Cryptography: HW3

Trevor Bramwell

Professor Mike Rosulek
January 30, 2015

1 Secure PRF: F'

Given $F'(k,r) = G(F(k,r))$ we will show that it is a secure PRF.

First we rewrite $F'(k,r)$ as an algorithm. Then after following a series of steps that do not affect the output of the program, we will arive at a double-length PRF.

(a)

$$\boxed{\begin{array}{l} \underline{\text{F'}(k,r)\text{:}} \\ \quad \textit{return } \text{G}(\text{F}(k,r)) \end{array}}$$

(b)

$$\boxed{\begin{array}{l} \underline{\text{F'}(k,r)\text{:}} \\ \quad s \leftarrow \text{F}(k,r) \\ \quad \textit{return } \text{G}(s) \end{array}}$$

(c)

$$\boxed{\begin{array}{l} \underline{\text{F'}(k,r)\text{:}} \\ \quad s \leftarrow \{0,1\}^n \\ \quad \textit{return } \text{G}(s) \end{array}}$$

(d)

$$\boxed{\begin{array}{l} \underline{\text{F'}(k,r)\text{:}} \\ \quad s \leftarrow \{0,1\}^{n+\ell} \\ \quad \textit{return } s \end{array}}$$

(a) This is the formation of F' as a algorithm.

(a)⇒(b) s is used to hold the output of $F(k, r)$. No effect on program.

(b)⇒(c) Because we are given F is a secure PRF, meaning it is indistinguishable from randomness, we can replace the call to $F(k, r)$ with a random string.

(c)⇒(d) By the same logic in (b)⇒(c) we can replace G.

(d) $F'(k, r)$ is a secure PRF.

2 Distinguisher for insecure F'

Given $F'(k, r) = F(k, r) \oplus F(k, \bar{r})$, there exists the following distinguisher A that can tell with non-negligible probability the use of $\mathcal{L}^{F'}_{\textsf{prg-real}}$ over $\mathcal{L}^{F'}_{\textsf{prg-rand}}$.

$$\boxed{\begin{array}{l} \underline{\text{A():}} \\ \quad k \leftarrow \{0,1\}^n \\ \quad l := \text{F'}(k, 0^n) \\ \quad m := \text{F'}(k, 1^n) \\ \quad return(l = m) \end{array}}$$

The bias for A is:

$$\begin{aligned} \text{bias}(A, \mathcal{L}^{F'}_{\textsf{prg-real}}, \mathcal{L}^{F'}_{\textsf{prg-rand}}) &= |Pr[A \diamond \mathcal{L}^{F'}_{\textsf{prg-real}} \text{ outputs } 1] - Pr[A \diamond \mathcal{L}^{F'}_{\textsf{prg-rand}} \text{ outputs } 1]| \\ &= |1 - \frac{1}{2^n}| \\ &= \text{Non-negligible amount} \end{aligned}$$

3 Insecurity of a 2-Round Feistel Network

Given two distinct strings L_1 and L_2, the following distinguisher can be used in a CPA attack against a 2-Round Feistel Network.

$$
\begin{array}{|l|}
\hline
\underline{\text{A}():} \\
\quad R \leftarrow \{0,1\}^n \\
\quad (a_L, a_R) := \text{F}(L_1, R) \\
\quad (b_L, b_R) := \text{F}(L_2, R) \\
\quad \text{return } a_L \oplus b_L = L_1 \oplus L_2 \\
\hline
\end{array}
$$

In a 2-round Feistel network, with distinct f round functions, the output of $F(L, R)$ is a 2-tuple:

$$(f_1(R) \oplus L,\ f_2(f_1(R) \oplus L) \oplus R.$$

Calling $F(L, R)$ twice, with a constant R, and distinct L_i provides the unique property of:

$$(f_1(R) \oplus L_1) \oplus (f_1(R) \oplus L_2)$$

which reduces to:

$$L_1 \oplus L_2$$

4 PRP Distinguisher

$$
\begin{array}{|l|}
\hline
\underline{\text{A}():} \\
\quad k \leftarrow \textsc{KeyGen} \\
\quad (r_1, z_1) := \textsc{Enc}(k, 0^n) \\
\quad (r_2, z_2) := \textsc{Enc}(k, 0^n) \\
\quad \text{return } (r_1 \oplus z_1 \oplus r_2 \oplus z_2) = 0 \\
\hline
\end{array}
$$

To show that F does **not** have CPA-security, the above distinguisher is given. $\textsc{Enc}$ returns a 2-tuple: (r, z) with the property of $r \oplus z = F(k, m)$. Given two calls to $\textsc{Enc}$ the distinguisher is able to check the equality of $F(k, m)$. $F(k, m)$ will not be equal when using $\mathcal{L}_{\textsf{prg-rand}}$.

The bias for A is:

$$
\begin{aligned}
\text{bias}(A, \mathcal{L}^F_{\textsf{prg-real}}, \mathcal{L}^F_{\textsf{prg-rand}}) &= |Pr[A \diamond \mathcal{L}^F_{\textsf{prg-real}} \text{ outputs } 1] - Pr[A \diamond \mathcal{L}^F_{\textsf{prg-rand}} \text{ outputs } 1]| \\
&= |1 - \frac{1}{2^n}| \\
&= \text{Non-negligible amount}
\end{aligned}
$$