NSUCRYPTO23 Problems

December 26, 2023

Problem 11.

Answer: $C' = (x_1 \vee x_9) \wedge (\neg x_1 \vee \neg x_9) \wedge (x_2 \vee \neg x_{10}) \wedge (\neg x_2 \vee x_{10})$
We denote $C(x_1, x_2, x_3, \ldots, x_{10}) = (x_1 \vee x_2 \vee x_9) \wedge (\neg x_1 \vee \neg x_2 \neg x_9) \wedge (x_1 \vee \neg x_2 \vee x_9) \wedge (\neg x_1 \vee x_2 \vee \neg x_9) \wedge (x_1 \vee x_2 \vee x_3) \wedge (\neg x_9 \vee \neg x_{10} \vee \neg x_3) \wedge (x_1 \vee \neg x_2 \vee x_4) \wedge (\neg x_9 \vee x_{10} \vee \neg x_4) \wedge (\neg x_1 \vee x_2 \vee x_5) \wedge (x_9 \vee \neg x_{10} \vee \neg x_5) \wedge (\neg x_1 \vee \neg x_2 \vee x_6) \wedge (\neg x_6 \vee x_9 \vee x_{10})$ (or C) to be the original CNF and C' to be the new CNF. According to the problem, by equivalent it is meant that for each pair of plaintext, the same ciphertext is derived from the equation, **thus in the new CNF C' we may only need to care and use the plaintext and ciphertext variables**. Now we need to find a new CNF C' that **only depends on** x_1, x_2, x_9, x_{10} satisfying the following properties:

1. For each pair $(x_1, x_2, x_3, \ldots, x_8, x_9, x_{10})$ satisfying C=$True$, then (x_1, x_2, x_9, x_{10}) also satisfies C'=$True$.

2. For each pair (x_1, x_2, x_9, x_{10}) satisfying C'=$True$, then there exists $(x_3, x_4, \ldots, x_8)$ such that $(x_1, x_2, x_3, \ldots, x_8, x_9, x_{10})$ satisfies C=$True$.

In other words, let

$$\mathcal{S} = \{(x_1, x_2, x_9, x_{10}) \in \mathbb{Z}_2^4 \mid \exists\ (x_3, x_4, \ldots, x_8) \in \mathbb{Z}_2^6 \text{ s.t C}{=}True\ \}$$

Then we need to find a new CNF C' such that C'=$True$ if and only if $(x_1, x_2, x_9, x_{10}) \in \mathcal{S}$. Let $A = (x_1 \vee x_2 \vee x_9) \wedge (\neg x_1 \vee \neg x_2 \neg x_9) \wedge (x_1 \vee \neg x_2 \vee x_9) \wedge (\neg x_1 \vee x_2 \vee \neg x_9)$, we see that **if $C{=}True$, then it holds that $A{=}True$ as well**, thus we are interested in determining (x_1, x_2, x_9) so that $A{=}True$. We see that, for each pair (x_1, x_2), we can uniquely determine x_9 so that $A = True$ as follows:

- If $(x_1, x_2) = (0, 0)$, then from $(x_1 \vee x_2 \vee x_9)$ we have $x_9 = 1$.
- If $(x_1, x_2) = (0, 1)$, then from $(x_1 \vee \neg x_2 \vee x_9)$ we have $x_9 = 1$.
- If $(x_1, x_2) = (1, 0)$, then from $(\neg x_1 \vee x_2 \vee \neg x_9)$ we have $x_9 = 0$.
- If $(x_1, x_2) = (1, 1)$, then from $(\neg x_1 \vee \neg x_2 \neg x_9)$ we have $x_9 = 0$.

From above, it holds that A=$True$ **if and only if** $x_9 = \neg x_1$. From this, for C=$True$, we must have $x_9 = \neg x_1$, but it is not sufficient. Next, for each (x_1, x_2), **given** $x_9 = \neg x_1$**, we need to determine** x_{10} **so that C**=$True$ **for some** $(x_3, x_4, \ldots, x_8)$. By trying all possible cases of (x_1, x_2), we see that x_{10} can be determined as follows:

- If $(x_1, x_2) = (0, 0)$, then from $(x_1 \vee x_2 \vee x_3) \wedge (\neg x_9 \vee \neg x_{10} \vee \neg x_3)$ we have $x_9 = 1$, $x_3 = 1$ and $x_{10} = 0$.
- If $(x_1, x_2) = (0, 1)$, then from $(x_1 \vee \neg x_2 \vee x_4) \wedge (\neg x_9 \vee x_{10} \vee \neg x_4)$ we have $x_9 = 1$, $x_4 = 1$ and $x_{10} = 1$.
- If $(x_1, x_2) = (1, 0)$, then from $(\neg x_1 \vee x_2 \vee x_5) \wedge (x_9 \vee \neg x_{10} \vee \neg x_5)$ we have $x_9 = 0$, $x_5 = 1$ and $x_{10} = 0$.
- If $(x_1, x_2) = (1, 1)$, then from $(\neg x_1 \vee \neg x_2 \vee x_6) \wedge (\neg x_6 \vee x_9 \vee x_{10})$ we have $x_9 = 0$, $x_6 = 1$ and $x_{10} = 1$.

From above, we can actually determine x_{10} uniquely just from x_1 and x_2. More specifically, we can easily check that $x_{10} = x_2$. Thus, from the equation C=$True$, **the ciphertext** (x_9, x_{10}) **can be derived from the plaintext** (x_1, x_2) **with the relation** $x_9 = \neg x_1$ **and** $x_{10} = x_2$. For the other direction, for any (x_1, x_2, x_9, x_{10}) satisfying $x_9 = \neg x_1$ and $x_{10} = x_2$, we can choose $(x_3, x_4, \ldots, x_8)$ so that C=$True$ as follows

1. If $(x1, x_2, x_9, x_{10}) = (0, 0, 1, 0)$, we choose $x_3 = 1, x_4 = 0, x_7 = 0, x_8 = 0$
2. If $(x1, x_2, x_9, x_{10}) = (0, 1, 1, 1)$, we choose $x_3 = 0, x_4 = 1, x_7 = 0, x_8 = 0$
3. If $(x1, x_2, x_9, x_{10}) = (1, 0, 1, 0)$, we choose $x_5 = 1, x_6 = 0, x_7 = 0, x_8 = 0$
4. If $(x1, x_2, x_9, x_{10}) = (1, 1, 0, 1)$, we choose $x_5 = 0, x_6 = 1, x_7 = 0, x_8 = 0$

From above, we conclude that the set $\mathcal{S}$ can be rewritten as follows:

$$\mathcal{S} = \{(x_1, x_2, x_9, x_{10}) \in \mathbb{Z}_2^4 \mid x_1 = \neg x_9 \ \wedge \ x_2 = x_{10}\}$$

Now, recall that our goal is to find a new CNF C' such that C'=$True$ if and only if $(x_1, x_2, x_9, x_{10}) \in \mathcal{S}$. Because C'=$True$ if and only if $x_1 = \neg x_9$ and $x_2 = x_{10}$, **we can write** $C' = X \wedge Y$**, where** X **and** Y **are CNFs such that** X=$True$ **if and only if** $x_1 = \neg x_9$ **and** Y=$True$ **if and only if** $x_2 = x_{10}$.
It is well known that $x_1 = \neg x_9$ if and only if $(x_1 \vee x_9) \wedge (\neg x_1 \vee \neg x_9)$=$True$, hence it holds that $X = (x_1 \vee x_9) \wedge (\neg x_1 \vee \neg x_9)$ and $Y = (x_2 \vee \neg x_{10}) \wedge (\neg x_2 \vee x_{10})$.
Thus we can write our new C' as C'= $(x_1 \vee x_9) \wedge (\neg x_1 \vee \neg x_9) \wedge (x_2 \vee \neg x_{10}) \wedge (\neg x_2 \vee x_{10})$, concluding the problem.