NSUCRYPTO2024

Problem 2: AntCipher 2.0

October 21, 2024

Solution:

The plaintext in iteration 1704:
M_{1704} = 1100 0001 1100 1110 0101 1100 0001 0101 0100 0011 0001 0010 1001 0101 1000 1100

Decomposition of the CNF C

First, we decompose C into four sub-expressions, where $C_{x_i} = 1$ serves as a function that accepts inputs x_1, x_2, x_3, x_4 and produces outputs x_i.

The function F_C is defined as follows:

$$F_C = (x_1 \vee x_2 \vee \neg x_5) \wedge (\neg x_1 \vee \neg x_2 \vee x_5) \wedge (x_1 \vee x_3 \vee \neg x_5) \wedge (\neg x_1 \vee \neg x_3 \vee x_5) \wedge (x_2 \vee x_3 \vee \neg x_5) \wedge (\neg x_2 \vee \neg x_3 \vee x_5)$$

$$\wedge (x_1 \vee x_2 \vee \neg x_6) \wedge (\neg x_1 \vee \neg x_2 \vee x_6) \wedge (x_1 \vee x_4 \vee \neg x_6) \wedge (\neg x_1 \vee \neg x_4 \vee x_6) \wedge (x_2 \vee x_4 \vee \neg x_6) \wedge (\neg x_2 \vee \neg x_4 \vee x_6)$$

$$\wedge (x_1 \vee x_3 \vee \neg x_7) \wedge (\neg x_1 \vee \neg x_3 \vee x_7) \wedge (x_1 \vee x_4 \vee \neg x_7) \wedge (\neg x_1 \vee \neg x_4 \vee x_7) \wedge (x_3 \vee x_4 \vee \neg x_7) \wedge (\neg x_3 \vee \neg x_4 \vee x_7)$$

$$\wedge (x_2 \vee x_3 \vee \neg x_8) \wedge (\neg x_2 \vee \neg x_3 \vee x_8) \wedge (x_2 \vee x_4 \vee \neg x_8) \wedge (\neg x_2 \vee \neg x_4 \vee x_8) \wedge (x_3 \vee x_4 \vee \neg x_8) \wedge (\neg x_3 \vee \neg x_4 \vee x_8).$$

Definitions of Sub-Expressions

We define the sub-expressions as follows:

$$C_{x_5} = (x_1 \vee x_2 \vee \neg x_5) \wedge (\neg x_1 \vee \neg x_2 \vee x_5) \wedge (x_1 \vee x_3 \vee \neg x_5) \wedge (\neg x_1 \vee \neg x_3 \vee x_5) \wedge (x_2 \vee x_3 \vee \neg x_5) \wedge (\neg x_2 \vee \neg x_3 \vee x_5)$$

$$C_{x_6} = (x_1 \vee x_2 \vee \neg x_6) \wedge (\neg x_1 \vee \neg x_2 \vee x_6) \wedge (x_1 \vee x_4 \vee \neg x_6) \wedge (\neg x_1 \vee \neg x_4 \vee x_6) \wedge (x_2 \vee x_4 \vee \neg x_6) \wedge (\neg x_2 \vee \neg x_4 \vee x_6)$$

$$C_{x_7} = (x_1 \vee x_3 \vee \neg x_7) \wedge (\neg x_1 \vee \neg x_3 \vee x_7) \wedge (x_1 \vee x_4 \vee \neg x_7) \wedge (\neg x_1 \vee \neg x_4 \vee x_7) \wedge (x_3 \vee x_4 \vee \neg x_7) \wedge (\neg x_3 \vee \neg x_4 \vee x_7)$$

$$C_{x_8} = (x_2 \vee x_3 \vee \neg x_8) \wedge (\neg x_2 \vee \neg x_3 \vee x_8) \wedge (x_2 \vee x_4 \vee \neg x_8) \wedge (\neg x_2 \vee \neg x_4 \vee x_8) \wedge (x_3 \vee x_4 \vee \neg x_8) \wedge (\neg x_3 \vee \neg x_4 \vee x_8)$$

Finally, we can express the overall CNF as:

$$C = C_{x_5} \wedge C_{x_6} \wedge C_{x_7} \wedge C_{x_8}$$

Bit Calculation for K_{1703} and K_{1704}

The truth table of C_{x_5} is showed in Table 1. We can construct similar truth tables for other C_{x_i} expressions and we observed that the F_C is not a bijective mapping. To be more precise, the input space contains $2^4 = 16$ elements, while the output space has 8 elements.

x_1	x_2	x_3	x_5	C_{x_5}
0	0	0	0	1
0	0	0	1	1
0	0	1	0	0
0	0	1	1	0
0	1	0	0	1
0	1	0	1	0
0	1	1	0	0
0	1	1	1	1
1	0	0	0	1
1	0	0	1	0
1	0	1	0	0
1	0	1	1	1
1	1	0	0	0
1	1	0	1	0
1	1	1	0	1
1	1	1	1	1

Table 1: Truth Table for x_1, x_2, x_3, x_5

Since K_{1702} is the output of K_{1701}, each of its 4-bit chunk must lies in the output space of F_C. This is also the case with K_{1703}. With this observation, we were able to recover K_{1703}.

$K_{1703} =$ 0101 0110 1111 0011 0011 1111 1100 0000 1111 0000 1010 0101 0110 0101 0000 1111

We then apply F_C on K_{1703} to obtain the K_{1704} and original plaintext M_{1704}

$K_{1704} =$ 0101 1001 1111 0011 0011 1111 1100 0000 1111 0000 1010 0101 1001 0101 0000 1111

$M_{1704} =$ 1100 0001 1100 1110 0101 1100 0001 0101 0100 0011 0001 0010 1001 0101 1000 1100

Please refer to the solution script for more details on NSUCRYPTO2024 Problem 2.