CSCI 5440: Theory of Cryptography

2019-2020 Term 1

Assignment 1

Student: ZHENG Yu Student ID: 1155113945

Acknowledge: Thank William H.Y. Mui, Jack P.K. Ma, and Yongjun Zhao for discussion.

Question 1

• Yes. t = 2. The construction is,

$$\operatorname{Res}(X_i, X_j) = \overline{X_i \operatorname{xor} X_j}$$

NEED TO SHOW THE DISTRIBU-TIONS ARE THE SAME

where X_i, X_j are shares.

Proof: Obviously each party does not know the secret, *i.e.*, t = 1. For any two parties, the secret is constructed. If two shares are different, the secret is 0; If two shares are same, the secret is 1.

- No. At least 5 shares can help to reconstruct the secret, thus $t \leq 5$. Suppose we are luck to get 5 zeros/ones. However, 5 shares can not reconstruct the secret sometimes. For all possible t, the distribution of shares in the subset for s=1 is not identically distributed to that in the subset for s=0 since the number of 1 and 0 is not equal.
- Yes. t = 2. The construction is,

$$\operatorname{\mathsf{Res}}(X_i,X_j) = X_i \mathsf{xor} X_j$$

where X_i, X_j are shares.

Proof: For party i, the share is r+i for s=1; r for s=0. This case is same as Q1(a). Obviously each party does not know the secret, i.e., t=1. For any two parties, the secret is constructed. If two shares are different, the secret is 1; If two shares are same, the secret is 0.

Question 2

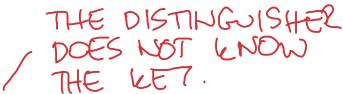
• Proof: Since $\mathsf{Enc}(K,M)$ and $\mathsf{Enc}(K,M')$ are strictly less than 1/2-statistically close, we have,

$$|\Pr[\mathsf{Enc}(K,M) = C] - \Pr[\mathsf{Enc}(K,M') = C]| < 1/2$$

That is,

$$-1/2 < \Pr[\mathsf{Enc}(K,M) = C] - \Pr[\mathsf{Enc}(K,M') = C] < 1/2$$

$$-1/2 + \Pr[\mathsf{Enc}(K,M') = C] < \Pr[\mathsf{Enc}(K,M) = C] < 1/2 + \Pr[\mathsf{Enc}(K,M') = C]$$



Since C is the encryption of M' under key K, the probability $\Pr[\operatorname{Enc}(K, M') = C] = 1$. Besides, the probability is [0, 1]. Thus, we have,

$$1/2 < \Pr[\mathsf{Enc}(K, M) = C] < 1$$

• Proof: Let $\mathcal{M}, \mathcal{K}, \mathcal{C}$ be message space, key space, and encryption space. For a fixed key, we get

$$\Pr[\mathsf{Enc}(K, M) = C | \mathcal{M} = M] = 1/2^k$$

Since the key is fixed and Enc(K, M) and Enc(K, M') are strictly less than 1/2-statistically close, we have,

$$\sum_{M' \in \mathcal{M}} \Pr[\mathsf{Enc}(K, M') = C] > 1/2^k \cdot (1/2) = 1/2^k \cdot (1/2^m) \cdot 2^{m-1}$$

The number of possible messages is lager than 2^{m-1} . Thus, we proved the possible encryption for more than half the messages.

• Proof: We want to show that Enc is not a perfectly secure scheme for k < m. To this end, we show that there exist messages M_0 and M_1 , and a ciphertext C, such that,

$$\Pr[\mathsf{Enc}(K, M_0)] > 0 \text{ and } \Pr[\mathsf{Enc}(K, M_1)] = 0$$

Here, K is a random variable, uniformly distributed over K. To do this, choose any message $M_0 \in \mathcal{M}$, and any key $K_0 \in K$. Let $C = \mathsf{Enc}(K_0, M_0)$. It is clear that $\mathsf{Pr}[\mathsf{Enc}(K, M_0)] > 0$ holds. Next, let,

$$\mathcal{S} = \{ \mathsf{Dec}(K_1, C) : K_1 \in \mathcal{K} \}$$

Then, we know,

$$|\mathcal{S}| \le k < m$$

where $|\cdot|$ denotes the bit-length. Then we choose a message $M_1 \in \mathcal{M} \setminus \mathcal{S}$. To prove $\Pr[\mathsf{Enc}(K, M_1)] = 0$, we need to show that there is no key K_1 such that $\mathsf{Enc}(K_1, M_1) = C$. We give the proof from contradiction. Assume that there exists $\mathsf{Enc}(K_1, M_1) = C$ for some K_1 . Then, for this key K_1 , by the correctness property for ciphers, we would have

$$\mathsf{Dec}(K_1,C)=M_1$$

which implies that M_1 belongs to S. This contradicts that $M_1 \in \mathcal{M} \setminus S$. Thus the we proved the statement.

Reference: Page 13, A Graduate Course in Applied Cryptography by Dan Boneh and Victor Shoup.

Question 3

• Yes. F' is pseudorandom.

WHAT IS THE JOINT DISTIZIBUTION OF R AND K ? IF THEY ARE

Proof: We know that F_K is a pseudorandom function, implying that the output of F_K is indistinguishable to a random variable. Suppose that F'(K) is not a pseudorandom function, there exists a distinguisher \mathcal{D} who can succeed in distinguishing a random variable R and function F', saying,

$$\Pr[\mathcal{D}(F'(x)) = 1] - \Pr[\mathcal{D}(R) = 1] > \epsilon$$

Since $F'_{K}(x) = F_{K}(x) + F_{K}(l(x))$, we have,

$$\Pr[\mathcal{D}(F_K(x) + F_K(l(x)) = 1] - \Pr[\mathcal{D}(R) = 1] > \epsilon$$

The output of F_K is indistinguishable to a random variable R, so we reduce the above inequality to,

$$\Pr[\mathcal{D}(R + F_K(l(x)) = 1] - \Pr[\mathcal{D}(R) = 1] > \epsilon$$

So the question turns to distinguish $F_K(l(x))$ and R. F(x) is a PRF, implying that F(x) and F(y) are independent for all x, y. The question is to prove a distinguisher \mathcal{D} that,

$$\Pr[\mathcal{D}(R + F_K(y) = 1] - \Pr[\mathcal{D}(R) = 1] > \epsilon$$

Similarly, the above inequality holds if \mathcal{D} can distinguish F_K and a random function. However, this contradicts the assumption in the first stage. Therefore, we have proved that F' is a pseudorandom function.

Remark: An exponential distinguisher can be constructed as following: For bit length k, the possibilities are 2^k . $\{F(0)+F(1)\},\{(F(1)+F(2)\},\ldots,\{F(2^k-2)+F(2^k-1)\},\{F(2^k-1)+F(0)\}\}$. The linear combination of above elements gives the answer, which contradicts the distinguisher should be in polynomial/constant/etc.

• No. F' is not pseudorandom.

Proof: Since this question does not limit the input to the function F, we can query the function F' (i.e., acting as an attacker/distinguisher) with some special inputs. Construct a distinguisher \mathcal{D} ,

$$\mathcal{D} = F'_{K,K'}(x,x) + F'_{K,K'}(x,y) + F'_{K,K'}(y,x) + F'_{K,K'}(y,y)$$

Simplify this equation,

$$\mathcal{D} = (F_K(x) + F_{K'}(x)) + (F_K(x) + F_{K'}(y)) + (F_K(y) + F_{K'}(x)) + (F_K(y) + F_{K'}(y))$$
$$= (F_K(x) + F_K(x)) + (F_{K'}(x) + F_{K'}(x)) + (F_K(y) + F_K(y)) + (F_{K'}(y) + F_{K'}(y))$$

For bit addition, $F_K(x) + F_K(x) = 0^n$. Thus, we know that the output of \mathcal{D} is equal to 0. That, there exists at least 1 distinguisher that can help us (or have some advantage) to distinguish the outputs of F' and random numbers.

• I guess the answer is no.

Question 4

• For writing the definition easily, let us use K_0 and K_1 to substitute K_A and K_B .

Definition 1. (Noise key encryption) A noise key encryption scheme $\Sigma = (\text{KeyGen}, \text{Enc}, \text{Dec})$ is a type of private-key encryption, which includes the following algorithms:

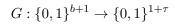
- KeyGen(k,b) is a key generation algorithm that inputs parameters k,b, where b < k. It outputs two keys $K_0, K_1 \in \mathbb{Z}_{2^k}$ satisfying that $|K_0 - K_1| \le 2^b$.
- $\mathsf{Enc}(K_i, M)$ is an encryption algorithm that inputs a message M and an encryption $key\ K_i,\ i \in \{0,1\}$. It outputs a ciphertext C.
- $\mathsf{Enc}(K_{1-i},C)$ is a decryption algorithm that inputs a ciphertext C and a decryption $\mathsf{key}\ K_{1-i}$. It outputs the message M.

Dec

• Yes.

Proof: Let's construct a special encryption scheme to prove the existence. According to Definition 1, we know that the key length is k. Suppose the message length is k-b-1. Since the error range of key is $[-2^b-1,2^b]$, the noise exists in the least significant b bits. We use the most significant k-b-1 bits of key to encrypt the message. Here, the most significant k-b-1 bits of K_0 and K_1 are exactly same, which can be regarded of the keys of secure general secret key encryption. Besides, the most significant k-b-1 bits of keys are elements of $\mathbb{Z}_{2^{k-b-1}}$, which are individually uniformly distributed. This satisfies the requirement of secure private key encryption. Therefore, we proved there exists a perfectly secure noise key encryption scheme.

- (1) Proof: Let's prove the statement by contradiction. For any messages with length $\geq k-b$, suppose the scheme satisfies perfect security. Let's start with the message with length k-b. For every key K_i and every pair of messages M, M' of length k-b, the random variables $\mathsf{Enc}(K_i, M)$ and $\mathsf{Enc}(K_i, M')$ are identically distributed. Since $\mathsf{Enc}(K_i, M)$ are noisy encryption scheme, we have another decryption key K_{1-i} corresponding to this message. For some pairs K_i and K_{1-i} , the bit at the location of k-b is different, i.e., one is 1 and the other is 0. In this case, we need keys more than the messages for the first k-b bits, which contradicts the uniform distribution. Similarly, for messages with length k-b, this distribution of encryptions is not identically distributed since the distribution of keys is not identically distributed for each message. Therefore, we proved the statement that "the message length is k-b or more then perfect security is no longer possible."
 - (2) Define that the message length is $k-b+\tau$, where $\tau \geq 0, \tau \in \mathbb{Z}_{b+1}$. The first k-b-1 bits of the message is encrypted by the most significant k-b-1 bits of K_0, K_1 . Notably, the most significant k-b-1 bits of K_0, K_1 defined by K^{left} are same and uniformly distributed over $\mathbb{Z}_{2^{k-b-1}}$. For the last $1+\tau$ bits, we use a pseudorandom generator (PRG) to generate them which are ϵ -indistinguishable from a uniformly random $(1+\tau)$ -bit string. Now, we define such a PRG:



where G outputs a pseudorandom number K^{right} for each key pair $\{K_0, K_1\}$. Then, we use $K^{\text{left}}||K^{\text{right}}$ as the encryption key, where || denotes concatenation.

Proof: By Q4(a), we know the first (k-b)-bit encryption is perfectly secure. The last $\tau+1$ encryption is encrypted by a key which is ϵ -indistinguishable from a random number. That is, the last $\tau+1$ encryption is ϵ -indistinguishable from a random number. By combining these two parts (using the technique of Theorem 8 in Lecture 2), we know that the whole encryption is ϵ' -indistinguishable from a random number. Therefore, the construction is computationally secure.