期中试卷讲解

Wenhao Wang

Nanjing University

期中试卷讲解 - Q1

Q1 (15 points)

Is the following cipher a perfectly secret encryption? Prove your answer.
(下述密码算法是完美保密加密吗？请证明你的答案。)
$M = \{1, 2, 3\}$, $K = \{1, 2, 3\}$;
Gen: Pick k uniformly at random from K;
Enc(m): $c = m * k \mod 4$; ($*$ means multiply with)

No. We can determine whether a cipher is perfectly secrecy based on the **Definition 2.3** (Page 27) or the **Lemma 2.5** (Page 28).
We calculate the conditional probability $Pr\{M = m | C = 0\}$:

- **When** $c = 0$: Only $m = 2$ can produce $c = 0$, so $Pr\{M = 2 | C = 0\} = 1$. This means that the ciphertext $c = 0$ completely reveals the plaintext $m = 2$.

Since there exists a ciphertext $c = 0$ that fully exposes the corresponding plaintext, the encryption scheme **does not satisfy perfect secrecy**.

期中试卷讲解 - Q2

Q2 (15 points)

Which of the following functions are negligible function in λ? (以下哪些是关于 λ 的可忽略函数？)

1. $\frac{1}{2^{\lambda/2}}$
2. $\frac{1}{2^{\log(\lambda^2)}}$
3. $\frac{1}{\lambda^{\log(\lambda)}}$
4. $\frac{1}{\lambda^2}$
5. $\frac{1}{2^{(\log\lambda)^2}}$

A function $f(\lambda)$ is negligible if, for every positive polynomial $p(\lambda)$, there exists some λ_0 such that for all $\lambda > \lambda_0$, $f(\lambda) < \frac{1}{p(\lambda)}$.

Yes, No, Yes, No, Yes

期中试卷讲解 - Q2 - 5

To prove that $f(\lambda) = \frac{1}{2^{(\log\lambda)^2}}$ is a negligible function, we need to show that: $f(\lambda) < \frac{1}{\lambda^c}$, for any constant c>0, when λ is sufficiently large.

$$\frac{1}{2^{(\log\lambda)^2}} < \frac{1}{\lambda^c}$$
$$2^{(\log\lambda)^2} > \lambda^c.$$
$$(\log\lambda)^2 > c \cdot \log\lambda$$
$$\log\lambda \cdot (\log\lambda - c) > 0$$

The inequality holds when:

$$\log\lambda > c.$$

We choose $\lambda_0 = 2^c$: For all $\lambda > \lambda_0$, we have:

$$(\log\lambda)^2 > c \cdot \log\lambda$$

This proves that $f(\lambda) = \frac{1}{2^{(\log\lambda)^2}} < \frac{1}{\lambda^c}$ for any constant $c > 0$, as long as λ is sufficiently large.

期中试卷讲解 - Q3-1

Q3-1 (10 points)

Let F be a PRF with input length 2λ, and let G be a length-doubling PRG of input length λ. Let $F'(k, x) = F(k, G(x))$.

- Is F' necessarily a PRF? Prove your claim.(F' 一定是 PRF 吗？证明你的结论)

No. We give a **counterexample**:
Define 2 blocks x_1, x_2 with length $= \lambda$ and they are different with each other. Let $G(x_1) = G(x_2)$.

We construct a distinguisher D' to distinguish an oracle for F' from an oracle for f, where f is a random function, as follows:

期中试卷讲解 - Q3-1

First, D' ask its oracle on x_1 and get the output y_1, then use x_2 to ask its oracle and get the output y_2. D' outputs 1 when it receives $y_1 = y_2$ and output 0 otherwise.

When the oracle is F', D' **always outputs** 1; When the oracle is a random function f, D' **outputs** 1 **with the probability** $\frac{1}{2^{2\lambda}}$.
Therefore, we have

$$\left| Pr\left[D^{F'(\cdot)}(1^{2\lambda}) = 1\right] - Pr\left[D^{f(\cdot)}(1^{2\lambda}) = 1\right] \right| = 1 - \frac{1}{2^{2\lambda}} = 1 + negl(\lambda)$$
$$> \frac{1}{2} + negl(\lambda),$$

which means F' is not a PRF.

期中试卷讲解 - Q3-2

Q3-2 (10 points)

Let F be a PRF with input length 2λ, and let G be a length-doubling PRG of input length λ. Let $F'(k, x) = F(k, G(x))$.

- If G is injective (i.e. $G(x) = G(y)$ implies $x = y$), is F' necessarily a PRF? Prove your claim. (**如果 G 是单射，F' 一定是 PRF 吗？证明你的结论**)

Yes. We prove it by reduction.

Setup: Assuming F' is not a secure PRF, there is a distinguisher D' to distinguish an oracle for F' from an oracle for $f: \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ which wins with non-negligible probability:

$$\left|\Pr\left[D'^{F'(\cdot)}\left(1^\lambda\right) = 1\right] - \Pr\left[D'^{f(\cdot)}\left(1^\lambda\right) = 1\right]\right| = \varepsilon(\lambda) \tag{1}$$

期中试卷讲解 - Q3-2

Queries: We construct a distinguisher D to distinguish an oracle for F from an oracle for f by invoking D'.
D is given input 1^λ and access to an oracle $O : \{0,1\}^{2\lambda} \to \{0,1\}^{2\lambda}$.
For every query x that D' makes to its oracle, D computes $G(x)$, query $O(\cdot)$ at $G(x)$, and return the answer $O(G(x))$ to D'.

Analysis: Finally, D output the same bit with D'.
When D's oracle is F, by query its oracle on x, D' gets the answer $F(k,(G(x)))$. The view of D' is identical to its view when it is given an oracle for F'. Thus,

$$\Pr\left[D^{F(\cdot)}(1^{2\lambda}) = 1\right] = \Pr\left[D'^{F'(\cdot)}(1^{\lambda}) = 1\right]. \tag{2}$$

期中试卷讲解 - Q3-2

When D's oracle is a random function, the answer of x is $f'(G(x))$, where $f' : \{0,1\}^{2\lambda} \to \{0,1\}^{2\lambda}$. Suppose that $q(n)$ is a bound on the number of queries made by D'. When D' is given an oracle for f, the view of D' is $f(x_1), f(x_2), \ldots, f(x_{q(n)})$. In the simulation of D, the view of D' is $f'(G(x_1))$, $f'(G(x_2)), \ldots, f'(G(x_{q(n)}))$.
Because G **is injective**, both views are the outputs of f at $q(n)$ different points with the same probability distribution. Thus,

$$\Pr\left[D'^{f(\cdot)}\left(1^{\lambda}\right)=1\right]=\Pr\left[D^{f'(\cdot)}\left(1^{2\lambda}\right)=1\right] \tag{3}$$

And,

$$\left|\Pr\left[D^{F(\cdot)}\left(1^{2\lambda}\right)=1\right]-\Pr\left[D^{f'(\cdot)}\left(1^{2\lambda}\right)=1\right]\right|=\varepsilon(\lambda), \tag{4}$$

where $\varepsilon(\cdot)$ is non-negligible.
D **breaks the security of** F which contradicts to the condition.
Therefore, F' **is a secure PRF.**

期中试卷讲解 - Q4

Q4 (30 points)

Assume a toy block cipher $e()$ for encryption of 5-bit blocks. The encryption function is a bit permutation, which depends on the key. We assume that for a given key the encryption (permutation) is as follows:

$$e(b_1 b_2 b_3 b_4 b_5) = (b_2 b_5 b_4 b_1 b_3)$$

Encrypt the message $x = 01101 \quad 11011 \quad 11010 \quad 00110$ with the four different modes of operation ECB, CBC, OFB and CTR, and provide the corresponding ciphertext y. Use IV $= 11001$ as initialization vector.

期中试卷讲解 - Q4 - ECB (Electronic Codebook Mode)

In ECB, each plaintext block is independently encrypted:
$y_i = e(x_i)$, for each block x_i.
Using the permutation function $e()$:

1. e(01101) = 11001
2. e(11011) = 11110
3. e(11010) = 10110
4. e(00110) = 00101

期中试卷讲解 - Q4 - CBC Cipher Block Chaining Mode

In CBC, each plaintext block is XORed with the previous ciphertext block before encryption:

$$y_1 = e(x_1 \oplus IV), \quad y_i = e(x_i \oplus y_{i-1}) \text{ for } i \geq 2$$

Here, $\oplus$ denotes bitwise XOR.

- $y_1 = IV = 11001$.
- $x_2 \oplus y_1 = 01101 \oplus 11001 = 10100$, then $e(10100) = 00011$. So $y_2 = 00011$.
- $x_3 \oplus y_2 = 11011 \oplus 00011 = 11000$, then $e(11000) = 10010$. So $y_3 = 10010$.
- $x_4 \oplus y_3 = 11010 \oplus 10010 = 01000$, then $e(01000) = 10001$. So $y_4 = 10000$.
- $x_5 \oplus y_4 = 00110 \oplus 10000 = 10110$, then $e(10110) = 00111$. So $y_5 = 00111$.

Ciphertext (CBC): $y = 11001 \quad 00011 \quad 10010 \quad 10000 \quad 00111$

期中试卷讲解 - Q4 - OFB (Output Feedback Mode)

In OFB, the output of the cipher is fed back as input, and the plaintext is XORed with the output:

$$z_i = e(z_{i-1}), \quad y_i = x_{i-1} \oplus z_i \text{ for } i \geq 2.$$

- $y_1 = z_1 = IV = 11001$.
- $z_2 = e(z_1) = e(11001) = 11010, y_2 = x_1 \oplus z_2 = 01101 \oplus 11010 = 10111$.
- $z_3 = e(z_2) = e(11010) = 10110, y_3 = x_2 \oplus z_3 = 11011 \oplus 10110 = 01101$.
- $z_4 = e(z_3) = e(10110) = 00111, y_4 = x_3 \oplus z_4 = 11010 \oplus 00111 = 11101$.
- $z_5 = e(z_4) = e(00111) = 01101, y_5 = x_4 \oplus z_5 = 00110 \oplus 01101 = 01011$.

Ciphertext (OFB): $y = 11001 \quad 10111 \quad 01101 \quad 11101 \quad 01011$

期中试卷讲解 - Q4 - CTR (Counter Mode)

In CTR, a counter value is encrypted and XORed with the plaintext:

$$z_i = e\left(\mathrm{CTR}_i\right), \quad y_{i+1} = x_i \oplus z_i$$

Assume the initial counter value is $CTR_1 = IV = 11001$, and subsequent counters increment by 1 .

- $y_1 = \mathrm{CTR}_1 = \mathrm{CTR} = 11001.$
- $\mathrm{CTR}_2 = 11010, z_1 = e(11010) = 10110, y_2 = x_1 \oplus z_1 = 01101 \oplus 10110 = 11011.$
- $\mathrm{CTR}_3 = 11011, z_2 = e(11011) = 11110, y_3 = x_2 \oplus z_2 = 11011 \oplus 11110 = 00101.$
- $\mathrm{CTR}_4 = 11100, z_3 = e(11100) = 10011, y_4 = x_3 \oplus z_3 = 11010 \oplus 10011 = 01001.$
- $\mathrm{CTR}_5 = 11101, z_4 = e(11101) = 11011, y_5 = x_4 \oplus z_4 = 00110 \oplus 11011 = 11101.$

Ciphertext (CTR): $y = 11001 \quad 11011 \quad 00101 \quad 01001 \quad 11101$

期中试卷讲解 - Q5-1

Q5-1 (10 points)

Let $\Pi = (E, D)$ be a cipher. Consider a cipher $\Pi' = (E', D')$, where $E'(k, m) = E(k, E(k, m))$.

- Show that there is an EAV-secure cipher Π such that Π' is NOT EAV-secure. (请找出一个 EAV 安全的密码 Π 使得相应的 Π' 不是 EAV 安全的。)

Let Construction 3.17 in textbook (Page 67) be Π, and then $E(k, m) = G(k) \oplus m$, where $G(\cdot)$ is a PRG. We have proved this construction is a EAV-secure scheme.
In the scheme Π', $E(k, m) = E(k, E(k, m)) = G(k) \oplus G(k) \oplus m = m$.
Obviously, Π' is not EAV-secure.

期中试卷讲解 - Q5-2

Q5-2 (10 points)

Let $\Pi = (E, D)$ be a cipher. Consider a cipher $\Pi' = (E', D')$, where $E'(k, m) = E(k, E(k, m))$.

- Prove if Π is CPA secure, then Π' is also CPA secure. (**请证明如果** Π **是 CPA 安全,** Π' **一定也是 CPA 安全。**)

We prove this by contradiction: Assuming Π' is not CPA-secure, we will find a PPT adversary $\mathcal{A}$ to break the CPA-security of Π.

Setup: Since Π' is not CPA-secure, there exists a PPT adversary $\mathcal{A}'$ and a non-negligible function $\varepsilon(n)$ such that:

$$\Pr\left[\mathrm{PrivK}^{\mathrm{CPA}}_{\mathcal{A}',\Pi'}(n) = 1\right] = \frac{1}{2} + \varepsilon(n).$$

Queries: Using the adversary $\mathcal{A}'$, construct the adversary $\mathcal{A}$ attacking Π as follows:
For every query m that $\mathcal{A}'$ makes to its encryption oracle, $\mathcal{A}$ asks for an encryption of m from its oracle (let c be the response), asks its oracle again for the encryption of c, and returns the second result to $\mathcal{A}'$.
When $\mathcal{A}'$ outputs a pair m_0, m_1, $\mathcal{A}$ asks for the encryption of m_0 and m_1, and outputs the encrypted pair. Then, upon receiving back a challenge ciphertext, $\mathcal{A}$ hands $\mathcal{A}'$ the challenge ciphertext directly.
When $\mathcal{A}'$ outputs a bit b', adversary $\mathcal{A}$ outputs b' as well and halts.
Analysis: We observe that the view of $\mathcal{A}'$ in this game by $\mathcal{A}$ is identical to its view in an execution of experiment $\mathrm{PrivK}^{CPA}_{\mathcal{A}',\Pi'}$. We have that

$$\Pr\left[\mathrm{PrivK}^{\mathrm{CPA}}_{\mathcal{A},\Pi}(n) = 1 | b = 0\right] = \Pr\left[\mathrm{PrivK}^{\mathrm{CPA}}_{\mathcal{A}',\Pi'}(n) = 1 | b = 0\right].$$

and likewise for $b = 1$. Therefore,

$$\Pr\left[\mathrm{PrivK}^{\mathrm{CPA}}_{\mathcal{A},\Pi}(n) = 1\right] = \Pr\left[\mathrm{PrivK}^{\mathrm{CPA}}_{\mathcal{A}',\Pi'}(n) = 1\right] = \frac{1}{2} + \varepsilon(n).$$

$\mathcal{A}$ breaks the CPA-security of Π which contradicts to the condition, so for every CPA-secure schemes Π, the scheme Π' is also CPA-secure.

The End