CS60088 Foundations of Cryptography, Spring 2015–2016

Class Test

18–April–2016 | CSE-119/120, 6:00–7:00pm | Maximum marks: 20

Roll no: ____________ **Name:** ____________________

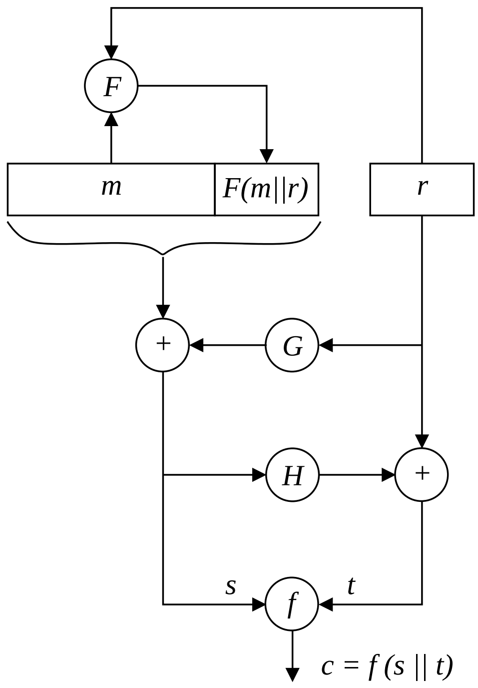
[*Write your answers in the question paper itself. Be brief and precise. Answer all questions.*]

1. Consider the following modification of f-OAEP. Instead of using a data-independent redundancy 0^{l_1}, we now use a redundancy which is a function of both the message m and the random salt r. Take $|m| = l_0$, $|r| = l_2$, and the redundancy of bit length l_1. The scheme uses three hash functions: $F : \{0,1\}^{l_0+l_2} \to \{0,1\}^{l_1}$, $G : \{0,1\}^{l_2} \to \{0,1\}^{l_0+l_1}$, and $H : \{0,1\}^{l_0+l_1} \to \{0,1\}^{l_2}$. Assume that f is a one-way trapdoor function from $\{0,1\}^{l_0+l_1+l_2}$ to some set of ciphertext messages.

The modified f-OAEP has the following encryption procedure:

$$\begin{aligned} s &= (m \,||\, F(m \,||\, r)) \oplus G(r), \\ t &= H(s) \oplus r, \\ m' &= s \,||\, t, \\ c &= f(m'). \end{aligned}$$

The ciphertext is c.



(a) Explain how decryption is carried out in this scheme. **(5)**

Solution The recipient uses the trapdoor to invert f and retrieve the padded message $m' = f_{td}^{-1}(c)$. This is then decomposed in two parts s and t with $|s| = l_0 + l_1$ and $|t| = l_2$. The salt is then recovered as $r = t \oplus H(s)$. This gives $\mu = s \oplus G(r)$ which is decomposed into two strings m and η with $|m| = l_0$ and $|\eta| = l_1$. If $F(m \,||\, r) = \eta$, m is returned as the decryption of c, else *failure* is reported.

We now focus on the IND-CCA2 security of the modified f-OAEP scheme in the random oracle model. Assume that there exists a PPT adversary Vera (named $\mathscr{A}$ in the class) who can break the IND-CCA2 security of the scheme with non-negligible advantage. A simulator Ronald (named Simon earlier) exploits the cryptanalytic prowess of Vera to invert f on a random ciphertext c^*. Ronald plays the IND-CCA2 game with Vera. He acts as a random oracle, and supplies answers to all hash queries (F, G, H) from Vera. He maintains three hash tables for this purpose. He also simulates the encryption and decryption procedures.

(b) During the IND-CPA part of the IND-CCA2 game, Vera supplies two plaintext messages m_0, m_1 (each of bit length l_0). Ronald chooses $b \in_U \{0,1\}$, and presents c^* to Vera as the challenge ciphertext. If c^* is a valid ciphertext of m_b, what constraints are imposed on the hash function values? **(5)**

Solution The challenge c^* uniquely identifies s^* and t^* such that $c^* = f(s^* \,||\, t^*)$. Choose some r^* not residing in Ronald's G and F tables. Since the game runs for a short time, such an r^* is easy to find. This defines

$$H(s^*) = t^* \oplus r^*.$$

Another equivalent alternative is to take any uniformly random value for $H(s^*)$ and define $r^* = H(s^*) \oplus t^*$. If r^* resides in the G or F table, we need to repeat.

Then, choose a uniformly random l_1-bit string as $F(m_b \,||\, r^*)$. Finally, define

$$G(r^*) = s^* \oplus (m_b \,||\, F(m_b \,||\, r^*)).$$

(c) Explain how Ronald simulates a decryption query from Vera. **(5)**

Solution Vera asks Ronald to decrypt c. In the pre-challenge phase, c can be any ciphertext. In the post-challenge phase, c must be different from c^*. For each r in the G-table and for each s in the H-table, Ronald computes

$$\begin{aligned} m' &= s \,||\, (H(s) \oplus r), \\ \mu &= s \oplus G(r). \end{aligned}$$

If $f(m') \neq c$, he continues to the next choice of r and s. Otherwise, Ronald takes m to be the first l_0 bits of μ. If $F(m \,||\, r)$ is not defined yet, or if $F(m \,||\, r)$ is already defined but does not match the last l_1 bits of μ, Ronald reports failure (invalid ciphertext). Otherwise (that is, if $F(m \,||\, r)$ is defined and is equal to the last l_1 bits of μ), m is returned to Vera as the decryption of c. If all choices of r, s fail to identify a decryption of c, failure is reported.

Notice that without making appropriate F, G, H queries, it is extremely unlikely for Vera to prepare a valid ciphertext c on some message m. Therefore the simulated decryption fails with only negligible probability.

(d) The IND-CPA part of the game introduces some restrictions on hash function values. Explain how hash queries are handled in the post-challenge phase. **(5)**

Solution The solution of Part (b) shows that any uniformly random value can be sent for any H or F query. A query of $G(r)$ is critical in the post-challenge phase. For each s in the H-table, Ronald computes $t = H(s) \oplus r$ (the query is on r). If $f(s \,||\, t) = c^*$, then $s = s^*$ and $t = t^*$, and Ronald's objective of inverting f on c^* is satisfied. In that case, Ronald checks whether $F(m_b \,||\, r)$ is defined. If not, any uniformly random value is stored as $F(m_b \,||\, r)$. Finally, $s \oplus (m_b \,||\, F(m_b \,||\, r))$ is returned to Vera as the value of $G(r)$. If all choices of s in the G-table fails to identify s^*, t^*, Ronald chooses and returns to Vera any uniformly random $l_0 + l_1$-bit string.

Note: As an offline exercise, try to figure out whether Shoup's attack can be mounted on this modified f-OAEP scheme. If the answer is *no*, prove it. Otherwise, can you suggest a remedy?

Use this space for leftover answers and rough work