Isaac Kim
CS 487
Professor Baldimtsi
Mar 1, 2023

Homework 3

1.1) Consider an adversary A that initially queries a message $m_\alpha =< m_{\alpha_1}, ..., m_{\alpha_t} >$ to the Challenger, and gets a ciphertext $c_\alpha =< c_{\alpha_0}, c_{\alpha_1}, ..., m_{\alpha_t} >$ in return, where $c_{\alpha_0} = IV$. By Kerckhoff's Principle, A knows that S sets $IV_i = IV_{i-1} + 1$. Let IV_{i-1} be the IV for m_α. Then, since m_α was just queried, A can pick messages m_0, m_1 such that for the first block of m_0:

$$\begin{aligned} m_{0_1} \oplus IV_i &= m_{\alpha_1} \oplus IV_{i-1} \\ m_{0_1} \oplus IV_i &= c_{\alpha_1} \\ m_{0_1} &= c_{\alpha_1} \oplus IV_i \end{aligned}$$

Then, pick m_1 such that the first block of m_1, or $m_{1_1} \neq m_{0_1}$. The following blocks of m_0, m_1 can be arbitrary. Then, when A sends m_0, m_1 to the Challenger and gets back $c* =< c*_0, c*_1, ..., c*_t >$ where $c*_0 = IV_i$, A only needs to compare the second blocks of $c*$ and c_α. If $c*_1 = c_{\alpha_1}$, then A outputs $b' = 0$, and otherwise, outputs $b' = 1$. Then, Pr[A wins] $= 1 = \frac{1}{2} + \frac{1}{2} = \frac{1}{2} + p(n)$ where $p(n)$ is a non-negligible value. Hence, this scheme is *not* CPA secure.

1.2) Let A be an adversary that queries messages $m_0 = 0^n$, $m_1 = 1^n$ to the Challenger. The Challenger will then flip a bit $b \in \{0, 1\}$, encrypt $c* = \text{Enc}(k, m_b)$ for some key k, and return $c* =< c*_0, c*_1, ...c*_t >$ to A.

Note that OFB Decryption is as follows: For some ciphertext $c =< c_0, c_1, ...c_t >$, $c_0 = IV$, $m_1 = F_k(c_0) \oplus c_1$,... in general, $m_n = F_k(F_k(c_{n-1})) \oplus c_n$.

Then, A can query s to the decryption oracle, where $s =< c*_0, \bar{c*}_1, ...c*_t >$, $\bar{c*}_1 = c*_1$ with its first bit flipped. Since $s \neq c*$, this is allowed, and A will get back a message $m_s = 10^n$ or 01^n. If the $m_s = 10^n$, then A outputs $b' = 0$, and otherwise, $m_s = 01^n$ and A outputs $b' = 1$. Then, Pr[A wins] $= 1 = \frac{1}{2} + \frac{1}{2} = \frac{1}{2} + p(n)$ where $p(n)$ is a non-negligible value. Hence, this scheme is *not* CCA secure.

2.1) Let A be an adversary that queries message $m_\beta = m_1 || ... || m_l$, $|m_\beta| = ln$, to the MAC oracle $\text{Mac}_k(\cdot)$, and gets back $t_\beta \leftarrow \text{Mac}_k(m_\beta)$. By Kerckhoff's Principle, A knows that $t_\beta = F_k(m_1) \oplus ... \oplus F_k(m_l)$. Then, A can output (m_α, t_β), where $m_\alpha = F_k(m_l) \oplus ... \oplus F_k(m_1)$. Then, $\text{Vrfy}(m_\alpha, t_\beta) = 1$ since t_β is a valid tag for m_α, but m_α was never previously authenticated. Hence, our MAC scheme is not secure.

2.2) Let $m_\alpha = m_3 || m_1$, $m_\beta = m_1 || m_2$, $|m_\alpha| = |m_\beta| = 2n$ and $|m_1| = |m_2| = |m_3| = n$. Let A be an adversary that queries messages m_α, m_β to the MAC oracle $\text{Mac}_k(\cdot)$, and gets back $t_\alpha \leftarrow \text{Mac}_k(m_\alpha)$ and $t_\beta \leftarrow \text{Mac}_k(m_\beta)$. By Kerckhoff's Principle, A knows that $t_\alpha = F_k(m_3)||F_k(F_k(m_1))$ and $t_\beta = F_k(m_1)||F_k(F_k(m_2))$. Then, A can output (m_γ, t_β), where $m_\gamma = m_1||m_1$ and $t_\gamma = F_k(m_1)||F_k(F_k(m_1))$. Then, $\text{Vrfy}(m_\gamma, t_\gamma) = 1$ since t_γ is a valid tag for m_γ, but m_γ was never previously authenticated. Hence, our MAC scheme is not secure.