Homework 1

Ari Gunnar Kristjónsson
Mikael Máni Eyfeld Clarke
Kristófer Birgir Hjörleifsson

Exercise 1.1

(1)

We show that the multiplicative one-time pad over $\{0, \dots, p-1\}^\lambda$ is **not** Real-or-Random (RoR) secure.

Adversary. The attacker chooses the all-zero message

$$\vec{m} = (0, 0, \dots, 0) \in \{0, \dots, p-1\}^\lambda.$$

- In the **Real world**, the ciphertext is

  $$\vec{c} = \vec{m} \odot \vec{k} = (0, 0, \dots, 0),$$

  which is deterministically all zeros.

- In the **Random world**, the ciphertext is chosen uniformly at random from $\{0, \dots, p-1\}^\lambda$. The probability it equals all zeros is

  $$\Pr[\vec{c} = (0, \dots, 0)] = \left(\frac{1}{p}\right)^\lambda.$$

Advantage. The adversary distinguishes with probability

$$\mathrm{Adv} = 1 - \left(\frac{1}{p}\right)^\lambda,$$

which is overwhelming as λ grows. Hence the scheme is *not* secure in the Real-or-Random sense.

(2)

Now let $p = 5$ and restrict the message space to

$$\mathcal{M} = \{1, 2, 3, 4\}^\lambda.$$

The key space is also $\mathcal{K} = \{1, 2, 3, 4\}^\lambda$. For any $\vec{m} \in \mathcal{M}$ and key $\vec{k}$, the ciphertext is

$$\vec{c}[i] = \vec{m}[i] \cdot \vec{k}[i] \pmod 5.$$

Ciphertext space. Since $\vec{m}[i] \in \{1, 2, 3, 4\}$, multiplication by $\vec{m}[i]$ modulo 5 is a permutation of $\{1, 2, 3, 4\}$. Therefore each ciphertext coordinate is uniformly distributed over $\{1, 2, 3, 4\}$. Thus the ciphertext space is

$$\mathcal{C} = \{1, 2, 3, 4\}^\lambda.$$

Conclusion. Because the ciphertext distribution is uniform over $\mathcal{C}$, independent of the message, the scheme is Real-or-Random secure for $p = 5$.

Bonus

The same reasoning applies for any prime $p > 2$. The set $\{1, \dots, p-1\}$ forms a multiplicative group modulo p. Multiplication by a nonzero element $\vec{m}[i]$ is a bijection of this group. Therefore, for any fixed message $\vec{m}$, the ciphertext distribution is uniform over $\{1, \dots, p-1\}^\lambda$, independent of $\vec{m}$. Hence the scheme is Real-or-Random secure for all primes $p > 2$.

Exercise 1.2

Let $F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$ be a PRF. The modified Feistel round (using bitwise AND in place of XOR) is

$$\mathrm{MF}_k(L, R) = \big(R,\ F(k, R)\ \&\ L\big),$$

where $L, R \in \{0,1\}^\lambda$. For keys $k_1, \dots, k_t$ we define the t-round construction recursively by $(L_i, R_i) = \mathrm{MF}_{k_i}(L_{i-1}, R_{i-1})$ with $(L_0, R_0) = x \in \{0,1\}^{2\lambda}$, and output $P_{k_1,\dots,k_t}(x) = (L_t, R_t)$.

Claim. For any odd $t \geq 1$, for all keys $k_1, \dots, k_t$ and all $R_0 \in \{0,1\}^\lambda$, if $L_0 = 0^\lambda$ then $R_t = 0^\lambda$ deterministically.

Proof. For $t = 1$,

$$(L_1, R_1) = \big(R_0,\ F(k_1, R_0)\ \&\ 0^\lambda\big) = (R_0, 0^\lambda).$$

Assume the statement holds for some odd $t = 2s-1$, so $R_{2s-1} = 0^\lambda$. Then

$$(L_{2s}, R_{2s}) = (R_{2s-1},\ F(k_{2s}, R_{2s-1})\ \&\ L_{2s-1}) = (0^\lambda,\ F(k_{2s}, 0^\lambda)\ \&\ L_{2s-1}).$$

Applying one more round,

$$(L_{2s+1}, R_{2s+1}) = (R_{2s},\ F(k_{2s+1}, R_{2s})\ \&\ L_{2s}) = (*,\ 0^\lambda).$$

Thus $R_{2s+1} = 0^\lambda$. By induction, the claim holds for all odd t.

Distinguisher for $t \geq 3$ (odd). Adversary $\mathcal{A}$ chooses random $R_0 \in \{0,1\}^\lambda$, sets $L_0 = 0^\lambda$, queries the oracle on $x = (L_0, R_0)$, and obtains $y = (L_t, R_t)$. It outputs "real" if $R_t = 0^\lambda$, else "random".

Analysis.

- If the oracle is $\mathsf{PRP}_{\mathrm{real}}$, the claim shows $R_t = 0^\lambda$ always, so

$$\Pr[\mathcal{A}^{\mathsf{PRP}_{\mathrm{real}}} \text{ outputs real}] = 1.$$

- If the oracle is $\mathsf{PRP}_{\mathrm{rand}}$, then the output is uniform in $\{0,1\}^{2\lambda}$, so

$$\Pr[\mathcal{A}^{\mathsf{PRP}_{\mathrm{rand}}} \text{ outputs real}] = 2^{-\lambda}.$$

Advantage.

$$\mathrm{Adv}_{\mathcal{A}} = 1 - 2^{-\lambda},$$

which is overwhelming in λ.

Conclusion. For any odd $t \geq 3$, the modified Feistel construction with & is not a pseudorandom permutation: there exists a one-query distinguisher with overwhelming advantage.