CS60088 Foundations of Cryptography, Spring 2016–2017

Class Test

10–April–2017 | CSE 107/120, 6:30–7:30pm | Maximum marks: 40

Roll no: ____________________ **Name:** ____

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

1. Bellare and Rogaway (ACM CCS 1993) propose the following public-key encryption scheme. Let f be a one-way trapdoor function, the message space be $\{0,1\}^l$, and $G : \{0,1\}^* \to \{0,1\}^l$ a hash function. The encryption of a message m is the pair (u,v), where $u = f(r)$ for a uniformly random r in the domain of f, and $v = m \oplus G(r)$.

(a) How can a ciphertext (u,v) prepared by this encryption scheme be decrypted? **(5)**

Solution The recipient uses his knowledge of the trapdoor to recover $r = f_{td}^{-1}(u)$. The message is then recovered as $m = v \oplus G(r)$.

(b) Prove that this scheme is IND-CPA secure in the random-oracle model, given that f is one-way. Ronald interacts with a hypothetical PPT adversary $\mathscr{A}$ that can win the IND-CPA game against this Bellare–Rogaway scheme with non-negligible advantage. Clearly mention: (i) the reduction objective of Ronald, (ii) how Ronald simulates encryption, (iii) how random-oracle queries are answered before and after the challenge, and (iv) how Ronald's objective is satisfied at the end of the game. **(20)**

Solution **(i) Objective of Ronald:** Ronald is supplied with a random u^* in the range of f. Ronald wants to compute $r^* = f_{td}^{-1}(u^*)$ without knowing the trapdoor.

(ii) Simulation of Encryption: $\mathscr{A}$ supplies two different l-bit messages m_0, m_1. Ronald chooses a random bit $b \in_U \{0,1\}$, and a random $v^* \in_U \{0,1\}^l$. Ronald sends to $\mathscr{A}$ the pair $c^* = (u^*, v^*)$ as the purported encryption of m_b. Ronald's input u^* uniquely identifies r^*. In order that c^* is a valid ciphertext of m_b, we must have $G(r^*) = v^* \oplus m_b$.

Solution **(iii) RO Queries:** Ronald maintains a G-table of $(Q, G(Q))$ pairs queried by $\mathscr{A}$. Now, suppose $\mathscr{A}$ asks Ronald to return $G(Q)$. Ronald can verify whether $Q = r^*$ by checking whether $f(Q) = u^*$. In the pre-challenge phase, we have $Q = r^*$ only with negligible probability, because without seeing u^* the probability that $\mathscr{A}$ makes this query is negligible.

If $Q \neq r^*$, then Ronald searches his G-table for Q. If Q is already present, the corresponding $G(Q)$ value is returned. Otherwise, Ronald generates a uniformly random string $\gamma \in_U \{0,1\}^l$, adds the pair (Q, γ) to his G-table, and returns γ to $\mathscr{A}$.

So suppose that $Q = r^*$, and this can happen, except with negligible probability, in the post-challenge phase. If $G(r^*)$ is already defined, the saved value is returned. Otherwise, Ronald computes $\gamma^* = v^* \oplus m_b$, stores the pair (r^*, γ^*) in his G-table, and returns γ^* to $\mathscr{A}$.

(iv) End of Game: If $G(r^*)$ is not defined, then both the values $m_0 \oplus v^*$ and $m_1 \oplus v^*$ are equiprobable to be the value of $G(r^*)$. Consequently, without making the oracle query of $G(r^*)$, the adversary $\mathscr{A}$ cannot have any advantage in deciding the bit b. But then since $\mathscr{A}$ is supposed to have a non-negligible advantage, it would make the query $G(r^*)$ at some point in the post-challenge phase. Whenever it does, Ronald sees $f(r^*) = u^*$, and his objective of inverting f on u^* is fulfilled.

(c) Show that this scheme not IND-CCA2 secure. **(5)**

Solution Let $c^* = (u^*, v^*)$ be the challenge ciphertext presented by the oracle as an encryption of m_b. But then, for any random l-bit string ρ, $c' = (u^*, v^* \oplus \rho)$ is an encryption of $m_b \oplus \rho$. Since $c' \neq c^*$ (if ρ is non-zero), a decryption query on c' is allowed in the post-challenge phase. If m' is returned, then $m_b = m' \oplus \rho$.

(d) We apply the Fujisaki–Okamoto transform to convert this Bellare–Rogaway scheme to an IND-CCA2 secure scheme. Explain how encryption and decryption work after the application of the FO transform. **(10)**

Solution Let $l = l_0 + l_1$. We now encrypt an l_0-bit message m padded by an l_1-bit random salt s. We need to use a second hash function H from $\{0,1\}^l$ to the domain of f. So the steps during encryption are as follows.

1. Choose $s \in_U \{0,1\}^{l_1}$.
2. Compute $r = H(m \,||\, s)$.
3. Compute $u = f(r)$ and $v = (m \,||\, s) \oplus G(r)$.
4. Output the ciphertext (u, v).

For decrypting (u, v), we proceed as follows.

1. Use the trapdoor to compute $r = f_{td}^{-1}(u)$.
2. Compute $\mu = v \oplus G(r)$.
3. If $r \neq H(\mu)$, return *failure*.
4. Decompose $\mu = m \,||\, s$ with $|m| = l_0$ and $|s| = l_1$.
5. Return m.

Use this space for leftover answers and rough work