NSUCRYPTO23 Problems

October 23, 2023

Problem 8.

Answer: Since there are two possible values of K, which are 00111100 and 01101100, we cannot find the exact key K.
We work in $\mathbb{F}_2$. First, we need to find $(b_i)_{i=1201}^{1208}$. To do this, we need to solve the following system of equations in modulo 2:

$$\begin{cases} b_{i+7} = b_i b_{i+2} + \gamma_i \ \forall \ i \in \{1201, 1202, \ldots, 1208\}, \\ b_{i+8} = b_i + b_{i+7} \ \forall \ i \in \{1201, 1202, \ldots, 1207\} \end{cases} \tag{1}$$

where $\gamma_{1203} = \gamma_{1208} = 1$ and $\gamma_i = 0$ for all $i \in \{1201, 1202, \ldots, 1208\} \backslash \{1203, 1208\}$. For the rest of the solution, the operations $+$ and $\cdot$ will be performed in modulo 2, and when we denote $A = B$, it is understood to be $A \equiv B \pmod 2$. We are ready to solve (1) to find $(b_i)_{i=1201}^{1208}$. We consider the following cases:

- *Case 1*: $b_{1201} = 1$. In this case, we have $b_{1208} = b_{1203}$ and $b_{1209} = b_{1208} + 1$. We consider two following subcases:

  - *Case 1.1*: $b_{1203} = 0$. In this case, we have $b_{1208} = 0$ and $b_{1209} = 1$, and since $b_{1209} = b_{1202} b_{1204}$, we must have $b_{1202} = b_{1204} = 1$. However, we also have that $b_{1210} = b_{1209} + b_{1202} = 1 + 1 = 0$ and $b_{1210} = b_{1203} b_{1205} + 1 = 0 + 1 = 1$, contradiction.
  - *Case 1.2*: $b_{1203} = 1$. In this case, we have $b_{1208} = 1$ and $b_{1209} = 0$. In addition, we also have $b_{1210} = b_{1203} b_{1205} + 1 = b_{1205} + 1$, $b_{1210} = b_{1202} + b_{1209} = b_{1202}$, $b_{1211} = b_{1203} + b_{1210} = b_{1210} + 1$, $b_{1214} = b_{1209} b_{1207} = 0$, $b_{1215} = b_{1208} b_{1210} + 1 = b_{1210} + 1$ and $b_{1215} = b_{1207} + b_{1214} = b_{1214}$. Thus it holds that

    $$b_{1210} = b_{1202} = b_{1211} + 1 = b_{1205} + 1 = b_{1215} + 1 = b_{1207} + 1. \tag{2}$$

    We consider two additional following subcases:

    - *Case 1.2.1*: $b_{1202} = 0$. In this case, from (2) we have $b_{1205} = 1, b_{1207} = 1, b_{1210} = 0, b_{1211} = 1, b_{1215} = 1$. Since $b_{1211} = b_{1204} b_{1206}$, we must have $b_{1204} = b_{1206} = 1$. However, we have $b_{1212} = b_{1205} b_{1207} = 1$ and $b_{1212} = b_{1211} + b_{1204} = 1 + 1 = 0$, thus $b_{1212} = 0 = 1$, contradiction.

- *Case 1.2.2*: $b_{1202} = 1$. In this case, from (2) we have $b_{1205} = 0, b_{1207} = 0, b_{1211} = 0$. In addition, we have that $b_{1212} = b_{1205}b_{1207} = 0$ and $b_{1212} = b_{1204} + b_{1211} = b_{1204}$, thus b_{1204}=0. Finally, we have that $b_{1213} = b_{1212} + b_{1205} = 0 + 0 = 0$ and $b_{1213} = b_{1206}b_{1208} = b_{1206}$, thus $b_{1206} = 0$. Hence in this case, $b_{1201}b_{1202}b_{1203}b_{1204}b_{1205}b_{1206}b_{1207}b_{1208} = 11100001$, which is indeed a solution of system (1).

- *Case 2:* $b_{1201} = 0$. In this case, we have $b_{1208} = b_{1201}b_{1203} = 0$ and $b_{1209} = b_{1201} + b_{1208} = 0$. In addition, we have that $b_{1213} = b_{1206}b_{1208} = 0, b_{1214} = b_{1207}b_{1209} = 0$, $b_{1206} = b_{1214} + b_{1213} = 0 + 0 = 0$, $b_{1215} = b_{1208}b_{1210} + 1 = 1$, $b_{1207} = b_{1205} + b_{1214} = 1 + 0 = 1$ and $b_{1210} = b_{1202} + b_{1209} = b_{1202}$. We consider the two additional following subcases:

  - *Case 2.1:* $b_{1202} = 0$. In this case, since $b_{1202} = b_{1210}$ we have $b_{1210} = 0$. In addition, since $b_{1210} = b_{1203}b_{1205} + 1$, we must have $b_{1203} = b_{1205} = 1$. We also have that $b_{1211} = b_{1203} + b_{1208} = 1 + 0 = 1$ and $b_{1211} = b_{1204}b_{1206}$, hence it holds that $b_{1204} = b_{1206} = 1$. However, since we already have $b_{1206} = 0$, thus $b_{1206} = 0 = 1$, contradiction.

  – *Case 2.2:* $b_{1202} = 1$. In this case, $b_{1202} = b_{1210}$ we have $b_{1210} = 1$. Since $b_{1209} = 0 = b_{1202}b_{1204}$, we must have $b_{1204} = 0$, and $b_{1211} = b_{1204}b_{1206} = 0$. Since $b_{1211} = 0 = b_{1203} + b_{1210} = b_{1203} + 1$, we must have $b_{1203} = 1$. Finally, since $b_{1212} = b_{1211} + b_{1204} = 0 + 0 = 0$, $b_{1213} = b_{1205} + b_{1212} = b_{1205}$, we must have $b_{1205} = 0$. Hence in this case, $b_{1201}b_{1202}b_{1203}b_{1204}b_{1205}b_{1206}b_{1207}b_{1208} = 01100010$, which is indeed a solution of system (1).

From the two case above, we got $b_{1201}b_{1202}b_{1203}b_{1204}b_{1205}b_{1206}b_{1207}b_{1208} \in \{01100010, 11100001\}$. Next, from $(b_i)_{i=1201}^{1208}$, we need to find back $(b_i)_{i=1}^{8}$. Now, we see that for each i, it holds that:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} b_i \\ b_{i+1} \\ b_{i+2} \\ b_{i+3} \\ b_{i+4} \\ b_{i+5} \\ b_{i+6} \\ b_{i+7} \end{pmatrix} = \begin{pmatrix} b_{i+1} \\ b_{i+2} \\ b_{i+3} \\ b_{i+4} \\ b_{i+5} \\ b_{i+6} \\ b_{i+7} \\ b_{i+8} \end{pmatrix}$$

in modulo 2. Hence by letting M and v_i to be

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

and $v_i = \begin{pmatrix} b_i & b_{i+1} & \dots & b_{i+7} \end{pmatrix}^\top$, then it holds that $Mv_i = v_{i+1}$ for all i. Hence, it holds that $M^{1200}v_1 = v_{1201}$ and $v_1 = M^{-1200}v_{1201}$. The script for computing $M^{-1200}v_{1201}$ will be attached with the file. When $v_{1201} = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}^\top$, we have $v_1 = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}^\top$ and thus $K = 01101100$, and when $v_{1201} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}^\top$, we have $v_1 = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}^\top$ and thus $K = 00111100$. Because there are two possible values of K, we cannot find the exact K.