Small Scale AES Toolbox: Algebraic and Propositional Formulas, Circuit-Implementations and Fault Equations

Maël Gay[2], Jan Burchard[1], Jan Horáček[2], Ange-Salomé Messeng Ekossono[2], Tobias Schubert[1], Bernd Becker[1], Martin Kreuzer[2], Ilia Polian[2]

[1] Albert-Ludwigs-University Freiburg
Georges-Köhler-Allee 051, 79110 Freiburg, Germany
[2] University of Passau
Innstraße 33 & 43, 94032 Passau, Germany

Cryptography is one of the key technologies ensuring security in the digital domain. As such, its primitives and implementations have been extensively analyzed both from a theoretical, cryptoanalytical perspective, as well as regarding their capabilities to remain secure in the face of various attacks.

One of the most common cyphers, the Advanced Encryption Standard (AES) [1] (thus far) appears to be secure in the absence of an active attacker. This renders the research and development of new or improved attacks difficult because it is unlikely that the entire cipher will be broken right away. To resolve this issue, [2] presented a small scale version of the AES with a variable number of rounds, number of rows, number of columns and data word size, and a complexity ranging from trivial up to the original AES.

In this paper we present a collection of various implementations of the relevant small scale AES versions based on hardware, algebraic representations and their translation into propositional formulas. Additionally, we present fault attack equations for each version.

The contribution is as follows: for each small scale AES version the collection contains:

- Fault attack equations, which generalize the results in [3], with both polynomial and CNF representation
- VHDL implementation
- Circuit implementation consisting of basic gates derived from the VHDL implementation for both encryption and decryption
- Propositional formula in conjunctive normal form (CNF) derived from the gate level circuit implementation
- Algebraic representation of the cypher with polynomials for the computer algebra software CoCoA [4] and Sage [5]
- Propositional formula in CNF derived from the algebraic representation

Having all these resources available in a single and well structured package allows researchers to combine the different sources of information which might reveal new patterns or solving strategies. Additionally, the fine granularity of difficulty between the different small scale AES versions allows for the assessment of new attacks or the comparison of different attacks.

All files are available at: http://afa.fim.uni-passau.de/en/benchmarks/

References

1. National Institute of Standards, Technology (NIST): Advanced Encryption Standard (FIPS PUB 197) (2001)
2. Cid, C., Murphy, S., Robshaw, M.J.B. In: Small Scale Variants of the AES. Springer Berlin Heidelberg, Berlin, Heidelberg (2005) 145–162
3. Tunstall, M., Mukhopadhyay, D., Ali, S. In: Differential Fault Analysis of the Advanced Encryption Standard Using a Single Fault. Springer Berlin Heidelberg, Berlin, Heidelberg (2011) 224–233
4. The ApCoCoA Team: ApCoCoA: Approximate computations in commutative algebra. (Available at `http://www.apcocoa.org`)
5. Stein, W., Joyner, D.: SAGE: System for algebra and geometry experimentation. ACM SIGSAM Bulletin **39**(2) (2005) 61–64. Available at `http://www.sagemath.org`