现代密码学. (4) Hash

4.6.

证明: 取 $x_1 \in \{0,1\}^{2m}$. ~~$x_1 \neq x_2$~~. $h(x_1) = f(x_1' \oplus x_1'')$

即证: $\exists\, x_2 \in \{0,1\}^{2m}$, $x_2 \neq x_1$. $x_2' \oplus x_2'' = x_1' \oplus x_1'' \Rightarrow h(x_1) = h(x_2)$.

~~令 $y = x_1' \oplus x_1''$~~ 令 $x_2' = \neg x_1'$. $x_2'' = \neg x_1''$

$x_2' \oplus x_2'' = (\neg x_1') \oplus (\neg x_1'') = x_1' \oplus x_1''$. 得证.

4.7 $M = 365$. $15 \le q \le 30$.

	$\epsilon = 1 - \frac{C_M^q}{M^q}$ 确	$\epsilon = 1 - e^{\frac{-q(q-1)}{2M}}$ 估计值
q=15	0.252901	0.249992
16	0.283604	0.280189
17	0.315008	0.311061
18	0.346911	0.342413
19	0.379119	0.374055
20	0.411438	0.405805
21	0.443688	0.437488
22	0.475695	0.468938
23	0.507297	0.500002
24	0.538344	0.530536
25	0.5687	0.560412
26	0.598241	0.589513
27	0.626859	0.617736
28	0.654461	0.644993
29	0.680969	0.671208
30	0.706316	0.69632

4.12.

(a) $Q=1$ $\epsilon=1$

设已知 $h_K(x_1.x_2 \dots x_n) = e_K(x_1) \oplus \dots \oplus (x_n)$

则可知 $h_K(x_2.x_1 \dots x_n) = e_K(x_2) \oplus e_K(x_1) \oplus \dots \oplus e_K(x_n) = h_K(x_1.x_2 \dots x_n)$

得证.

(b) $Q=2$ $\epsilon=1$

若 $x_1 \dots x_n$ 不全相等. 由同(1)理 $\Rightarrow$ $h(x) = e_K(x_1)$. $h(x') = e_K(x_2)$ 可得到 x_1 x_2 任意组合的MAC.

若 $x_1 = x_2 = \dots = x_n$. $\begin{cases} n奇. & h(x_1 \dots x_n) = e_K(x_1) \\ n偶 & h(x_1 \dots x_n) = 0 \end{cases}$ $\Rightarrow$ $h(x) = 0$ $h(x') = 0$ 可得到偶数个 x_1 与偶数个 x_j 组合而成的MAC. $h(x_1 \dots x_j' \dots) = 0$