No.

Date. / /

4.6

给定 $x=x'\|x''$，计算 $h(x)=f(x'\oplus x'')$

构造 $x^*=x''\|x'$，显然 $x^*\neq x$

但 $h(x^*)=f(x''\oplus x')=h(x)$

∴ h不是第二原像稳定的

4.7 $M=365$

$Q=15$ 时，准确值 $=1-\frac{364}{365}\times\frac{363}{365}\times\cdots\times\frac{365-15+1}{365}\approx 0.2529$

估计值 $=1-e^{\frac{-15\times(15-1)}{2\times365}}\approx 0.25$

∴ $\delta Q=0.0029$

$Q=16$ 时，准确值 $=1-\frac{364}{365}\times\frac{363}{365}\times\cdots\times\frac{365-16+1}{365}\approx 0.2836$

估计值 $=1-e^{\frac{-16\times(16-1)}{2\times365}}\approx 0.28$

∴ $\delta Q=0.0036$

...

$Q=30$ 时，准确值 $=1-\frac{364}{365}\times\frac{363}{365}\times\cdots\times\frac{365-30+1}{365}\approx 0.7063$

估计值 $=1-e^{\frac{-30\times(30-1)}{2\times365}}\approx 0.6963$

∴ $\delta Q=0.01$

∴ 可见，随着Q增加，估计值的误差在逐步增大

4.12

(a) 查询 $x=(x_1,x_2,\cdots,x_n)$，得到 $t=h_k(x)$

若 $x_1\neq x_2$，则构造 $x'=(x_2,x_1,\cdots,x_n)$

$h_k(x')=e_k(x_2)\oplus e_k(x_1)\oplus\cdots\oplus e_k(x_n)=t$ 且 $x'\neq x$

∴ (x',t) 是一个有效的伪造

∴ 这是1个(1,1)假冒者

No.
Date. / /

(b) ① 若 $x_1, \cdots, x_n$ 中至少2个不同(假设 x_1 为不一样的那个)

则与(a)同理可构造 $(x_2, x_1, \cdots, x_n)$ 与 $(x_2, x_2, x_1, \cdots, x_n)$

∴为(1,2)假混淆

② 若 $x_1 = x_2 = \cdots = x_n$

1、若n为偶数，则 $h_k(x_1, x_2, \cdots, x_n) = 0$

则任意n为偶数且 $x_1 = x_2 = \cdots = x_n$ 的均满足条件

∴可达到(1,2)假混淆

2、若n为奇数，则 $h_k(x_1, \cdots, x_n) = e_k(x)$

则将 $x_1, \cdots, x_n$ 中任意偶数个替换为y时，因偶数个 $e_k(y)$ 进行异或仍为0

∴ $h_k(\underbrace{y, \cdots, y}_{2k个}, x_{2k+1}, \cdots, x_n)$ 的排列均为 $e_k(x)$

∴可达到(1,2)假混淆

∴综上，可达到(1,2)假混淆，对任一消息。