HIT — Cryptography — Solutions 2

1603202-1150810613-Qiuhao Li

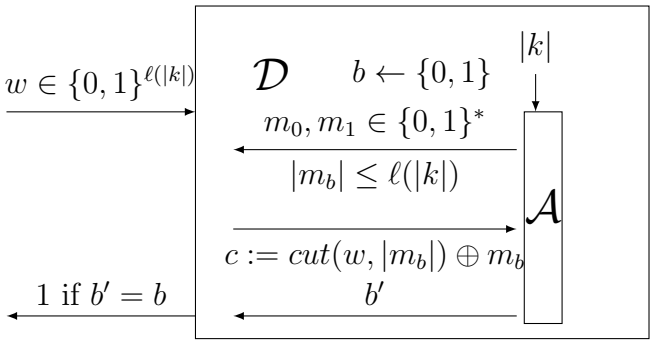
December 31, 2018

Problem 1. Assuming the existence of a variable output-length pseudorandom generator, present a construction of variable-length encryption scheme, and prove that your construction has indistinguishable encryptions in the presence of an eavesdropper. Hint: the construction of secure fixed-length encryption scheme also holds here.

Solution 1.

Precondition: $m \in \{0,1\}^*$, $|m| \leq \ell(|k|)$. Gen: $k \in \{0,1\}^n$. Enc: $c := G(k, 1^{|m|}) \oplus m$. Dec: $m := G(k, 1^{|m|}) \oplus c$.

Proof. We can use $\mathcal{A}$ to construct D for G, so that D distinguishes G when $\mathcal{A}$ breaks $\tilde{\Pi}$. Since D cannot distinguish G, so that $\mathcal{A}$ cannot break $\tilde{\Pi}$:



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

If w is r chosen *u.a.r*, then $\tilde{\Pi}$ is OTP.

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

If w is $G(k)$, then $\tilde{\Pi} = \Pi$.

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

Since we know G is a pseudorandom generator:

$$|\Pr[D(r) = 1] - \Pr[D(G(k)) = 1]| = \varepsilon(n) \leq \mathsf{negl}(n).$$

Finally we can conclude:

$$|\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1] - \frac{1}{2}| = \varepsilon(n) \leq \mathsf{negl}(n).$$

□

Problem 2. Assume $f(s)$ and $f'(s)$ are PRGs. Is $g(s) = f(s) \oplus f'(s)$ also necessarily a PRG? How about $g(s) = f(s) \oplus s$?

Solution 2.

Actually it should be $g(s) = f(s) \oplus (s * \ell(|s|))$ instead of $g(s) = f(s) \oplus s$.

For $g(s) = f(s) \oplus f'(s)$, it's not necessarily, which depends on the relationship between $f()$ and $f'()$. For instance, if the pseudorandom sequence generated by $f'(s)$ is just simply reverse every bit in the result of $f(s)$, then the $g(s)$ wouldn't be a PRG while $f(s)$ and $f'(s)$ are PRGs.

For $g(s) = f(s) \oplus (s * \ell(|s|))$, it's not necessarily, either. For instance, let's say, $\ell(|s|) = 2 * |s| = 2n$, and the first three bits in $f(s)$ is exactly first three of s (BTW, $|s| > 3$), then $f(s)$ is still a PRG, since adversary have to try the alternative s, which is exponential time of n (2^{n-3}). But in this case, the first three bits of $g(s)$ must be zeros, which lets the adversary can win the challenge with possibility around 7/8 instead of 1/2.

Problem 3. Assuming the existence of a pseudorandom function, prove that there exists an encryption scheme that has indistinguishable multiple encryptions in the presence of an eavesdropper, but is not CPA-secure. Hint: You will need to use the fact that in a CPA the adversary can choose its queries to the encryption oracle adaptively (i.e., new query may be constructed from previous queries).

Solution 3.

The well-known *chained CBC mode*, in which the last block of the previous ciphertext is used as the IV when encrypting the next message, has indistinguishable multiple encryptions in the presence ofan eavesdropper, but is not CPA-secure.

Since when *chained CBC mode* encounters with multiple encryptions, it is identical to the *Cipher Block Chaining (CBC) mode*, which is secure, I will just prove it is not secure in the context of CPA.

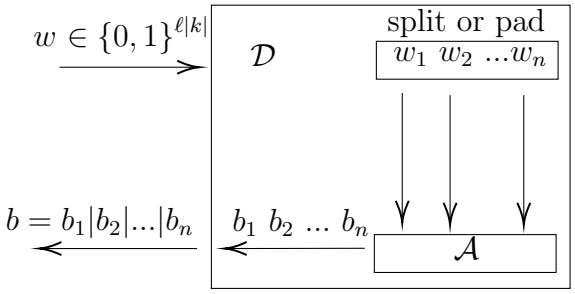
Proof. The basis of the attack is that the adversary knows in advance the initialization vector that will be used for the second encrypted message.

First, the attacker send a plaintex m_3 to the oracle, and observes a ciphertext c_3. Then he challenges the Π with $m_0 = IV \oplus c_3 \oplus m_3$, $m_1 = \{0\}^{\ell(n)}$. Obviously, if Π choose to encrypt m_0, the c_b will be identical to c_3, thus making adversary win the challenge with constant possibility — $(\frac{1}{2} - \frac{1}{2^n})$. □

Problem 4. Present a construction of a variable output-length pseudorandom generator from any pseudorandom function. Prove that your construction satisfies Definition: 'a variable output-length pseudorandom generator'.

Solution 4.

Let F be a pseudorandom function mapping n-bit inputs to n-bit outputs. Define $F_k[\ell]$ to be the series $F_k(0)||F_k(1)||F_k(2)$,... truncated to exactly ℓ bits (there are 2^n possible inputs to F and thus $F_k[\ell]$) is well-defined for any $\ell \leq 2^n$). Define $G(s, 1^\ell = F_s[\ell]$. So the ouput length of G is ℓ. Also $\ell < \ell'$ implies that $G(s, 1^\ell)$ is a prefix of $G(s, 1^{\ell'})$. It is easy to prove that G is a pseudorandom generator for any polynomial ℓ, by a straightforward reduction to the pseudorandomness of F:



Proof. Since we know F is a pseudorandom function, thus $\forall$ PPT distinguishers D,

$$\left|\Pr[D^{F_k(\cdot)}(1^n) = 1] - \Pr[D^{f(\cdot)}(1^n) = 1]\right| \leq \mathsf{negl}(n),$$

where f is chosen $u.a.r$ from Func_n.

And because the number of $F_k()$ used in this experiment (n) is polynomial, then we can get:

$$\left|Poly(n)\right| * |\Pr[D^{F_k(\cdot)}(1^n) = 1] - \Pr[D^{f(\cdot)}(1^n) = 1]\big| \leq \mathsf{negl}(n),$$

We also know that:

$$\Pr[D(G(k)) = 1] = |Poly(n)| * |\Pr[D^{F_k(\cdot)}(1^n) = 1]|.$$

$$|\Pr[D(r) = 1]| = |Poly(n)| * |\Pr[D^{f(\cdot)}(1^n) = 1]|.$$

Thus we can conclude that:

$$|\Pr[D(G(k)) = 1] - |\Pr[D(r) = 1]| \leq \mathsf{negl}(n).$$

□

Problem 5. Show that the CBC mode do not yield CPA-secure encryption in the case that the IV is predicable. Hint: The messages presented by the adversary could be constructed from the predicable IV and previous queries.

Solution 5.

Please refer to the third question above(Why chained CBC mode *is not CPA-secure) for the answer to this question.*

Problem 6. Show that the CBC, OFB and CTR modes do not yield CCA-secure encryption schemes (regardless of F). Hint: If one bit of Ciphertext is flipped, so does one bit of Plaintext.

Solution 6.

Consider an adversary $\mathcal{A}$ running in the CCA indistinguishability experiment who chooses $m_0 = 0^n1^n$ and $m_1 = 1^n0^n$. Then, upon receiving a ciphertext c $= < IV, c_0c_1 >$, the adversary can flip the first bit of c and ask for a decryption of the resulting ciphertext c'. Since $c' \neq c$, this query is allowed.

For CBC mode, if the decryption oracle's answers are x^n01^{n-1}, then $b = 0$. Else if the decryption oracle's answers are x^n10^{n-1}, then $b = 1$.

For OFB and CTR mode, if the decryption oracle's answers are $10^{n-1}1^n$, then $b = 0$. Else if the decryption oracle's answers are $01^{n-1}0^n$, then $b = 1$.

Happy  Hacking!