CSCI971 Advance Computer Security: Homework #8

Mei Wangzhihui
2019124044

Problem 1

For a RSA trapdoor function, if it is used directly as the encryption, then We assume the Challenger $\mathcal{C}$ produce RSA params with $G()$ and get $pk = (N, e), sk = (N, d)$, then Adversary produce two message m_1, m_2 and $|m_1| = |m_2|$, Challenger select b randomly and perform encryption $c_b = E(pk, m_b) = m_b^e$, the decryption should be $m_b = c_b^d$. The Adversary get pk and generate b.

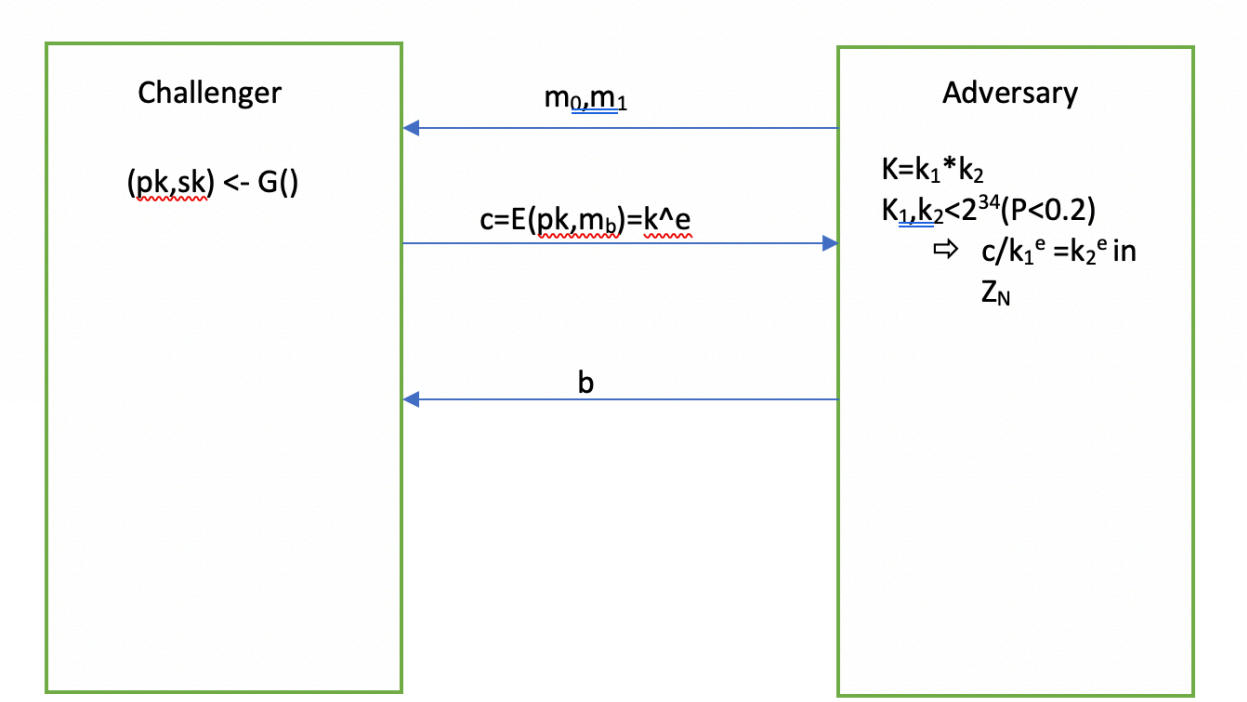

Figure 1: Attack Game

We suppose k is 64bits, $k \in \{0, ...2^{64}\}$, it get $c = k^e$ in Z_N if $k = k_1 * k_2$ where $k_1, k_2 < 2^34$ ($Pr \approx 0.2$) then $c/k_1^e = k_2^e$ in Z_N, firstly, Adversary $\mathcal{A}$ can build table of $k_2^e = c/1^e, c/2^e ..., c/2^{34e}$ then he can itertablely test if k_2^e is in table. he can output matching k_1, k_2.

Problem 2

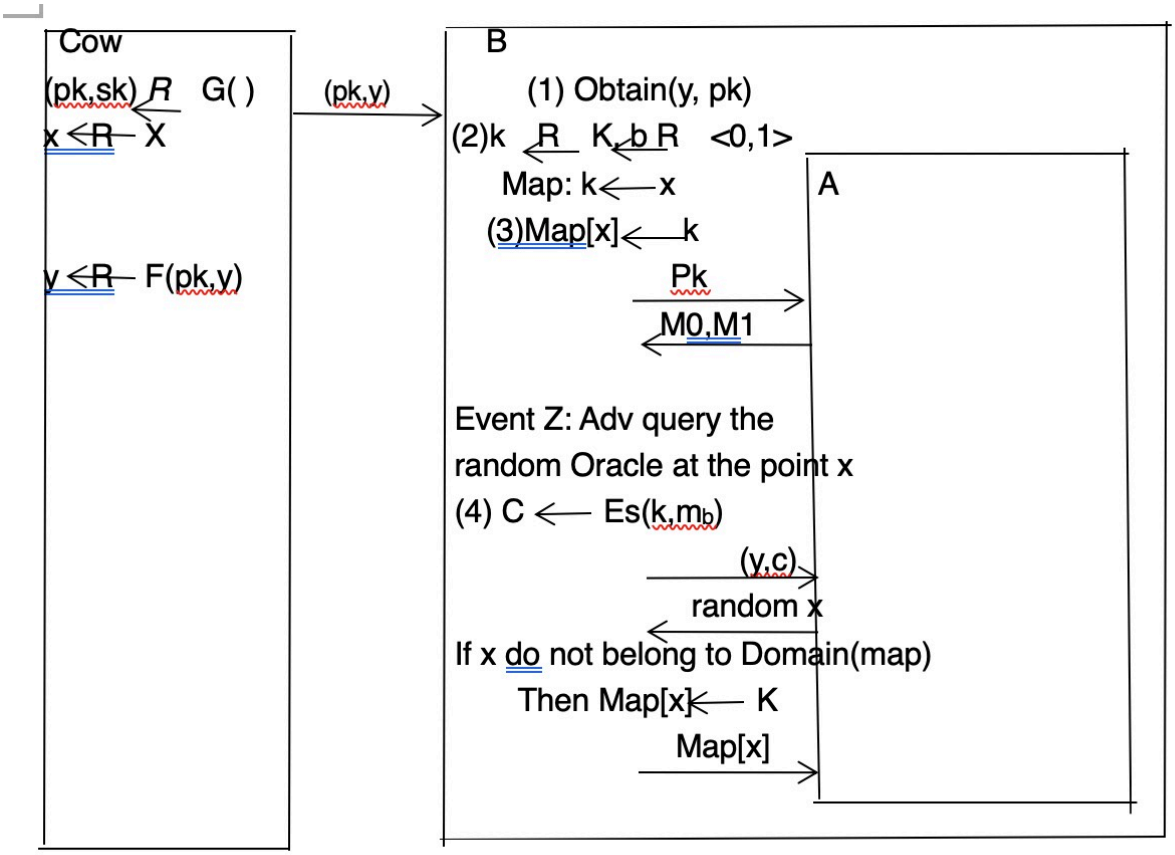

Figure 2:

As $SSadv[\mathrm{A},\epsilon_{TDF}] = 2SS^{ro}adv^*[A,\epsilon_{TDF}]$. We need to prove:

$$SS^*adv[A,\epsilon_{TDF}] \leq OWadv[B_{ow},T] + SSadv^*[B_s,\epsilon_s]$$

We can defind Game0 and Game1 like this: Set W_j as $\widehat{b}$ = b in Game j, (j=0,1).
Then get $|Pr[W_1]| - |Pr[W_0]|$ is negligible and $|Pr[W1]| \approx 1/2$.
Then $SS^{ro}adv^*[A,\epsilon_{TDF}]$ = |Pr[W0]-1/2| is negligible.
Game0: Adversary can make any number of random oracle queries but at most one encryption query.
Game1: The (PK,y) is obtained by Cow .

Set Z: Adversary queries the random oracle at the point x in Game1. At this time, Game0 and Game1 proceed identically unless Z occurs, So We can have:

$$|Pr[W1] - Pr[W0]| <= Pr[Z]$$

If event Z happens, then one of the adv's random queries is the inverse of y under $F(pk,)$. In Game1, the value of x is only used to define y.
Then use that breaks the OW for TDF with advantage equal to Pr[Z].
Lets view Game1 and the game between Bow and Cow. By the definition above Z occurs if and only if x $\in$ Domain(Map) when Bow finishes its game. So we can indicate:

$$Pr[Z] = OWadv[B_{ow}, T]$$

Observe that in Game1,the key k is only used to encrypt the challenge plaintext. As such, the adversary is attacking the bit-guessing version as Attack Game 2.1 from which we can know that:

$$|Pr[W-1] - 1/2| = SSadv^*[B_s], \epsilon_s$$

Then delete the process of (2),(3) change (4) to forward(m_0, m_1) to Cs, obtaining c. Additionly"
When A outputs $\widehat{b}$.then output $\widehat{b}$
Then we can conclude

$$SS^{ro}\text{adv[A,}\epsilon_{TDF}] <= 2OWadv[B_{ow}, T] + SSadv[B_s, E_s]$$