Analyzing the influence of linear redundancy in S-boxes with affine equivalence within XSL-like round functions

Nguyen Bui Cuong, Nguyen Van Long, Hoang Dinh Linh

Vietnam Government Information Security Commission
Ministry of National Defence, Vietnam

June 8, 2016

Our Contributions

In this paper, we present some theoretical results which related to linear redundancy of S-boxes and affine equivalence within XSL-like round functions:

1. Firstly, we show that S-boxes which are generated based on finite field inversion always possess complete linear redundancy.
2. Next, we will consider the influence of linear redundancy of S-boxes on the affine equivalence of component functions within XSL-like round functions in the general case.
3. We propose an effective practical approach to test this. Finally, some experimental results on the round functions within the Kyznyechik, AES are presented

Affine equivalent AES-like of S-boxes

Proposition 1

Given two affine equivalent S-boxes S_1, S_2 of size $n \times n$ bit. Then, if S_1 possess linear redundancy then S_2 also possess linear redundancy. More over, if S_1 possess the completely linear redundancy then so does S_2.

Corolary 1

All AES-like 8 bit S-boxes possess the completely linear redundancy.

In case that S-box possess complete linear redundancy

Proposition 2

All output Boolean functions of XSL-like round function that use S-boxes possess complete linear redundancy are belong to the same affine equivalent class. Moreover, their combinations are also belong to this affine equivalent class.

Test for affine equivalence of two coordinate functions in XSL-like round function

Inputs: Positions t, t' of two coordinate functions for $t, t' = 0, ..., m-1$.

Output: If two functions are equivalent then return 1 otherwise, return 0.

1. $D \leftarrow \varnothing, a \leftarrow \varnothing, b \leftarrow \varnothing, c = 0$
2. **For** $i = 0$ to $k-1$ **If** (*checkafffine*

$$(\mathrm{Tr}\left[\beta_t \times h_{\lfloor \frac{t}{n} \rfloor, i} \times S(X)\right], \mathrm{Tr}\left[\beta_t \times h_{\lfloor \frac{t'}{n} \rfloor, i} \times S(X)\right]))$$

$D \leftarrow D_i, a \leftarrow a_i, b \leftarrow b_i, c \leftarrow c \oplus c_i$;
(D_i, a_i, b_i, c outputs of the algorithm 1 in [1])
else Return 0
3. **Return** 1.

Check the affine equivalence of output functions of the Kuznyechik's round function

- There does not exist any affine equivalent functions pair.
- Check the affine equivalence of output functions of the round function include the S-box layer has 16 identical S-box possess a large linear redundancy and the Kuznyechik's linear transformation layer. We have conducted check on 5000 S-boxes possess large linear redundancy but we could not find any affine equivalent Boolean function pair of the linear layer.

AES-like round functions

- Check the affine equivalence of output functions of the round function that includes Kuznyechik's S-box layer and the AES's linear layer. The experimental results indicate no output Boolean function pair of the above round function are affine equivalent to each other.
- Check the affine equivalence of output functions of the round function that include a S-box layer possess large linear redundancy and the AES's linear layer. The experimental results showed that there are some output function pairs of the above round functions are affine equivalent to each other.

References

- Joanne Fuller and William Millan. " *Linear redundancy in S-boxes*." Fast Software Encryption (FSE). 2003.
- Georgi Ivanov, Nikolay Nikolov, and Svetla Nikova. "*Reversed genetic algorithms for generation of bijective s-boxes with good cryptographic properties*", Cryptography and Communications, 2014.
- Amr M Youssef and Stafford E Tavares. "*Affine equivalence in the AES round function*", Discrete Applied Mathematics, 2005.

Thank you for listening!!!