Generalizations of the Advanced Encryption Standard

Liljana Babinkostova¹, Kevin Bombardier², Matthew Cole³, Thomas Morrell⁴, and Cory Scott⁵
¹Boise State University, ²Wichita State University, ³University of Notre Dame, ⁴Washington University in St. Louis, ⁵Colorado 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.

The Group Generated by the Round Functions

We consider generalized AES round functions as sets of permutations of the field \(GF(2^{128})\). Classical AES is a set of permutations of \(GF(2^{128})\). 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 \(r\) be a set of AES round functions over \(GF(2^{128})\). If \(r \geq 5\), then \(G_r\), the generated group by \(r\), is the alternating or symmetric group.

**Theorem**

Let \(r\) satisfy the above hypotheses. \(G_r\) is \(A_r\) when \(r\) is a set of even permutations, and \(S_r\) when \(r\) is a set of odd permutations.

**Multiple Rounds**

When the group \(G_r = A_{r, m}\), then \(G_r = A_{r, m}\). When \(G_r = S_{r, m}\), then \(G_r = S_{r, m}\) if \(s\) is even and \(G_r = S_{r, m}\) 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.

References