Introduction to Cryptography: HW 3 Solutions

1. (30 pt)Assume that you are given a secure pseudo-random function $F : K \times \{0,1\}^n \mapsto \{0,1\}^n$. Let $E : K \times \{0,1\}^n \mapsto \{0,1\}^n$ be symmetric key encryption scheme. Show that $E_K(M) = (r, F_K(r) \oplus M)$ for randomly chosen r is a secure encryption scheme. Specifically, Let A be an adversary (for attacking the IND-CPA security of SE) that runs in time at most t and asks at most q queries, these totaling at most q n-bit blocks. Then there exists an adversary B (attacking the PRF security of F) such that

$$Adv_{SE}^{ind-cpa}(A) \leq 2.Adv_F^{prf}(B) + \frac{q^2}{2^n}$$

(Hint: Condition on what happens if r is repeated)

Answer:

Let us define the adversary B attacking the F using the the adversary A attacking the encryption algorithm. We know that

Algorithm 1 B^g attacking F

```
$b \xleftarrow{\$} \{0,1\}$
repeat
  Run A and answer its queries $M_o, M_1$
  $R \xleftarrow{\$} \{0,1\}^n$
  Return $(R, R \oplus g(M_b))$ to $A$
until $A$ halts and outputs bit $b_a$
if $b = b_a$ then
  return 1
else
  return 0
end if
```

$$Adv_F^{prf}(B) \quad = \quad Pr[B^g \text{ outputs 1 in world 1}] - Pr[B^g \text{ outputs 1 in world 0}]$$

Also we can easily determine the $Pr[B^g$ outputs 1 in world 1]

$$\begin{aligned} Pr[B^g \text{ outputs 1 in world 1}] &= Pr[\text{A guesses b correctly in world 1}] && (1) \\ &= \frac{1}{2} + \frac{1}{2} Adv_E^{ind-cpa}(A) && (2) \end{aligned}$$

Note that in world 1 for B, A directly observes the actions of the encryption oracle. Also Equation 2 directly follows from the Proposition 4.9 from Bellare-Rogaway book. In order to calculate the probability $Pr[B^g$ outputs 1 in world 0$]$, we will condition on the event whether any of the random R values are repeated or not (i.e. there exits a collision or not). Since in world O, g is random function and if there is not collision on R values, then the output of $g(R)$ will be totally random and the advantage A in distinguishing the encryptions will be zero. In the case of an collision, at most A can predict the correct b value with probability one. Using the above intuition, we can write

$$\begin{aligned}
Pr[B^g \text{ outputs 1 in world 0}] &= Pr[\text{A guesses b correctly in world 0}] \\
&= (Pr[\text{A guesses b correctly in world 0}|\text{No-collision}]. \\
&\quad Pr[\text{No-collision}]) \\
&\quad +(Pr[\text{A guesses b correctly in world 0}|\text{collision}] \\
&\quad .Pr[\text{collision}]) \\
&\leq (\frac{1}{2}(1 - Pr[\text{collision}])) + Pr[\text{collision}] \\
&\leq \frac{1}{2} + \frac{1}{2}.Pr[\text{collision}]
\end{aligned}$$

So we can state that

$$\begin{aligned}
Adv_F^{prf}(B) &= Pr[B^g \text{ outputs 1 in world 1}] - Pr[B^g \text{ outputs 1 in world 0}] \\
&= \frac{1}{2} + \frac{1}{2}Adv_E^{ind-cpa}(A) \\
&\quad -\frac{1}{2} + \frac{1}{2}.Pr[\text{collision}] \\
&\geq \frac{1}{2}Adv_E^{ind-cpa}(A) - \frac{1}{2}.Pr[\text{collision}]
\end{aligned}$$

Using birthday paradox bounds, we can bound the $Pr[\text{collision}] \leq \frac{q^2}{2^n}$

2. (20 pt)Bellare-Rogaway Book: Problem 4.4
Answer: Part a
We can define adversary A as follows:

Note that above adversary A works because the decryption query does not ask the exact C, instead A asks the modified version of the C. the

Algorithm 2 $A^{E_K^{(m)}(LR(.,.,b)),D_K^{(m)}()}$ attacking symmetric encryption

```
$M_0 \leftarrow 0^{mn}$ ,$M_1 \leftarrow 1^{mn}$
$C \leftarrow E_K(LR(M_o, M_1, b))$
$M \leftarrow D_K(C[m]||C[m-1]\dots||C[1])$ {Valid decryption query}
if $M[1] = 1^n$ then
  return 1
else
  return 0
end if
```

$Adv_{SE}^{ind-cca}(A) = 1$ because $M[1]$ will be always $= 1^n$ if $b = 1$.

Answer: Part b

Since B outputs whatever A outputs and exactly simulates the $E_K^{(m)}(LR(.,.,b))$.

Algorithm 3 $B^{E_K(LR(.,.,b)),D_K()}$ attacking symmetric encryption

```
Runs $A^{E_K^{(m)}(LR(.,.,b))}$ and answers $A$'s queries by using oracle $E_K(LR(.,.,b))$
and the encryption defined in Figure 4.11
Output whatever $A$ outputs
```

We can conclude that

$$Adv_{SE}^{ind-cpa}(B) \geq Adv_{SE^{(m)}}^{ind-cpa}(A)$$

3. (20 pt)Bellare-Rogaway Book: Problem 5.1 (Correction $Y_i = E_K(Y_{i-1} \oplus M_i)$)

   Answer

   Choose $M \in \{0,1\}^n$ and set $M' = M||M \oplus E_K(M)$ Note that $H(M)$ is equal to $E_K(0^n \oplus M) = E_K(M)$ and $H(M')$ is equal to

   $$H(M') = E_K(E_K(0^n \oplus M) \oplus M \oplus E_K(M)) = E_K(M)$$

   Although $M \neq M'$, we get $H(M) = H(M')$

4. (30 pt) Bellare-Rogaway Book: Problem 6.3

   Answer

   a) Not secure because message is sent in plaintext form

b) Secure because message and a attached secure mac tag is encrypted using a secure encryption scheme

c) Since message is not transmitted, this does not satisfy the secure channel requirement

d) Secure only if MAC tag does not reveal any information about the message. For generic MACs, we do not know whether this is the case, therefore we say it is not secure for generic MACs.

e) Secure due to secure encryption and secure MAC.

f) In order to create a valid MAC, you need to know only K_2. Therefore, we may not be sure whether the sender knows the K_1

g) Not secure. Consider the one-time pad or CTR mode of encryption

Among the secure alternatives b and e, I will choose the b because once the MAC is computed, we need to do only one encryption call. In practice, initialization costs could be huge for encryption and calling the function once could improve the performance.