Eavesdrop

Let G be a pseudorandom generator with expansion factor l. Define a private-key encryption scheme for messages of length l as follows:

• Gen: on input 1^n, choose $k \leftarrow \{0, 1\}^n$ uniformly at random and output it as the key.

• Enc: on input a key $k \in \{0, 1\}^n$ and a message $m \in \{0, 1\}^{l(n)}$, output the ciphertext

$c := G(k) \oplus m.$

• Dec: on input a key $k \in \{0, 1\}^n$ and a ciphertext $c \in \{0, 1\}^{l(n)}$, output the plaintext message

$m := G(k) \oplus c.$

Let Π denote this construction.

Let A be a probabilistic polynomial-time adversary, and define ε as

$$\varepsilon(n) \stackrel{\text{def}}{=} \Pr\left[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1\right] - \frac{1}{2}.$$

We use A to construct a distinguisher D for the pseudorandom generator G, such that D "succeeds" with probability ε(n). The distinguisher is given a string w as input, and its goal is to determine whether w was chosen uniformly at random (i.e., w is a "random string") or whether w was generated by choosing a random k and computing w := G(k) (i.e., w is a "pseudorandom string"). D emulates the eavesdropping experiment for A (in a manner described below), and observes whether A succeeds or not. If A succeeds then D guesses that w must have been a pseudorandom string, while if A does not succeed then D guesses that w was a random string. In detail:

Distinguisher D:

D is given as input a string $w \in \{0, 1\}^{l(n)}$. (We assume n can be determined from l(n))

1. Run $A(1^n)$ to obtain the pair of messages m0, m1 $\in \{0, 1\}^{l(n)}$.

2. Choose a random bit $b \leftarrow \{0, 1\}$. Set $c := w \oplus mb$.

3. Give c to A and obtain output b'. Output 1 if b' = b, and output 0 otherwise.

The main observations are as follows:

1. If w is chosen uniformly at random from $\{0, 1\}^{l(n)}$, then the view of A when run as a sub-routine by D is distributed identically to the view of A in experiment

$PrivK^{eav}_{A,\Pi}(n)$. This is because A is given a ciphertext c = w ⊕ mb where $w \in \{0, 1\}^{l(n)}$ is a completely random string.

2. If w is equal to G(k) for $k \leftarrow \{0, 1\}^n$ chosen uniformly at random, then the view of A when run as a sub-routine by D is distributed identically to the view of A in experiment $PrivK^{eav}_{A,\Pi}(n)$. This is because A is given a ciphertext c = w ⊕ m_b where w = G(k) for a uniformly-distributed value $k \leftarrow \{0, 1\}^n$.

It therefore follows that for $w \leftarrow \{0, 1\}^{l(n)}$ chosen uniformly at random,

$$\Pr[D(w) = 1] = \Pr\left[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\tilde{\Pi}}(n) = 1\right] = \frac{1}{2},$$

In contrast, when w = G(k) for $k \leftarrow \{0, 1\}^n$ chosen uniformly at random we have

$$\Pr[D(w) = 1] = \Pr[D(G(k)) = 1] = \Pr\left[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1\right] = \frac{1}{2} + \varepsilon(n)$$

Therefore,

$$|\Pr[D(w) = 1] - \Pr[D(G(s)) = 1]| = \varepsilon(n)$$

where, above, w is chosen uniformly from $\{0, 1\}^{l(n)}$ and s is chosen uniformly from $\{0, 1\}^n$. Since G is a pseudorandom generator (by assumption), it must be the case that ε is negligible. Because of the way ε was defined this concludes the proof that Π has indistinguishable encryptions in the presence of an eavesdropper.