Assignment-1

2020111013

EAV

③ Construction of Secure Encryption Scheme

For a key $k \in \{0,1\}^n$ which is chosen uniformly and a message $m \in \{0,1\}^{l(n)}$ PRG G is defined as

$$G: \{0,1\}^n \to \{0,1\}^{l(n)}$$

And Encryption scheme is defined as

$$Enc_k(m): c = G(k) \oplus m \Rightarrow Dec_k(c): m = G(k) \oplus c$$

Proof of Security

Since the PRG used is provably secure, and its output is being directly bitwise XOR'd with the message, we can say that for that for a distinguisher D, and Adversary A, the probability of the Adversary cracking the encryption scheme would be the same as the probability of distinguisher distinguishing between output of PRG & a string w chosen uniformly at random.

$$\therefore Pr[D(G(k)) = 1] = Pr[PrivK^{eav}_{A,\Pi}(n) = 1] \quad - (1)$$

By definition of PRG,

$$Pr[D(G(k)) = 1] - Pr[D(w) = 1] \leq negl(n)$$

($Pr[D(w) = 1] \to \frac{1}{2}$ since w is uniformly random)

$$\Rightarrow Pr[D(G(k)) = 1] \leq \frac{1}{2} + negl(n)$$

$$\boxed{\Rightarrow Pr[PrivK^{eav}_{A,\Pi}(n) = 1] \leq \frac{1}{2} + negl(n)}$$

$\therefore$ Probability of Adversary cracking encryption scheme, is at maximum negligibly better than the adversary randomly guessing

$\therefore$ Given encryption scheme is provably secure.