Improved MITM preimage attack on 4-round Ascon-XOF

December 11, 2022

We find an improved MITM preimage attack on 4-round Ascon-XOF as shown in Figure 1. The starting state $A^{(0)}$ contains 4 ■ bits and 54 ■ bits. There are totally 44 conditions on ■ of $A^{(0)}$, which are listed in Table 1. In the computation from $A^{(0)}$ to $A^{(3)}$, the accumulated consumed degrees of freedom of ■ is 50 and there is no DoF of ■ consumed. Therefore, $\mathrm{DoF}_{\mathcal{B}} = 4$, $\mathrm{DoF}_{\mathcal{R}} = 54 - 50 = 4$. The four matching bit equations ($\mathrm{DoM} = 4$) are:

$$\begin{cases} A^{(3)}_{\{15,4\}} \cdot A^{(3)}_{\{15,1\}} + A^{(3)}_{\{15,3\}} + A^{(3)}_{\{15,2\}} \cdot A^{(3)}_{\{15,1\}} + A^{(3)}_{\{15,2\}} + A^{(3)}_{\{15,1\}} \cdot A^{(3)}_{\{15,0\}} + A^{(3)}_{\{15,1\}} + A^{(3)}_{\{15,0\}} = S^{(3)}_{\{15,0\}}, \\ A^{(3)}_{\{25,4\}} \cdot A^{(3)}_{\{25,1\}} + A^{(3)}_{\{25,3\}} + A^{(3)}_{\{25,2\}} \cdot A^{(3)}_{\{25,1\}} + A^{(3)}_{\{25,2\}} + A^{(3)}_{\{25,1\}} \cdot A^{(3)}_{\{25,0\}} + A^{(3)}_{\{25,1\}} + A^{(3)}_{\{25,0\}} = S^{(3)}_{\{25,0\}}, \\ A^{(3)}_{\{47,4\}} \cdot A^{(3)}_{\{47,1\}} + A^{(3)}_{\{47,3\}} + A^{(3)}_{\{47,2\}} \cdot A^{(3)}_{\{47,1\}} + A^{(3)}_{\{47,2\}} + A^{(3)}_{\{47,1\}} \cdot A^{(3)}_{\{47,0\}} + A^{(3)}_{\{47,1\}} + A^{(3)}_{\{47,0\}} = S^{(3)}_{\{47,0\}}, \\ A^{(3)}_{\{57,4\}} \cdot A^{(3)}_{\{57,1\}} + A^{(3)}_{\{57,3\}} + A^{(3)}_{\{57,2\}} \cdot A^{(3)}_{\{57,1\}} + A^{(3)}_{\{57,2\}} + A^{(3)}_{\{57,1\}} \cdot A^{(3)}_{\{57,0\}} + A^{(3)}_{\{57,1\}} + A^{(3)}_{\{57,0\}} = S^{(3)}_{\{57,0\}}. \end{cases} \tag{1}$$

We choose (M_1, M_2) to make the 44 conditions hold, and perform the MITM attack with the 3rd message block M_3. The total time complexity is about $2^{124.4}$. The memory is 2^{54}.

$A^{(0)}_{\{0,1\}} = 0, A^{(0)}_{\{0,3\}} + A^{(0)}_{\{0,4\}} = 1; A^{(0)}_{\{4,1\}} = 1, A^{(0)}_{\{4,3\}} + A^{(0)}_{\{4,4\}} = 1; A^{(0)}_{\{5,1\}} = 0; A^{(0)}_{\{7,1\}} = 0; A^{(0)}_{\{8,1\}} = 0;$
$A^{(0)}_{\{10,1\}} = 0; A^{(0)}_{\{11,1\}} = 1; A^{(0)}_{\{15,1\}} = 0; A^{(0)}_{\{17,1\}} = 1,\ A^{(0)}_{\{17,3\}} + A^{(0)}_{\{17,4\}} = 1; A^{(0)}_{\{18,1\}} = 1;$
$A^{(0)}_{\{20,1\}} = 1; A^{(0)}_{\{21,1\}} = 1; A^{(0)}_{\{22,1\}} = 1,\ A^{(0)}_{\{22,3\}} + A^{(0)}_{\{22,4\}} = 1; A^{(0)}_{\{24,1\}} = 0,\ A^{(0)}_{\{24,3\}} + A^{(0)}_{\{24,4\}} = 1;$
$A^{(0)}_{\{27,1\}} = 1; A^{(0)}_{\{29,1\}} = 0,\ A^{(0)}_{\{29,3\}} + A^{(0)}_{\{29,4\}} = 1; A^{(0)}_{\{32,1\}} = 0, A^{(0)}_{\{32,3\}} + A^{(0)}_{\{32,4\}} = 1;$
$A^{(0)}_{\{36,1\}} = 1, A^{(0)}_{\{36,3\}} + A^{(0)}_{\{36,4\}} = 1; A^{(0)}_{\{37,1\}} = 0; A^{(0)}_{\{39,1\}} = 0; A^{(0)}_{\{40,1\}} = 0;$
$A^{(0)}_{\{42,1\}} = 0; A^{(0)}_{\{43,1\}} = 1; A^{(0)}_{\{47,1\}} = 0; A^{(0)}_{\{49,1\}} = 1,\ A^{(0)}_{\{49,3\}} + A^{(0)}_{\{49,4\}} = 1; A^{(0)}_{\{18,1\}} = 1;$
$A^{(0)}_{\{52,1\}} = 1; A^{(0)}_{\{53,1\}} = 1; A^{(0)}_{\{54,1\}} = 1,\ A^{(0)}_{\{54,3\}} + A^{(0)}_{\{54,4\}} = 1;$
$A^{(0)}_{\{56,1\}} = 0,\ A^{(0)}_{\{56,3\}} + A^{(0)}_{\{56,4\}} = 1; A^{(0)}_{\{59,1\}} = 1; A^{(0)}_{\{61,1\}} = 0,\ A^{(0)}_{\{61,3\}} + A^{(0)}_{\{61,4\}} = 1;$

Table 1: Bit Conditions in 4-round Attack on Ascon-XOF

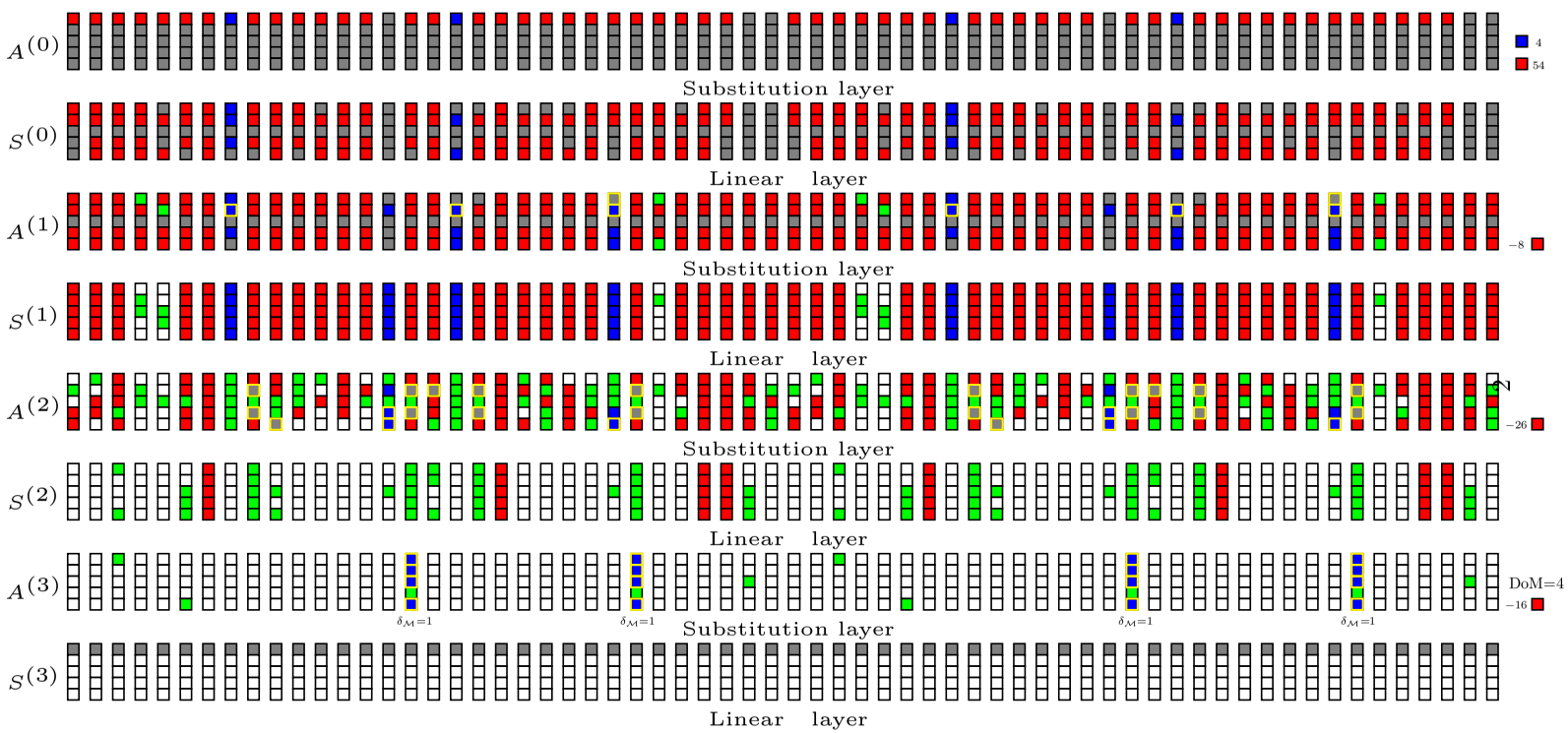

Figure 1: The mitm preimage attack on 4-round `Ascon-XOF`