Problem 11. Ant cipher

Dung Le Quoc

October 22, 2023

1 Problem

The cipher must be represented by the equation CNF=True. In Sam's CNF, x_1 and x_2 correspond to the plaintext, x_9 and x_{10} correspond to the ciphertext, while the remaining 6 variables are auxiliary. The equation is as follow:

$$\begin{aligned}(x_1 \vee x_2 \vee x_9) \wedge (\neg x_1 \vee \neg x_2 \vee \neg x_9) \wedge (\neg x_1 \vee x_2 \neg x_9) \wedge (x_1 \vee \neg x_2 \vee x_9) \wedge \\ (x_1 \vee x_2 \vee x_3) \wedge (\neg x_9 \vee \neg x_{10} \vee \neg x_3) \wedge (x_1 \vee \neg x_2 \vee x_4) \wedge (\neg x_9 \vee x_{10} \vee \neg x_4) \wedge \\ (\neg x_1 \vee x_2 \vee x_5) \wedge (x_9 \vee \neg x_{10} \vee \neg x_5) \wedge (\neg x_1 \vee \neg x_2 \vee x_6) \wedge (x_9 \vee x_{10} \vee \neg x_6) \wedge \\ (x_1 \vee x_2 \vee x_3 \vee x_4 \vee \neg x_7) \wedge (x_2 \vee x_3 \vee x_4 \vee \neg x_7 \vee \neg x_8) = True\end{aligned}$$

2 Solution

By examing truth table of equation above, I get some notice. Suppose that I write vectors by order $(x_1, x_2, \ldots, x_{10})$.

According to the problem, (x_1, x_2) is encrypted to (x_9, x_{10}) where the value in truth table is True.

This means that, where $f(x_1, x_2, \ldots, x_9, x_{10}) = 1$ with f is boolean function above, then (x_1, x_2) is encrypted to (x_9, x_{10}).

From truth table, I see that $(0, 0)$ is encrypted to $(1, 0)$, $(0, 1)$ is encrypted to $(1, 1)$, $(1, 0)$ is encrypted to $(0, 0)$, $(1, 1)$ is encrypted to $(0, 1)$.

As a result, we can ignore all variables $x_3, x_4, x_5, x_6, x_7, x_8$, because they do not affect how we decrypt the ciphertext. This is because the encryption from (x_1, x_2) to (x_9, x_{10}) is bijection.

In fact, we only need to consider truth table of 4 variables, where

$$\begin{gathered} f(0,0,1,0) = 1, \\ f(0,1,1,1) = 1, \\ f(1,0,0,0) = 1, \\ f(1,1,0,1) = 1 \end{gathered}$$

Full truth table is written in table 1.

x_1	x_2	x_9	x_{10}	f
0	0	0	0	0
0	0	0	1	0
0	0	1	0	1
0	0	1	1	0
0	1	0	0	0
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	0
1	1	0	0	0
1	1	0	1	1
1	1	1	0	0
1	1	1	1	0

Table 1: Boolean function f

By method Karnaugh map, I convert this truth table to CNF and receive the following equation

$$\begin{aligned} f(x_1, x_2, x_9, x_{10}) = &(\neg x_1 \vee \neg x_9) \wedge (x_1 \vee x_9) \wedge \\ &(\neg x_1 \vee \neg x_2 \vee x_{10}) \wedge (x_1 \vee x_2 \vee \neg x_{10}) \wedge \\ &(\neg x_1 \vee x_2 \vee \neg x_{10}) \wedge (x_1 \vee \neg x_2 \vee x_{10}) \end{aligned}$$

This CNF has four variables and 16 literals.