32

CSCI 5440: Theory of Cryptography **2020-2021 Term 1**

Midterm

Student: Yu Zheng Student ID: 1155113945

Question 1

- Consider a 2-party secret-sharing scheme $(Share, Rec)$, where $Share$ is a randomized algorithm that inputs secret K' and outputs shares K_0, K_1, and Rec is an algorithm that inputs K_0, K_1 and outputs s with probability one. To define chosen plaintext attack (CPA) security, we model Eve as a circuit interacting with an encryption oracle, and he knows either K_0 or K_1. The encryption oracle $Enc_{K'}$ holds its key K' which can be reconstructed by inputting both K_0 and K_1 to Rec.

  Definition 1. *A scheme (Enc, Dec) is (s, q, ϵ)-universal CPA simulatability (by size t) against 1-of-2 leaked keys if there exists a sampler Sim (of size t) such that for every size-s, q-query oracle circuit D, the view $D^{Enc_{K'}, K_{i,i\in\{0,1\}}}$ and the output of Sim are (s, q, ϵ)-indistinguishable.*

- Construct the following secret-key encryption scheme based on a (s, q, ϵ)-pseudo-random function $F_K : \{0,1\}^k \to \{0,1\}^m$:

$$Enc(K, M) = \{\text{choose random } X \sim \{0,1\}^m, \text{ output } (X, M + F_K(X))\}$$

$$Dec(K, (X, C)) = C + F_K(X)$$

  where message $M \sim \{0,1\}^m$, and $K = Rec(K_0, K_1)$ (as defined in Q1(a)).

  Proof: We pretend the pseudorandom function F_K behaves like a truly random function R. To analyze the security, we first replace R by F_K with a secret-key K, then reconstructing K by K_0, K_1. By the first replacement, we know that the views $D^{Enc_{F_K}}$ and D^{Enc_R} are ϵ-indistinguishable for any $(s - O(mq))$-size, q-query circuit D. This can be easily proved by contradiction. Suppose there is a PRF-distinguisher D'. When D queries its oracle at M, D' queries its oracle F at a random X and forwards $(X, M + F(X))$ as the answer. Now we show how to simulate the view D^{Enc^R} without knowing R. Since expecting different queries to Enc^R to result in independent random ciphertexts, we consider a simulator Sim that outputs uniform random bits. If q queries of X's are different, the ciphertexts are distinct. The probability of getting a collision among Xs is at most $\binom{q}{2} \cdot 2^{-n}$. That is, the random variables Enc^R and Sim are identically distributed unless an event of probability at most $\binom{q}{2} \cdot 2^{-n}$ occurs. Thus, we proved that (Enc, Dec) is $(s - O(mq), q, \epsilon + \binom{q}{2} \cdot 2^{-n})$-CPA simulatable. The second part is to argue the scheme against 1-of-2 leaked keys. Notably, we analyze security above without referring the secret key which is owned by the oracle securely, *i.e.*, no secret key on the adversary's view. Now consider the secret-sharing scheme on K defined in Q1(a). The adversary has either K_0 or K_1. By the definition, the adversary cannot reconstruct the secret key K since he does not know both K_0 and K_1,

10

which implies knowing one K_i does nothing with the above security analysis. Therefore, we proved the statement as required.

Question 2

- Proof: F is $(s+t, q, \epsilon)$-pseudorandom, which means indistinguishable with advantage at most ϵ by a circuit of size at most s that makes at most q oracle queries. To prove that F' is a pseudorandom function, we need to compare the view of the distinguisher D' interacting with F' to the view of D' interacting with a truly random function R'. The question is that the input to F is a hash function H. If we can find a collision of H, D' can distinguish F' with R'. The reason is that inputting different x', x results in same F' and random R'. Thus, for q queries of F, the inputs $H_{K'}(x)$ should be not collision. The possibilities of collision are at most $\binom{q}{2}$, *i.e.*, $O(q^2)$. Let $s' = s + O(q^2 t)$, then H is (s', ϵ)-collision resistant. This means that for every circuit C of size at most s, the probability $C(K')$ outputs a collision for $H_{K'}$ over random choice of K' is at most ϵ. When the distinguisher D' interacts with F', the simulating circuit provides the input to F'. Consider outputting the collision cases at most $O(q^2)$ and the circuit size t, the circuit size for F' is $s' - O(q^2 t) = s + O(q^2 t) - O(q^2 t)$, which is equal to s. As analysis above, the circuit of size at most s is also make q queries the same as cases with F. Now, we consider the advantage. Since having advantage either to distinguish F or to distinguish H would help to distinguish F', the advantage should be at most $\epsilon + \epsilon$. Therefore, we proved the statement involving a triple $(s, q, 2\epsilon)$.

- Proof: The statement is same to "If F' is an $(s+O(t), 2, \epsilon - 2^{-m})$-pseudorandom function, then H is (s, ϵ)-collision resistant." Let's first consider the intuitive proof and ignore the parameters. If F' is a pseudorandom function, then we know H should not be "broken" easily under some assumption. This can be easily proved by contradiction since we can differentiate the outputs of F' with different inputs x', x (collision means same inputs to F_K). Next, let's work out the parameter part. The expected q independent queries to H are distinct but colliding is the total number $\binom{q}{2}$. A single collide is at least $2^{-m} - 2^{-k}$, where k is the input length and m is the output length. Thus, for $q = 2$, the probability is $\binom{q}{2} \cdot 2^{-m} = \dfrac{q(q-1)}{2 \cdot 2^m} = 2^{-m}$. The probability of finding a collision of H is $(\epsilon - 2^{-m}) + (2^{-m}) = \epsilon$ by either F' or the analysis above. Consider a circuit of size s acting of an adversary to H. The circuit size for F' should be $s + O(t)$ by considering the additional function size. Therefore, we proved the statement as required.

Question 3

- Decryption: Let $C = PK_A^R \cdot PK_B^R \cdot M$. Then, we have,

$$C = g^{AR} \cdot g^{BR} \cdot M = (g^R)^A \cdot (g^R)^B \cdot M$$

After receiving encryption from Charlie, Bob and Alice know the g^R and C. Alice computes $(g^R)^A$ under her private key A and send it to Bob. Bob computes $(g^R)^B$ under his private key B and send it to Alice. Now, both Alice and Bob have g^{AR}, g^{BR} and compute

$PK' = g^{AR} \cdot g^{BR}$. At last, both of them decrypt to get message M by $\frac{C}{PK'}$. During above decryption, Alice keeps A secretly, and Bob keeps B secretly. ✓

- Proof by contradiction: Suppose Alice's view is not $(s - O(t), \epsilon)$-simulatable, *i.e.*, having probability $> \epsilon$ to get M on her view. This is equal to that she can know $g^{AR} \cdot g^{BR} = g^{AR} \cdot (g^R)^B$ by viewing g^R, g^{AR}. The needs to break one DDH problem for $(g^R)^B$ with probability $> \epsilon$. Yet, this contradicts the assumption. Consider Alice has a simulator of size s' to find the message M. According to the analysis above, she need to work out the group operation with 1 DDH. Then, the circuit (acting as an adversary) to DDH should be $s' + O(t)$, which is equal to s. We have $s' = s - O(t)$. Therefore, we proved the statement corresponding to the parameters. ✓

10

Question 4

- If (s, ϵ)-DDH holds, the following two-party computation for the equality function ($f(x, y) = 1$ if $x = y$ and 0 if not): (1) Alice sends (g^R, g^{xR}) for a random R; (2) Upon receiving (h, k), Bob outputs 1 if $h^y = k$ and 0 otherwise; are (s, ϵ)-simulatable against honest-but-curious parties in size $t + O(op)$.

  Proof: Alice receives nothing from Bob, so she knows nothing about the output of the equality function. She's view only consists of (R, g^R) which are sampled and computed by her. Next, let's consider the Bob's view. When $x = y$, Bob's view consists (h, k, h^y), where $h^y = k$. In this case, he knows $x = y$. When $x \neq y$, Bob's view consists (h, k, h^y), where are simulatable to random variables (i, j, v) with probability ϵ. By the DDH simulatability, this view is (s, ϵ)-simulatable in size t. Altogether, given his output and input, Bob can simulate his view in size $t + O(op)$, where op stands generically for the size of an efficient operation like sampling a random element.

3

NO, BECAUSE x IS NOT RANDOM.