Generalizations of the Advanced Encryption Standard

Liljana Babinkostova[1], Kevin Bombardier[2], Matthew Cole[3], Thomas Morrell[4], and Cory Scott[5]

[1]Boise State University, [2]Wichita State University, [3]University of Notre Dame, [4]Washington University in St. Louis, [5]Colorado College

Introduction

AES (Advanced Encryption Standard) is a block cipher chosen in 2001 as the United States' official cryptosystem for Top Secret information. Although all current attacks on AES are too slow to be effective, it is inevitable that the security of AES will decrease over time. This issue was postponed for DES (Data Encryption Standard), AES's predecessor, by implementing Triple-DES. However, this solution depends on the fact that the encryption functions of DES do not form a group under functional composition. We generalize the round functions of AES and ask if the encryption functions of the resulting cipher form such a group.

Description of the Round Functions

AES consists of several concurrent rounds of each of the following permutations in the order: SubBytes, ShiftRows, MixColumns, AddRoundKey. There is also an initial round, consisting solely of AddRoundKey, and a final round, exempting MixColumns. The round functions are detailed below.

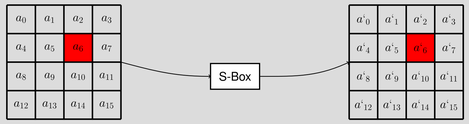

Figure 1: The SubBytes function λ

Figure 2: The ShiftRows function π

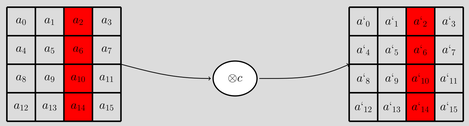

Figure 3: The MixColumns function ρ

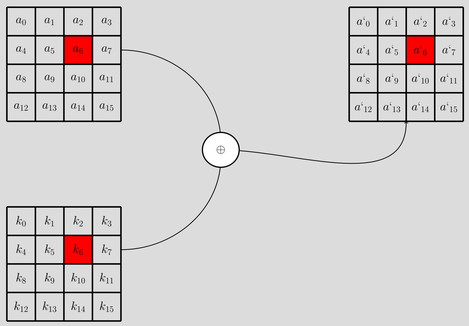

Figure 4: The AddRoundKey function $\sigma[k]$

Definition

Let $\mathcal{K} = GF(p^r)^{mn}$ denote the set of all encryption subkeys. The function $T_k = \sigma[k] \circ \rho \circ \pi \circ \lambda$ for $k \in \mathcal{K}$ is called an AES round function.

Definition

Let $\tau = \{T_k : k \in \mathcal{K}\}$ denote the set of all AES round functions. The group $G_\tau = \langle \tau \rangle$ denotes the group generated by the round functions, and the group

$$G_\tau^s = \langle T_{k_s} \circ T_{k_{s-1}} \circ \cdots \circ T_{k_1} : k_i \in \mathcal{K}, 1 \leq i \leq s \rangle$$

denotes the group generated by an arbitrary composition of s round functions.

Parity of the Round Functions

Theorem

- If $rmn > 1$, then σ and π are always even permutations.
- The function ρ is an odd permutation if and only if p, n, and $(p^{rm} - 1)/|\langle c \rangle|$ are odd, where $\rho(x) = cx$.
- The function λ is an odd permutation if and only if p, m, and n are both odd, and either:
  - $p \equiv_4 3$, r is odd, and $(p^r - 1)/|\langle a \rangle|$ is odd, OR
  - either $p \equiv_4 1$ or r is even, and $(p^r - 1)/|\langle a \rangle|$ is even,

  where $\lambda(x) = ax^{-1} + b$.

So T_k is an odd permutation if and only if λ or ρ is odd, but not both. Since the parity of T_k does not depend on k, all permutations in τ have the same parity.

References

[1] A. Caranti, F. Dalla Volta, and M. Sala, "On some block ciphers and imprimitive groups," *Applicable Algebra in Engineering, Communication, and Computing*, **20:5-6** (2009), pp. 339-350.

[2] C. Cid, S. Murphy, and M.J.B. Robshaw, *Algebraic Aspects of the Advanced Encryption Standard*, Springer, New York, (2006).

[3] J. Daemen, and V. Rijmen, "The Design of Rijndael", Springer-Verlag, Berlin, (2002).

[4] R. Wernsdorf, "The Round Functions of RIJNDAEL Generate the Alternating Group," *Fast Software Encryption*, **2365** (2002), pp. 143-148.

The Group Generated by the Round Functions

We consider generalized AES round functions as sets of permutations of the field $GF(p^r)^{mn}$. (Classical AES is a set of permutations of $GF(2^8)^{4\times 4}$.) A set of permutations generates a permutation group, the largest of which are the alternating and symmetric groups. We obtained the following results:

Theorem

Let τ be a set of AES round functions over $GF(p^r)^{mn}$. If $r \geq 5$, $mn \geq 2$, and $\gcd(c_1, \ldots, c_m, n) = 1$, then G_τ, the group generated by τ, is the alternating or symmetric group.

Theorem

Let τ satisfy the above hypotheses. G_τ is $\mathcal{A}_{p^{rmn}}$ when τ is a set of even permutations, and $\mathcal{S}_{p^{rmn}}$ when τ is a set of odd permutations.

Multiple Rounds

Theorem

When the group $G_\tau = \mathcal{A}_{p^{rmn}}$, then $G_\tau^s = \mathcal{A}_{p^{rmn}}$. When $G_\tau = \mathcal{S}_{p^{rmn}}$, then $G_\tau^s = \mathcal{A}_{p^{rmn}}$ if s is even and $G_\tau^s = \mathcal{S}_{p^{rmn}}$ if s is odd.

Future Work

- What group is generated by classical AES when the key schedule is considered?
- What group is generated by generalized AES when the key schedule is considered?

Acknowledgments

Funding for this project was provided by the National Science Foundation under grant DMS 1062857 and by Boise State University.