Relation for Algebraic Attack on E0 combiner

N. Rajesh Pillai, S. S. Bedi, Sanjay Kumar, Roopika Chaudhary

Abstract

The low degree relation for algebraic attacks on E0 combiner given in [1] had an error. The correct version of low degree relation for the E0 combiner for use in algebraic attack is given.

1 Introduction

In this article, equation for algebraic attack for the E0 cipher (a stream cipher used in Bluetooth) is computed. A brief description of the cipher is given followed by description of the results obtained by us by applying our attack.

2 Description of E0

The E0 stream cipher has 4 LFSRs and a combiner with 4-bit memory which takes 4 input bits and produces 1 output bit. The registers are of length 25, 31, 33 and 39 respectively adding up to 128 bits. Let $(x_1^t, x_2^t, x_2^t, x_4^t)$ denote the 4 LFSR outputs which are inputs to the combiner at time t and let $\mathcal{S}^t = (q^t, p^t, q^{t-1}, p^{t-1})$ denote the combiner state at time t. The output bit z^t and the new combiner state $\mathcal{S}^{t+1}$ are given as follows.

$$\begin{array}{rcl}
z^t & = & x_1^t \oplus x_2^t \oplus x_3^t \oplus x_4^t \oplus p^t \\
\mathcal{S}^{t+1} & = & (q^{t+1}, p^{t+1}, q^t, p^t) \\
\text{where} & & \\
q^{t+1} & = & s_1^{t+1} \oplus q^t \oplus p^{t-1} \\
p^{t+1} & = & s_0^{t+1} \oplus q^{t-1} \oplus p^t \oplus p^{t-1} \\
(s_1^{t+1}, s_0^{t+1}) & = & \lfloor \dfrac{x_1^t + x_2^t + x_3^t + x_4^t + 2q^t + p^t}{2} \rfloor
\end{array}$$

3 Algebraic Relation for the E0 combiner

The Theorem by Krause and Armknecht says that a relation of degree 10 involving 5 sets of consecutive inputs will always exist for E0. The complexity of the attack with a 10 degree relation will be more than exhaustive trials of all keys. So finding low degree equations is required. Armknecht and Krause [1] derived the following low degree relation by symbolic manipulations.

$$\begin{aligned}
0 = {} & 1 \oplus z^{t-1} \oplus z^{t} \oplus z^{t+1} \oplus z^{t+2} \\
& \oplus \pi_1(t)(z^t z^{t+2} \oplus z^t z^{t+1} \oplus z^t z^{t-1} \oplus z^{t-1} \oplus z^{t+1} \oplus z^{t+2} \oplus 1) \\
& \oplus \pi_2(t)(1 \oplus z^{t-1} \oplus z^{t} \oplus z^{t+1} \oplus z^{t+2}) \oplus \pi_3(t) z^t \oplus \pi_4(t) \\
& \oplus \pi_1(t-1) \oplus \pi_1(t-1)\pi_1(t)(1 \oplus z^t) \oplus \pi_1(t-1)\pi_2(t) \\
& \oplus \pi_1(t+1) z^{t+1} \oplus \pi_1(t+1)\pi_1(t) z^{t+1}(1 \oplus z^t) \oplus \pi_1(t+1)\pi_2(t) z^{t+1} \\
& \oplus \pi_2(t+1) \oplus \pi_2(t+1)\pi_1(t)(1 \oplus z^t) \oplus \pi_2(t+1)\pi_2(t) \\
& \oplus \pi_1(t+2) \oplus \pi_1(t+2)\pi_1(t)(1 \oplus z^t) \oplus \pi_1(t+2)\pi_2(t)
\end{aligned} \tag{1}$$

where $\pi_i(t)$ denotes the symmetric function of degree i on $x_1^t, x_2^t, x_2^t, x_4^t$, the input variables at time t.

The algebraic equation for the E0 combiner was computed using an optimized implementation of the algorithm in [2]. The expression obtained by us is given below.

$$\begin{aligned}
0 = {} & z^{t-1} \oplus z^{t} \oplus z^{t+1} \oplus z^{t+2} \\
& \oplus \pi_1(t)(z^{t-1} \oplus z^{t} \oplus z^{t+1} \oplus z^{t+2} \oplus z^t z^{t+1} \oplus z^t z^{t+2} \oplus z^t z^{t-1}) \\
& \oplus \pi_2(t)(z^{t-1} \oplus z^{t} \oplus z^{t+1} \oplus z^{t+2}) \oplus \pi_3(t) z^t \oplus \pi_4(t) \\
& \oplus \pi_1(t-1) \oplus \pi_1(t-1)\pi_1(t)(1 \oplus z^t) \oplus \pi_1(t-1)\pi_2(t) \\
& \oplus \pi_1(t+1) z^{t+1} \oplus \pi_1(t+1)\pi_1(t) z^{t+1}(1 \oplus z^t) \oplus \pi_1(t+1)\pi_2(t) z^{t+1} \\
& \oplus \pi_2(t+1) \oplus \pi_2(t+1)\pi_1(t)(1 \oplus z^t) \oplus \pi_2(t+1)\pi_2(t) \\
& \oplus \pi_1(t+2) \oplus \pi_1(t+2)\pi_1(t)(1 \oplus z^t) \oplus \pi_1(t+2)\pi_2(t)
\end{aligned} \tag{2}$$

It was observed that the low degree relation (2) obtained by us was different from (1) by few terms. The xor of the two expressions is $1 + \pi_1(t)(1 + z^t) + \pi_2(t)$ We could obtain the same expression by following the symbolic manipulations indicated in [1] also.

4 Verification

For verification of the correctness the expressions, the relations were evaluated for all possible input-output pairs generated by the E0 combiner. Outputs of four consecutive time steps of the E0 combiner for all the $2^{4*4} = 2^{16}$ possible combinations of input bits and for all the 2^4 possible choices for memory bits were computed. Correct relations should hold for all the 2^{20} input-output pairs.

The equation (2) was holding for all the 2^{20} pairs where as equation (1) was not holding for 393216 of the 2^{20} cases. In hindsight the fact that the expression (1)was incorrect could have been easily detected by checking on the case where all inputs and initial memory is zero.

The new relation (2) was used to successfully recover the initial contents in algebraic attacks against variants of E0 with shorter LFSRs and in algebraic attack on E0 itself when 56 bits of LFSR 1 and LFSR 2 were assumed to be known and remaining 72 unknown.

Acknowledgements

The authors wish to thank Dr. P. K. Saxena, Director SAG, for his support and encouragement for the work.

References

[1] F. Armknecht and M. Krause. Algebraic attacks on combiners with memory. In D. Boneh, editor, *CRYPTO*, volume 2729 of *Lecture Notes in Computer Science*, pages 162–175. Springer, 2003.

[2] N. Courtois. Algebraic attacks on combiners with memory and several outputs. In C. Park and S. Chee, editors, *ICISC*, volume 3506 of *Lecture Notes in Computer Science*, pages 3–20. Springer, 2004.