2025 期中试卷讲解

Assistants

Nanjing University

期中试卷讲解 - Q1

Q1 (10 points)

1) 什么是柯克霍夫准则 (Kerckhoff's Principle)？(5 分)
2) 请举出一个完美保密的加密算法的例子。为什么实际生活中，人们通常不会使用完美保密加密算法来保护数据？(5 分)

1) Kerckhoff's Principle: The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.
2) **完美保密举例**: One-time pad (一次一密): 密钥长度 = 明文长度；密钥是真随机且只能使用一次；加密按位异或。
不常用的原因:

- 密钥管理困难：每次通信需要共享与消息等长的随机密钥，且不能重用；
- 密钥分发问题：安全传送大密钥需要安全信道；
- 存储与带宽开销大：传输和存储密钥的成本高。

期中试卷讲解 - Q2

Q2 (10 points)

若 g,h 都是可忽略函数，则以下哪些函数 f 一定是可忽略的 (negligible)？请直接给出结论，不需要说明理由。(10 分)

1. $f(n) = (\log n)^{-\log n}$
2. $f(n) = (C_n^c)^{-1} = \left(\frac{n!}{c!(n-c)!}\right)^{-1}$
3. $f(n) = \begin{cases} f\left(\frac{n}{3}\right), & \text{if } n = 0 \pmod 3 \\ 3^{-n}, & \text{otherwise} \end{cases}$
4. $f(n) = g(n) + h(n)$
5. $f(n) = g(n)/h(n)$

Note that, " **一定是**"。

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, No, Yes, No

期中试卷讲解 - Q2-1

To prove that $f(n) = (\log n)^{-\log n}$ 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.

$$
\begin{aligned}
(\log\lambda)^{-\log\lambda} &< \frac{1}{\lambda^c} \\
(\log\lambda)^{\log\lambda} &> \lambda^c. \\
e^{\log\lambda \cdot \log\log\lambda} &> e^{c \cdot \log\lambda} \\
\log\lambda \cdot \log\log\lambda &> c \cdot \log\lambda \\
\log\lambda(\log\log\lambda - c) &> 0
\end{aligned}
$$

The inequality holds when:

$$\log\log\lambda > c.$$

We choose $\lambda_0 = e^{e^c}$: For all $\lambda > \lambda_0$, the above inequality holds. This proves that $f(\lambda) = (\log\lambda)^{-\log\lambda} < \frac{1}{\lambda^c}$ for any constant $c > 0$, as long as λ is sufficiently large.

期中试卷讲解 - Q3

Q3 (20 points)

假设 G 是一个伪随机数发生器，请问以下函数是否一定是伪随机数发生器？请简要说明理由。其中 $|a|$ 符号表示 a 的比特长度。(20 分)

1. 定义 $G'(s) \stackrel{\text{def}}{=} G(s_1 s_2 \cdots s_{|s|-1}) \| s_{|s|}$，其中 $\|$ 表示比特串拼接。
2. 定义 $G'(s) \stackrel{\text{def}}{=} G(s) \bigoplus (s \| 0^{|G(s)|-|s|})$，其中 $\bigoplus$ 表示按位异或运算。
3. 定义 $G'(s)$ 如下：若二进制串 s 中 1 的个数恰好为 $\lfloor \frac{|s|}{2} \rfloor$，则 $G'(s) \stackrel{\text{def}}{=} 0^{|G(s)|}$，否则 $G'(s) \stackrel{\text{def}}{=} G(s)$。
4. 定义 $G'(s) = G(s \bigoplus 1^{|s|})$.

1) **是**。由于 s 均匀随机，$s_1 s_2 \cdots s_{|s|-1}$ 也均匀随机，因此 $G(s_1 s_2 \cdots s_{|s|-1})$ 是伪随机的。而拼接上的 $s_{|s|}$ 是均匀随机且独立的比特，因此整体输出与均匀随机字符串不可区分。

2) **不一定**。一个反例是，G 会直接暴露 s 的第一位，$G(s)_1 = s_1$，这样 $G'(s)$ 的第一位一定是 0，显然不是 PRG。

期中试卷讲解 - Q3

3) **不一定**。根据斯特林公式 $s! \approx \sqrt{2\pi s}\left(\frac{s}{e}\right)^s$，有 $\binom{s}{\lfloor s/2 \rfloor} = \Theta\left(\frac{2^s}{\sqrt{s}}\right)$，进而 $\frac{\binom{s}{\lfloor s/2 \rfloor}}{2^s} = \Theta\left(\frac{1}{\sqrt{s}}\right)$，这意味着 $G'(s) = 0^{|G(s)|}$ 的概率不可忽略。

4) **是**。由于 s 均匀随机，$s \oplus 1^{|s|}$ 也均匀随机，因此 $G'(s)$ 的分布与 $G(s)$ 相同。若 G 是 PRG，则 G' 也是 PRG。

期中试卷讲解 - Q4

Q4 (20 points)

已知 F 是一个伪随机函数，请问下面的 F' 是否一定是伪随机函数，请简要说明理由。(20 分)

1. $F'(k,x) = F(k,x) \| F(k,\bar{x})$ ，$\|$ 表示比特串拼接，$\bar{x}$ 表示 x 按位取反.
2. $F'(k,x) = F(k, G(x))$ ，F 是输入长度为 2λ 的伪随机函数，G 是扩展因子 $l(n) = 2n$ 的伪随机数发生器.

1) **不一定 (No)**。
F' 的输出具有明显的对称结构。
Distinguisher: 敌手选择输入 x，查询得到 $y_1 = F'(k,x) = a \| b$ 。然后查询 x 的反码 $\bar{x}$，得到 $y_2 = F'(k,\bar{x}) = b \| a$ 。若 y_1 的后半段等于 y_2 的前半段，则输出 1。对于真随机函数，此情况发生概率为 $2^{-\lambda}$ (可忽略)。

期中试卷讲解 - Q4

2) **不一定 (No)**。
理由：PRG 的定义仅保证针对**均匀随机**输入的输出不可区分，并不保证对**特定**输入无碰撞（Collision Resistance）。
Counterexample：题目中说 G 是一个安全的 PRG，我们可以构造 G'：当 $x = 0^n$ 或 $x = 1^n$ 时，$G'(x) = 0^{2n}$，其余情况 $G'(x) = G(x)$。

- G' 仍是 PRG：因为随机输入命中 0^n 或 1^n 的概率可忽略。
- F' 不是 PRF：**敌手特意查询** $x_1 = 0^n, x_2 = 1^n$。

$$F'(k, 0^n) = F'(k, 1^n) = F(k, 0^{2n})$$

输出发生必定碰撞，而真随机函数碰撞概率极低。

期中试卷讲解 - Q5

Q5 (20 points)

已知 F 是一个安全的伪随机函数，请证明 $F'(k,x) = F(k,x) \oplus x$ 也是一个安全的伪随机函数.

期中试卷讲解 - Q5

使用反证法. 为叙述方便，我们使用 F'_k, F_k 分别代指 $F'(k,x), F(k,x)$. 假设存在多项式时间的敌手 A 能够区分 F'_k 和一个真正随机函数 f. 即，

$$|\Pr[A^{F'_k} = 1] - \Pr[A^f = 1]| > negl(n) \tag{1}$$

那么我们构造敌手 B 以区分 F_k 和真正随机函数 f. 敌手 B 具体算法如下：

- Input: Oracle $\mathcal{O}_B$
- Output: 0 或 1
- 模拟 Oracle $\mathcal{O}'_A$, 其中 $\mathcal{O}'_A(x) = \mathcal{O}_B(x) \oplus x$ 作为敌手 A 算法的输入
- 将 A 的运行结果 b 直接输出作为结果

期中试卷讲解 - Q5

此时我们有

$$\Pr[B^{F_k} = 1] = \Pr[A^{F'_k} = 1] \tag{2}$$

$$\Pr[B^{f} = 1] = \Pr[A^{f \oplus x} = 1] \tag{3}$$

由于 f 是真正的随机函数，f 和 $f \oplus x$ 的概率分布一致，我们有

$$\Pr[A^{f \oplus x} = 1] = \Pr[A^{f} = 1] \tag{4}$$

综合 (1)(2)(3)(4), 得到

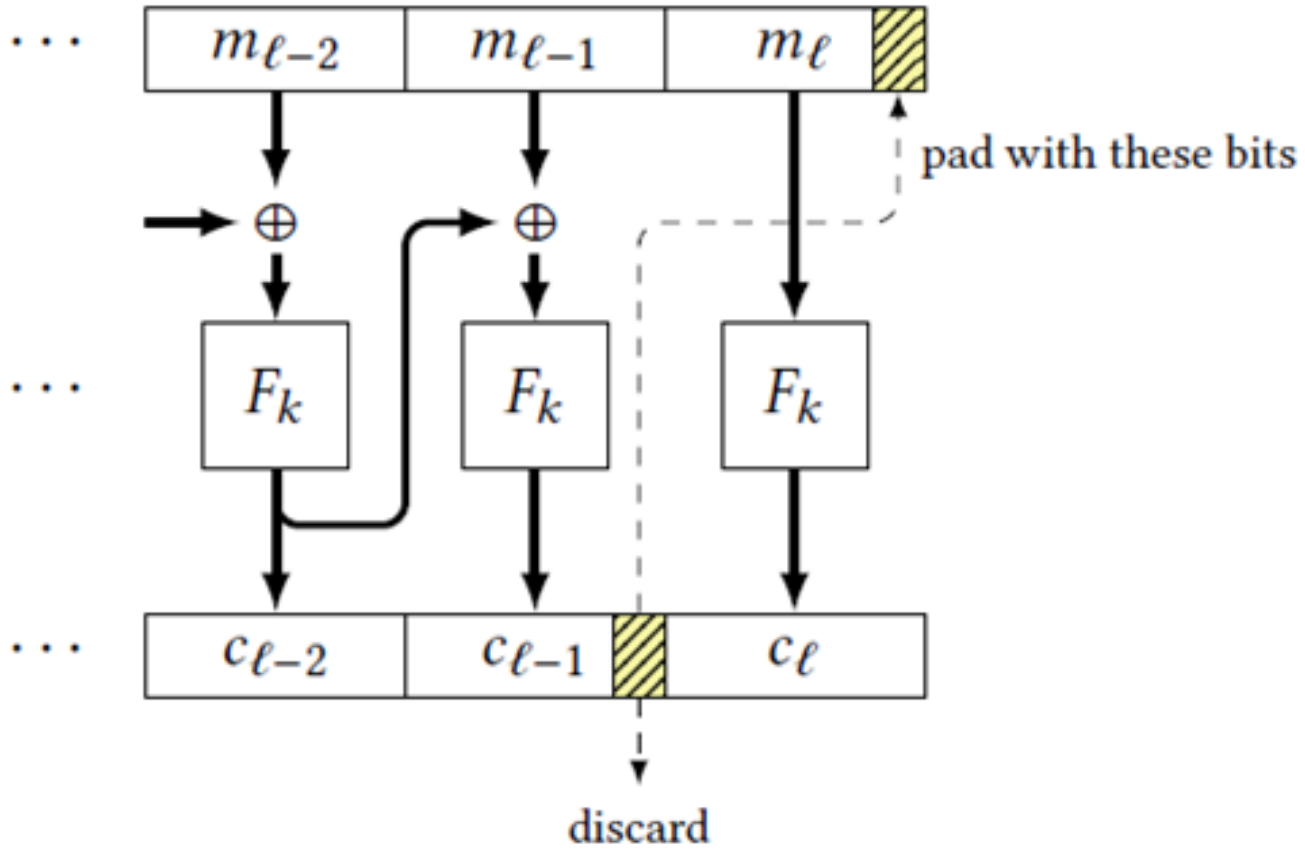
$$|\Pr[B^{F_k} = 1] - \Pr[B^{f} = 1]| > negl(n)$$

即得到了一个多项式时间可区分 F_k 与 f 的敌手，与题设矛盾. 故假设不成立，F'_k 是伪随机函数.

期中试卷讲解 - Q6

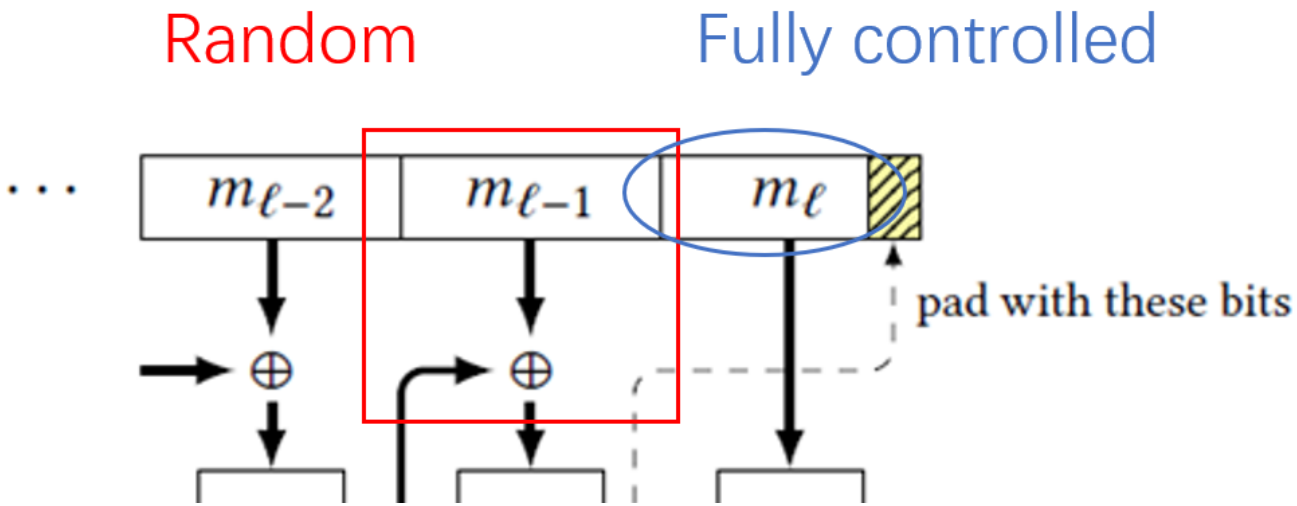
Q6 (20 points)

证明以下方案不是 CPA 安全的。给出一个攻击方案，并计算该方案在 CPA 不可区分实验中的具体获胜概率。(20 分)



期中试卷讲解 - Q6

直观的讲，CBC 模式之所以是安全的，是因为每一个 block 在输入 F_k 前都会和前一个 block 的密文进行异或，因此所有 bit 都具有随机性；而在本题的方案中，最后一个 block 的前半部分是可以被敌手完全控制的。虽然我们不能完全指定最后一个 F_k 的实际输入，但是可以通过多次查询，知道一个指定前缀的明文集合对应的密文集合。



期中试卷讲解 - Q6

我们设计一个敌手 $\mathcal{A}$ 如下：

$\mathcal{A}$ 随机选择两个长度为 $blen*(l-1)+blen-1$ 的 bit 串作为输入，记作 $M_0 = m_{01}||m_{02}||\cdots||m_{0l}$，$M_1 = m_{11}||m_{12}||\cdots||m_{1l}$，并保证 $m_{0l} \neq m_{1l}$，即最后一个长度为 $blen-1$ 的 block 不相等。挑战者挑选 $b \xleftarrow{\$} \{0,1\}$，因此最后一个 F_k 的实际输入只有两种情况，$m_{bl}||0$ 和 $m_{bl}||1$。

接下来 $\mathcal{A}$ 进行查询，每次查询时，保证最后一个 block 为 m_{0l}，前 $l-1$ 个 block 随机选择。记第一次查询时，最后一个 block 的输出为 c_{l0}。当 $\mathcal{A}$ 观察到最后一个 block 出现不等于 c_{l0} 的输出（记为 c_{l1}），或者查询次数达到 $q(n)$ 时，查询停止。

定义 $\mathcal{A}$ 收到的挑战者发回来的密文为 $c_1||c_2||\cdot||c_l$，

1. 若 $c_l = c_{l0}$，$\mathcal{A}$ 输出 0；
2. 若查询中找到了 c_{l1}，且 $c_l = c_{l1}$，$\mathcal{A}$ 输出 0；
3. 否则，$\mathcal{A}$ 输出 1.

期中试卷讲解 - Q6

一个示例如下，假设 $blen = 4$，m_0 的最后一个 block 为 000，m_1 的最后一个 block 为 001，那么查询时令最后一个 block 为 000，通过多次查询，我们有很大概率知道 $\{0000, 0001\}$ 对应的 F_k 的输出集合：

b	m_l	Probable Input	Probable Output
0	000	{0000,0001}	{1101,1000}
1	001	{0010,0011}	{1001,0110}

- If $c_l = 1101$ or $c_l = 1000$, output 0;
- Else output 1.

$$\Pr[PrivK^{CPA}_{\mathcal{A},\Pi} = 1] = \frac{1}{2}(\Pr[b' = b|b = 0] + \Pr[b' = b|b = 1])$$

$$= \frac{1}{2}(\Pr[c_l = c_{l0}]\Pr[b' = b|c_l = c_{l0}] + \Pr[c_l = c_{l1}]\Pr[b' = b|c_l = c_{l1}]) + \frac{1}{2}$$

$$= \frac{1}{2}(\frac{1}{2} \cdot 1 + \frac{1}{2}(1 - \frac{1}{2^{q(n)-1}})) + \frac{1}{2}$$

$$= 1 - \frac{1}{2^{q(n)+1}}$$

The End