CSCI971 Advance Computer Security: Homework #2

Mei Wangzhihui 2019124044

Problem 1

Solution
We define the outputs as O_0, O_1
for 0^{64}, there is

$$R_0 = 0^{32},\ L_0 = 0^{32}$$

$$L_1 = R_0 = 0^{32},\ R_1 = F(k_1, R_0) \oplus L_0 = F(k_1, R_0)$$

$$L_2 = R_1 = F(k_1, R_0),\ R_2 = F(k_2, R_1) \oplus L_1 = F(k_2, F(k_1, 0^{32}))$$

Similarly, for $1^{32}0^{32}$, there is

$$L_2 = \bar{F}(k_1, 0^{32}),\ R_2 = F(k_2, \bar{F}(k_1, 0^{32}))$$

thus we can define, $m_0 = F(k_1, 0^{32})$, $c_0 = F(k_2, m_0)$, $m_1 = \bar{F}(k_1, 0^{32}) = \bar{m_0}$, $c_1 = F(k_2, m_1)$
if two outputs are from PRP, then the left 32 bits of $O_1 \oplus O_2$ is 1^{32}
we can easily find that 2) is from PRP, and the other 3 is from random permutation.

Problem 2

Solution
We can draw the whole process of the protocol

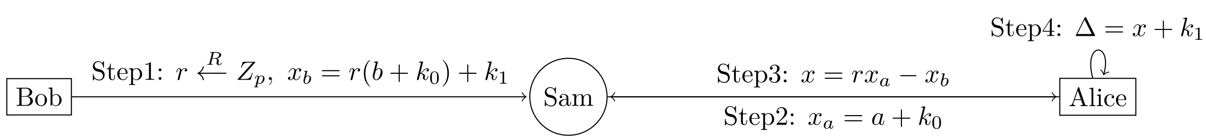

Figure 1: The protocol procedure

As $\Delta = x + k_1 = r(a - b)$ so we get the condition that $r \neq 0$