现代密码学第四次作业

2050249 徐正扬

2024 年 6 月 23 日

4.6 假定 $f:\{0,1\}^m \to \{0,1\}^m$ 是一个原像稳固的双射。定义 $h:\{0,1\}^{2m} \to \{0,1\}^m$ 如下：给定 $x \in \{0,1\}^{2m}$，记

$$x = x' \parallel x''$$

其中 $x', x'' \in \{0,1\}^m$，然后定义

$$h(x) = f(x' \oplus x'')$$

证明：h 不是第二原像稳固的。

证明. 取 $x_1 = x' \parallel x'', x_2 = x' \oplus 1 \parallel x'' \oplus 1$，显然 $x_1, x_2 \in \{0,1\}^{2m}$ 且 $x_1 \neq x_2$。
容易发现 $x' \oplus x'' = x' \oplus 1 \oplus x'' \oplus 1$，即 $h(x_1) = h(x_2)$。
因此，h 不是第二原像稳固的。 □

4.7 对 $M = 365$，$15 \leqslant q \leqslant 30$，比较定理 4.4 公式中给出的 ϵ 的准确值和定理证明后推导的对 ϵ 的估计值。

准确值计算公式为

$$\epsilon = 1 - \prod_{i=1}^{q-1} \frac{M-i}{M}$$

估计值计算公式为

$$\epsilon = 1 - e^{\frac{-Q(Q-1)}{M}}$$

计算结果如下：

q	准确值	估计值	q	准确值	估计值
15	0.252901	0.249992	23	0.507297	0.500002
16	0.283604	0.280189	24	0.538344	0.530536
17	0.315008	0.311061	25	0.5687	0.560412
18	0.346911	0.342413	26	0.598241	0.589513
19	0.379119	0.374055	27	0.626859	0.617736
20	0.411438	0.405805	28	0.654461	0.644993
21	0.443688	0.437488	29	0.680969	0.671208
22	0.475695	0.468938	30	0.706316	0.69632

4.12 假定 $(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$ 是一个内嵌式密码体制，其中 $\mathcal{P}=\mathcal{C}=\{0,1\}^m$。令 $n\geqslant 2$ 是一个整数，定义 Hash 函数族 $(\mathcal{X},\mathcal{Y},\mathcal{K},\mathcal{H})$ 如下 $(\mathcal{X}=(\{0,1\}^m)^n,\mathcal{Y}=\{0,1\}^m)$:

$$h_K(x_1,\cdots,x_n)=e_K(x_1)\oplus\cdots\oplus e_K(x_n)$$

按如下方式证明 $(\mathcal{X},\mathcal{Y},\mathcal{K},\mathcal{H})$ 不是一个安全的消息认证码:

1. 证明该 Hash 函数族存在一个 $(1,1)$ 假冒者。
2. 证明该 Hash 函数族存在一个 $(1,2)$ 假冒者: 对任意的消息 $(x_1,\cdots,x_n)$，均可伪造 MAC(这种伪造被称为选择假冒: 这些假冒在前面被考虑为存在假冒的例子)。注意，当 $x_1=\cdots=x_n$, 时情况较复杂。

证明. 1. 若 $x_i, i\in[1,n]$ 不全相同，不妨设其中两个不相同的元素为 x_1,x_2，通过一个已知的请求得到 $(x_1,\cdots,x_n)$ 和 $h_K(x_1,\cdots,x_n)$, 可以构造一个 $(x_2,x_1,\cdots,x_n)$ 和 $h_K(x_2,x_1,\cdots,x_n)=h_K(x_1,\cdots,x_n)$, 这是因为 $e_K(x_1)\oplus e_K(x_2)=e_K(x_2)\oplus e_K(x_1)$。因此该 Hash 函数族存在一个 $(1,1)$ 假冒者。

2. (a) 先讨论 $x_1=\cdots=x_n$ 的情况，假设通过一个请求得到 $(x_1,\cdots,x_n)$ 和 $h_K(x_1,\cdots,x_n)$，我们任意改变两个 $x_i=y,x_j=y$，此时 $h_K(x_2,x_1,\cdots,x_n)$ 的值保持不变，直接构造即可。

   (b) 否则，同第 1 小问中任意找到两对不相同的元素，交换位置构造即可。

□

5.10 假定 $n=pq$，其中 p 和 q 为不同的奇素数，且 $ab\equiv 1 \mod (p-1)(q-1)$。RSA 加密运算是 $e(x)\equiv x^b \mod n$ 且解密运算为 $d(y)\equiv y^a \mod n$。我们已证明 $d(e(x))=x$ 对于 $x\in\mathbb{Z}_n^*$ 成立。现在证明这个断言对于任一 $x\in\mathbb{Z}_n$, 都成立。
提示: 利用如下事实:$x_1\equiv x_2 \mod pq$ 当且仅当 $x_1\equiv x_2 \mod p$ 且 $x_1\equiv x_2 \mod q$ 这可以由中国剩余定理得出。

证明. 下证 $x^{ab}\equiv x \mod n$ 对于任一 $x\in\mathbb{Z}_n$ 成立。
首先，若 $(x,p)=1$，由 Fermat 小定理得到 $x^{p-1}\equiv 1 \mod p$，得到 $x^{ab-1}\equiv x^{(p-1)(q-1)}\equiv 1 \mod p$。即 $x^{ab}\equiv x \mod p$。若 $p\mid x$，那么 $x^{ab-1}\equiv 0\equiv x \mod p$。所以 $\forall x\in\mathbb{Z}_n$ 均有 $x^{ab}\equiv x \mod p$。
同理，$\forall x\in\mathbb{Z}_n$ 均有 $x^{ab}\equiv x \mod q$。由提示，原命题得证! □

5.14 证明 RSA 密码体制对于选择密文攻击是不安全的。特别地，给定密文 y，描述如何选择密文 $\hat{y}\neq y$，使得根据明文 $\hat{x}=d_K(\hat{y})$ 可以计算出 $x=d(y)$。
提示: 使用 RSA 密码体制的乘法性质，即 $e_K(x_1)e_K(x_2) \mod n\equiv e_K(x_1x_2) \mod n$。

证明. 随机选择整数 $r\in\mathbb{Z}_n^*$，选择密文 $\hat{y}=ry \mod n$，那么 $\hat{x}=d_K(\hat{y})=d_K(e_K(rx))\equiv rx \mod n$ □

5.34 证明与函数 half 和 parity 相关的等式 (5.3) 和 (5.4)

1. $half(y)=parity(y\times e_K(2) \mod n)$
2. $parity(y)=half(y\times e_K(2^{-1}) \mod n)$

证明. 1. 默认 $2\nmid n$ 的情况下，$parity(y\times e_K(2) \mod n)=parity(e_K(2x) \mod n)$。
那么显然当 $0\leqslant x<\dfrac{n}{2}$ 时 $half(y)=parity(e_K(2x) \mod n)=0$。
当 $\dfrac{n}{2}<x\leqslant n-1$ 时 $half(y)=parity(e_K(2x) \mod n)=1$。

2. 当 $2 \mid x$ 时，$half(y \times e_K(2^{-1}) \mod n) = half(e_K(\frac{x}{2}) \mod n)$。
   注意到 $x \leqslant n-1$，那么 $\frac{n}{2} > \frac{x}{2} \in \mathbb{Z}_n$，因此有 $parity(y) = half(e_K(\frac{x}{2}) \mod n) = 0$。
   当 $2 \nmid x$ 时，$\frac{n}{2} < \frac{x+n}{2} \in \mathbb{Z}_n$，因此有 $parity(y) = half(e_K(\frac{x}{2}) \mod n) = 1$。

□

E6.1 ：对 $\mathbb{Z}_P^*$ 上的 ElGamal 公钥加密体制做如下变形:
公钥 α, β, p，私钥 a 如 ElGamal 体制所定义，加密如下定义:
选取随机数 $x \in \mathbb{Z}_P^*$，

$$e_K(x,k) = (y_1, y_2)$$

其中

$$y_1 = \alpha^k \mod p$$

且

$$y_2 = x + \beta^k \mod p$$

要求:

1. 给出解密运算
2. 课本中已证明 ElGamal 体制具有如下结论: 任何解 CDH 的算法，都可以用于解密密文，反之亦然。请证明该结论对以上所定义的加密体制同样成立。

证明. 1. 解密运算为 $x = y_2 - y_1^a \mod p$

2. (a) 假设有 CDH 算法已知 g, g^a, g^b 能求出 g^{ab}
   将 $\alpha, y_1 = \alpha^k \mod p, \beta = \alpha^a \mod p$ 带入得到 α^{ka}, 那么计算 $x = y_2 - \alpha^{ka} \mod p$ 即可解密
   (b) 假设有算法已知密文 (y_1, y_2) 和公钥 (α, β, p) 能够解出明文 x
   也就是说已知 $\alpha, y_1 = \alpha^k \mod p, \beta = \alpha^a \mod p$ 时能够求解出 x, 这等价于求解出 $\beta^k = \alpha^{ka}$, 也即求解了 CDH 算法.

□

E6.2 设在 ElGamal 密码体制中，私钥 $a \in \mathbb{Z}_{p-1}$，公钥为 (p, α, β)，其中 p 为素数，α 为模 p 本原元，$\beta = \alpha^a \mod p$。如果加密运算中泄露了随机数 k，会带来什么安全问题?

1. 注意到 $y_2 = x\beta^k \mod p$, 在已知 β, k, p, y_2 的情况下可以解出 x, 也即消息泄露.
2. 已知 k 的情况下, 可以通过离散对数问题的算法可以计算出私钥 a
3. 此外还可以伪造签名

E7.1 RSA' 签名方案如下: 公钥 (n, b)，其中 $n = pq$，p 和 q 为素数，$b \in \mathbb{Z}_n$。私钥 $a \in \mathbb{Z}_n$，满足

$$ab = 1 \mod (p-1)(q-1)$$

签名算法 (x): 对消息 $x \in \mathbb{Z}_n$ 计算

$$y = x^{2a} \mod n$$

验证算法 (x, y): 如果 $x^2 = y^b \mod n$，则输出 true，否则输出 false.
请给出 RSA' 签名算法的一个安全分析，并指出是哪种类型的分析 (如已知消息攻击的存在性伪造)

这里给出一个已知消息攻击的存在性伪造. 对于任意消息 $x \in \mathbb{Z}_n$, 伪造明文 $x' = n - x$ 和密文 $y' = y$ 注意到

$$y = x^{2a} \equiv (n-x)^{2a} \mod n$$

, 而且

$$(x')^2 = (n-x)^2 \equiv x^2 \equiv y^b \mod n$$

因此攻击者可以伪造一个 (x', y') 签名.