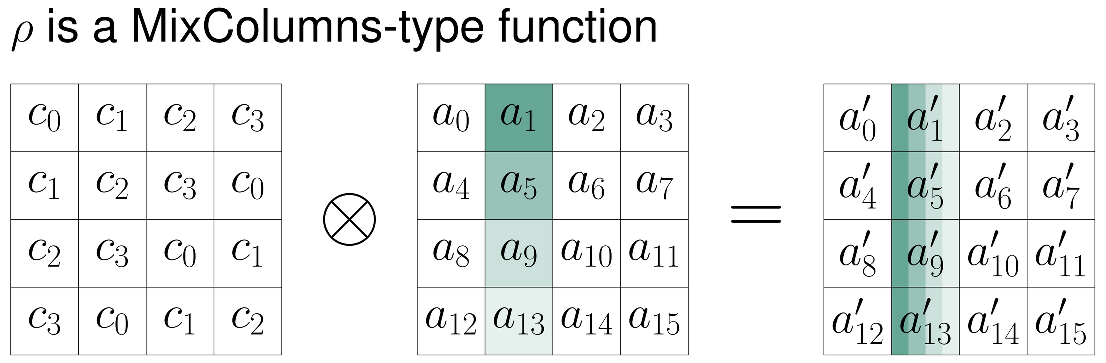
- λ is a SubBytes-type function



- π is a ShiftRows-type function



- ρ is a MixColumns-type function



- σ_k is an AddRoundKey-type function

Results

The results of [1] provide conditions that guarantee a cipher will generate either $A_{\mathcal{M}}$ or $S_{\mathcal{M}}$. Our primary objective is to generalize and expand these results. It can be seen that AES-based ciphers that have a *surjective key schedule* and contain a *proper mixing layer* meet these requirements. Our results reduce the restrictions on these conditions and characterize AES-based ciphers.

Non-Surjective Key Schedule

In [1], the results assume a surjective **key mapping function**. This assumption is used to show that $\langle T[k] : k \in \mathcal{K}\rangle$ contains the set of all translations, $T(V)$. Our result shows that surjectivity is not necessary for $T(V) \subset \langle T[k] : k \in \mathcal{K}\rangle$.

Key Schedule vs. Key Mapping

$$\begin{tikzcd}
\mathcal{K} \arrow[r, "KS(k)"] \arrow[d, "\phi_i(k)"'] & \mathcal{K}^s \arrow[d, "P_i(k_1,\ldots,k_s)"] \\
\mathcal{M} & \mathcal{K} \arrow[l, "\zeta(k_i)"]
\end{tikzcd}$$

Proper Mixing Layer

Definition. Let $\mathcal{M}$ be a vector space $\mathcal{M} = V_1 \oplus \cdots \bigoplus V_n$, where $V_i \cong \mathrm{GF}(p^r)$. A linear transformation ψ is a **proper mixing layer** if it leaves no sum $\bigoplus V_i$, besides $\{0\}$ and V, invariant.

Definition. A matrix $C \in M_{m,m}(\mathrm{GF}(p^r))$ is a **proper mixing matrix** if it properly mixes $M_{m,1}(\mathrm{GF}(p^r)) \cong V_1 \oplus \cdots \oplus V_m$.

$$C = \begin{bmatrix} 1 & 2 & 3 & 4 & 3 \\ 0 & 2 & 0 & 3 & 2 \\ 2 & 1 & 3 & 4 & 2 \\ 0 & 2 & 0 & 3 & 4 \\ 0 & 3 & 0 & 4 & 1 \end{bmatrix}, \qquad W = \begin{bmatrix} w_1 \\ 0 \\ w_3 \\ 0 \\ 0 \end{bmatrix}$$

Example of a Matrix in W-Form

Theorem

A matrix $C \in M_{m,m}(\mathrm{GF}(p^r))$ leaves $W = \oplus V_i$ invariant if and only if it is in W-form.

Theorem

Let $C \in M_{m,m}(\mathrm{GF}(p^r))$ be a circulant matrix with first row $[0,\ldots,0,a_{\alpha+1},0\ldots,0,b_{\beta+1},0,\ldots,0]$. Then C is a proper mixing matrix if and only if $\langle \alpha, \beta\rangle \cong \mathbb{Z}_m$.

Theorem

The composition $\rho \circ \pi$ is a proper mixing layer if and only if ρ properly mixes columns and for all $k \in (1,\ldots,n-1)$, there exists some $I \subseteq \{1,\ldots,n\}$ and constants $j_i \in \mathbb{Z}^+$ such that $\sum_{i\in I} j_i c_i \equiv_n k$.

Main Result

Theorem

Let $T[k]$ be an AES-based cipher with a proper mixing layer and a key mapping which is onto a set of generators of the message space. Then $\langle T[k] : k \in \mathcal{K}\rangle$ is either $A_{\mathcal{M}}$ or $S_{\mathcal{M}}$.

Implications

- Our conditions are sufficient to prevent many attacks, including those that exploit intransitivity and imprimitivity.
- We expand the framework for developing future AES-based ciphers.
- We show the existence of proper mixing matrices containing zero entries. This implies we can improve the efficiency of the MixColumns computations.

Future Work

- Classify types of key schedules that are both computationally efficient and algebraically strong.
- Determine groups generated by encryption functions of ciphers with non-surjective key schedules.

Acknowledgements

Boise State University and NSF DMS 1359425

References

[1] R. Aragona, A. Caranti, F. Dalla Volta, and M. Sala, *On the group generated by the round functions of translation based ciphers over arbitrary finite fields*, **Finite Fields and Their Applications**, Vol. 25 293-305, (2014).

[2] L. Babinkostova, K. Bombardier, M. Cole, T. Morrell, and C. Scott, *Algebraic Structure of generalized Rijndael-like SP networks*, **Groups Complexity Cryptology**, Vol. 6 Issue 1 37-54, (2014)

[3] R. Sparr, R. Wernsdorf, *Group Theoretic Properties of Rijndael-like Ciphers*, **Discrete Applied Mathematics**, 156(16): 3139-3149 (2008)

BOISE STATE UNIVERSITY