Homework 2

Adrián Enríquez Ballester

February 22, 2022

1 Ideal PRGs?

Recall that, given a PRG candidate $G : \{0,1\}^n \to \{0,1\}^{n+1}$ and a distinguisher D, we defined

$$PRGAdv[D, G] = \Big| \Pr[D(G(s)) = 1 \mid s \leftarrow \{0,1\}^n] - \Pr[D(r) = 1 \mid r \leftarrow \{0,1\}^{n+1}] \Big|$$

The standard PRG definition states that for any PPT D it must be

$$PRGAdv[D, G] = negl(n)$$

Let us say that G is an *ideal* PRG if $PRGAdv[D, G] = 0$, for any PPT distinguisher D. We are going to prove that there does not exist such PRG.

For that purpose, we define the following distinguisher by fixing an element of $\{0,1\}^{n+1}$. We are using 0^{n+1} as an example:

```
D(y):
  if y = $0^{n+1}$:
    return 1
  else:
    return 0
```

When D is called with a random input in $\{0,1\}^{n+1}$, the probability of it to output 1 is $1/2^{n+1}$ (i.e. one over the total number of elements).

The interesting part comes when D is called with $G(x)$ where x is sampled randomly from $\{0,1\}^n$. As G's codomain is greater than its domain, it cannot be surjective and its image must have at most as many elements as its domain. This means that there are two possible cases, depending on G:

$$\Pr[D(G(s)) = 1 \mid s \leftarrow \{0,1\}^n] = \begin{cases} 0 & \text{if } 0^{n+1} \notin Im(G) \\ 1/2^n & \text{otherwise} \end{cases}$$

As $|1/2^n - 1/2^{n+1}| = 1/2^{n+1}$ and $|0 - 1/2^{n+1}| = 1/2^{n+1}$, its advantage ends up being the same in both cases:

$$\begin{aligned}
PRGAdv[D,G] &= \Big|\Pr[D(G(s)) = 1 \mid s \leftarrow \{0,1\}^n] - \Pr[D(r) = 1 \mid r \leftarrow \{0,1\}^{n+1}]\Big| \\
&= \Big|\Pr[D(G(s)) = 1 \mid s \leftarrow \{0,1\}^n] - 1/2^{n+1}\Big| \\
&= 1/2^{n+1}
\end{aligned}$$

This simple distinguisher has a non zero advantage over any PRG, so there does not exist an ideal one.

2 PRF candidates

Suppose that $F : \{0,1\}^n \times \{0,1\}^n \mapsto \{0,1\}^n$ is a secure pseudo-random function. We are going to show a couple of derived PRFs in terms of F, one of them insecure and the other one secure.

Recall that the $PRFAdv$ of an adversary A over a PRF F is defined as

$$PRFAdv[A,F] = \Big|\Pr[PRFExp[A,F,0] = 1] - \Pr[PRFExp[A,F,1] = 1]\Big|$$

where $PRFExp$ is

```
PRFExp[A,F,b]:
  if b = 0:
    k $\xleftarrow{\$}$ {0,1}$^n$
    f ← F(k,·)
  else:
    f $\xleftarrow{\$}$ Funcs[{0,1}$^n$,{0,1}$^n$]
  b' ← A$^{f(\cdot)}$
  return b'
```

and F is secure if $PRFAdv[A,F] = negl(n)$ for any PPT adversary.

2.a An insecure derived PRF

Let $F^1 : \{0,1\}^n \times \{0,1\}^n \mapsto \{0,1\}^{2n}$ be the PRF candidate defined as

$$F^1(k,x) := F(k,x) \mid\mid F(k, x \oplus 1^n)$$

It holds that $x \oplus 1^n \oplus 1^n = x \;\forall x \in \{0,1\}^n$, so the fact that

$$\begin{aligned}
F^1(k,x) &= F(k,x) \mid\mid F(k, x \oplus 1^n) \\
F^1(k, x \oplus 1^n) &= F(k, x \oplus 1^n) \mid\mid F(k,x)
\end{aligned}$$

allows us to build the following adversary:

```
A:
  x $\overset{\$}{\leftarrow}$ {0,1}$^n$
  y$_1$ $\leftarrow$ O(x)
  y$_2$ $\leftarrow$ O(x $\oplus$ 1$^n$)
  if (y$_1$[0,n-1], y$_2$[0,n-1]) = (y$_2$[n,2n-1], y$_1$[n,2n-1]):
    return 1
  else:
    return 0
```

For this efficient adversary, $\Pr[PRFExp[A, F^1, 0] = 1] = 1$ due to the above observation.

The chances for it to output 1 when the function is random depends on the amount of elements in $(\{0,1\}^{2n}, \{0,1\}^{2n})$ which also satisfy the checked property over its total. It can be deduced that these are 2^{2n} over 2^{4n}, which means that $\Pr[PRFExp[A, F^1, 1] = 1] = 1/2^{2n}$, so

$$PRFAdv[A, F^1] = 1 - (1/2^{2n})$$

This means that F^1 is not secure, as A has a non negligible advantage over it.

2.b A secure derived PRF

Let $F^2 : \{0,1\}^n \times \{0,1\}^n \mapsto \{0,1\}^n$ be the PRF candidate defined as

$$F^2(k, x) = F(k, x) \oplus x$$

Suppose that we have a PPT adversary A which has a non negligible advantage over F^2. We can build a PPT adversary which also plays the role of oracle for A as follows:

```
B$^{O(\cdot)}$:
  b' $\leftarrow$ A$^{E(\cdot)}$
  return b'
```

where the oracle simulated by B is

```
E(x):
  y $\leftarrow$ O(x)
  return y $\oplus$ x
```

When the oracle for B is a random function, as it also sends random responses to A, both experiments have a direct correspondence:

$$\Pr[PRFExp[B, F, 1] = 1] = \Pr[PRFExp[A, F^2, 1] = 1]$$

It is also the case when the oracle for B uses F due to the way that F^2 has been defined, so

$$\Pr[PRFExp[B, F, 0] = 1] = \Pr[PRFExp[A, F^2, 0] = 1]$$

This implies that

$$PRFAdv[A, F^2] = PRFAdv[B, F]$$

and it means that $PRFAdv[B, F]$ would also be non negligible, which is not possible because F is secure, thus there does not exist such adversary as A.

3 Encryption candidate

Suppose that $F : \{0,1\}^n \times \{0,1\}^n \mapsto \{0,1\}^n$ is a pseudo-random function. The SKE construction from PRFs that we have analyzed in class encrypts a message of n bits and produces a ciphertext of $2n$ bits. Consider the following candidate for SKE that encrypts a message of $2n$ bits producing a ciphertext of $3n$ bits (instead of $4n$ as it would be obtained by simply executing twice the encryption algorithm of the scheme seen in class).

$$E(k, (m_1, m_2)) := (r, F(k, r) \oplus m_1, F(k, r \oplus 1^n) \oplus m_2)$$

where r is randomly chosen in $\{0,1\}^n$.

3.a The decryption algorithm

The decryption algorithm can be stated as follows:

$$D(k, (r, c_1, c_2)) := (F(k, r) \oplus c_1, F(k, r \oplus 1^n) \oplus c_2)$$

It is correct as, $\forall k, m_1, m_2 \in \{0,1\}^n$ and where $r \in \{0,1\}^n$ comes up with the encryption, we have that

$$\begin{aligned}
&D(k,\, E(k, (m_1, m_2)) \\
&\qquad = D(k, (r, F(k, r) \oplus m_1, F(k, r \oplus 1^n) \oplus m_2)) \\
&\qquad = (F(k, r) \oplus F(k, r) \oplus m_1, F(k, r \oplus 1^n) \oplus F(k, r \oplus 1^n) \oplus m_2) \\
&\qquad = (m_1, m_2)
\end{aligned}$$

3.b The scheme is secure

Suppose that we have a PPT adversary A which has a non negligible CPA advantage over this SKE scheme. We can build an also PPT adversary which at the same time plays the role of oracle for A as follows:

```
$B^{O(\cdot)}$:
  b $\xleftarrow{\$}$ {0,1}
  b’ $\leftarrow$ $A^{E((\cdot,\cdot),(\cdot,\cdot))}$
  if b’ = b:
    return 1
  else:
    return 0
```

where the oracle simulated by B is

```
E(($m_{01}$,$m_{02}$),($m_{11}$,$m_{12}$)):
  r $\xleftarrow{\$}$ {0,1}$^n$
  $y_1 \leftarrow$ O(r)
  $y_2 \leftarrow$ O(r $\oplus$ $1^n$)
  return (r,$y_1 \oplus m_{b1}$,$y_2 \oplus m_{b2}$)
```

When the oracle for B is a random function, as it sends random responses to A for any experiment b of B, we have that $\Pr[b' = b] = 1/2$ and thus

$$\Pr[PRFExp[B, F, 1] = 1] = 1/2$$

When it is using the PRF (i.e. experiment 0), the probability of observing the output 1 is the probability of b' to be equals to b in this experiment:

$$\begin{aligned}
\Pr[PRFExp[B, F, 0] = 1] &= \Pr[b' = b] \\
&= \Pr[b = 0] \Pr[b' = 0 | b = 0] + \Pr[b = 1] \Pr[b' = 1 | b = 1] \\
&= (1/2) \Pr[b' = 0 | b = 0] + (1/2) \Pr[b' = 1 | b = 1] \\
&= (1/2)(1 - \Pr[b' = 1 | b = 0]) + (1/2) \Pr[b' = 1 | b = 1] \\
&= (1/2)(1 - \Pr[b' = 1 | b = 0] + \Pr[b' = 1 | b = 1])
\end{aligned}$$

where $\Pr[b' = 1 | b = 0]$ and $\Pr[b' = 1 | b = 1]$ correspond precisely to $\Pr[CPAExp[A, 0] = 1]$ and $\Pr[CPAExp[A, 1] = 1]$.

Finally, all these results lead to

$$\begin{aligned}
PRFAdv[B, F] &= \Big| \Pr[PRFExp[B, F, 0] = 1] - \Pr[PRFExp[B, F, 1] = 1] \Big| \\
&= \Big| (1/2)(1 - \Pr[b' = 1 | b = 0] + \Pr[b' = 1 | b = 1]) - (1/2) \Big| \\
&= (1/2) \Big| \Pr[b' = 1 | b = 1] - \Pr[b' = 1 | b = 0] \Big| \\
&= (1/2) \Big| \Pr[CPAExp[A, 1] = 1] - \Pr[CPAExp[A, 0] = 1] \Big| \\
&= CPAAdv[A, E]/2
\end{aligned}$$

As the advantage of A over the scheme is non negligible, due to this relation, the advantage of B over F is also non negligible, which is not possible because F is a secure PRF.

3.c Why is this possible?

The encryption algorithm $E(k, (m_1, m_2))$ could have been defined by using the PRF candidate from the Exercise 2.a as $(r, F^1(k, r) \oplus (m_1, m_2))$ and, although we have seen that it is not a secure PRF, this scheme is secure.

On the one hand, the SKE scheme seen in class states that it is secure given a PRF function, but it says nothing about the converse (i.e. that it will be insecure when the used function is not a PRF). There can be more ways of making an SKE scheme given a PRF, even with another kind of cryptographic objects. In this case, we have seen a new way of making an SKE scheme with a PRF which overlaps syntactically with the one seen in class giving this paradoxical appearance.

On the other hand, the role of a PRF in the SKE is for obtaining apparently random derived keys seeded from a secret key in an efficient way. In this case, even if we use the perspective of $(r, F^1(k, r) \oplus (m_1, m_2))$, it seems that the function F^1 although weaker than a PRF is being compliant with this role, which can be seen more clearly as using a real PRF for encoding two messages like in the scheme of this exercise.