Cryptography – Homework 3

冯诗伟 161220039

1

a

No. Construct a new message $m' = m_2||m_1||m_3||\cdots||m_\ell$ by swapping the first two blocks of m and use m' to query the oracle. We can get $t' = \mathcal{O}(m') = \mathsf{Mac_k}(m') = F_k(m_2) \oplus F_k(m_1) \oplus F_k(m_3) \oplus \cdots \oplus F_k(m_\ell) = \mathsf{Mac_k}(m)$. So we successfully forge a valid tag t' such that $\mathsf{Vrfy_k}(m, t') = 1$ and $(m, t') \notin \mathcal{Q}$.

b

No. Given $m = m1||m2$, we can easily find two messages $m1', m2'(m1' \neq m1,\ m2' \neq m2)$. Then we can constrcut two new messages m_A and m_B, where $m_A = m1'||m2$, $m_B = m1||m2'$.

Query the oracle with m_A, we can get $\mathcal{O}(m_A) = F_k(m_1')||F_k(F_k(m_2))$. Query the oracle with m_B, we can get $\mathcal{O}(m_b) = F_k(m_1)||F_k(F_k(m_2'))$. By concatenating the former half of $\mathcal{O}(m_b)$ with the latter half of $\mathcal{O}(m_A)$, we can forge a valid tag $t = F_k(m_1)||F_k(F_k(m_2)) = \mathsf{Mac}_k(m)$, where $\mathsf{Vrfy_k}(m, t) = 1$ and $(m, t) \notin \mathcal{Q}$.

c

No. Given $m = m_1||m_2||m_3||\cdots||m_\ell$, we can construct the following three messages:

$$m_A = m_1||m_2||m_2||\cdots||m_\ell$$

$$m_B = m_2||m_2||m_2||\cdots||m_\ell$$

$$m_C = m_2||m_2||m_3||\cdots||m_\ell$$

Then we query the oracle with these three new messages and produce a tag t by XOR the three responses.

$$\begin{aligned}
t &= \mathcal{O}(m_A) \oplus \mathcal{O}(m_b) \oplus \mathcal{O}(m_c) \\
&= F_k(<1>|m_1) \oplus F_k(<2>|m_2) \oplus F_k(<3>|m_2) \oplus \oplus_{i=4}^{\ell} F_k(<i>|m_i) \\
&\oplus F_k(<1>|m_2) \oplus F_k(<2>|m_2) \oplus F_k(<3>|m_2) \oplus \oplus_{i=4}^{\ell} F_k(<i>|m_i) \\
&\oplus F_k(<1>|m_2) \oplus F_k(<2>|m_2) \oplus F_k(<3>|m_3) \oplus \oplus_{i=4}^{\ell} F_k(<i>|m_i) \\
&= F_k(<1>|m_1) \oplus F_k(<2>|m_2) \oplus F_k(<3>|m_3) \oplus \oplus_{i=4}^{\ell} F_k(<i>|m_i) \\
&= F_k(<1>|m_1) \oplus F_k(<2>|m_2) \oplus F_k(<3>|m_3) \oplus \cdots \oplus F_k(<\ell>|m_\ell) \\
&= \mathsf{Mac}_k(m)
\end{aligned}$$

So we successfully forge a valid tag t where $\mathsf{Vrfy_k}(m, t) = 1$ and $(m, t) \notin \mathcal{Q}$.

d

No. Given $m = m_1||m_2||m_3||\cdots||m_\ell$, we can first construct the following messages:

$$m_A = m_1||m_2||m_2||\cdots||m_\ell$$

Then we query the oracle with m_A and get the response:

$$\begin{aligned}\mathcal{O}(m_A) &= (r, m_r)\\ &= (r,\ F_k(r) \oplus F_k(<1>|m_1) \oplus F_k(<2>|m_2) \oplus F_k(<3>|m_2) \oplus \oplus_{i=4}^{\ell} F_k(<i>|m_i))\end{aligned}$$

We can parse r as $r =<x>|r'$, where the former half is the $\frac{n}{2}$-encoding of the integer x.

Construct the second message:

$$m_B = m_2||m_2||m_2||\cdots||r'||\cdots||m_\ell$$

where r' is the x-th block and $\ell = 2^{\frac{n}{2}}$. We can query the oracle with m_A mutiple times until $x \geq 4$.

Then we query the oracle with m_B and get the response:

$$\begin{aligned}\mathcal{O}(m_B) &= (p, m_p)\\ &= (p,\ F_k(p) \oplus F_k(<1>|m_2) \oplus F_k(<2>|m_2) \oplus F_k(<3>|m_2) \oplus F_k(<x>|r') \oplus \oplus_{i=5}^{2^{\frac{n}{2}}} F_k(<i>|m_i))\end{aligned}$$

Similarly, We can parse p as $p =<y>|p'$, where the former half is the $\frac{n}{2}$-encoding of the integer y.

Construct the third message:

$$m_C = m_2||m_2||m_3||\cdots||p'||\cdots||m_\ell$$

where p' is the y-th block and $\ell = 2^{\frac{n}{2}}$. We can query the oracle with m_B mutiple times until $y \geq 4$.

Then we query the oracle with m_C and get the response:

$$\begin{aligned}\mathcal{O}(m_C) &= (q, m_q)\\ &= (q,\ F_k(q) \oplus F_k(<1>|m_2) \oplus F_k(<2>|m_2) \oplus F_k(<3>|m_3) \oplus F_k(<y>|p') \oplus \oplus_{i=5}^{2^{\frac{n}{2}}} F_k(<i>|m_i))\end{aligned}$$

Notice that $F_k(<x>|r') = F_k(r),\ F_k(<y>|p') = F_k(p)$, we can produce the tag $t = (q, M)$ and

$$\begin{aligned}M &= m_r \oplus m_q \oplus m_q\\ &= F_k(r) \oplus F_k(<1>|m_1) \oplus F_k(<2>|m_2) \oplus F_k(<3>|m_2) \oplus \oplus_{i=4}^{\ell} F_k(<i>|m_i)\\ &\oplus F_k(p) \oplus F_k(<1>|m_2) \oplus F_k(<2>|m_2) \oplus F_k(<3>|m_2) \oplus F_k(<x>|r') \oplus \oplus_{i=5}^{2^{\frac{n}{2}}} F_k(<i>|m_i)\\ &\oplus F_k(q) \oplus F_k(<1>|m_2) \oplus F_k(<2>|m_2) \oplus F_k(<3>|m_3) \oplus F_k(<y>|p') \oplus \oplus_{i=5}^{2^{\frac{n}{2}}} F_k(<i>|m_i)\\ &= F_k(q) \oplus F_k(<1>|m_1) \oplus F_k(<2>|m_2) \oplus F_k(<3>|m_3) \oplus \oplus_{i=4}^{\ell} F_k(<i>|m_i)\\ &\oplus F_k(r) \oplus F_k(<x>|r') \oplus F_k(p) \oplus F_k(<y>|p')\\ &= F_k(q) \oplus F_k(<1>|m_1) \oplus F_k(<2>|m_2) \oplus F_k(<3>|m_3) \oplus \oplus_{i=4}^{\ell} F_k(<i>|m_i)\end{aligned}$$

The discussion above is based on the condition that x and y are greater than 4.

$$\begin{aligned}\Pr[x \geq 4 \wedge y \geq 4] &= \Pr[x \geq 4]\Pr[y \geq 4]\\ &= (1 - 2^{\frac{n}{2}-2})^2\end{aligned}$$

So we can construct an adversary $\mathcal{A}$ conducting the steps mentioned above so that

$$\Pr[\mathsf{Mac-sforge}_{\mathcal{A},\Pi}] = 1 = (1 - 2^{\frac{n}{2}-2})^2$$

which is non-negligible.

With a non-negligible probability we successfully forge a valid tag $t = (q, M)$ where $\mathsf{Vrfy_k}(m, t) = 1$ and $(m, t) \notin \mathcal{Q}$, so this MAC is not strongly secure.

2

a

b

c

d

Additional 3.26