HomeWork4

120L020614-刘昕烨

Problem 1：

由题意我们可以知道F_k:$\{0,1\}^n \to \{0,1\}^n$，及函数 F 的输入与输出位数相同。我们构造如下的攻击者$\mathcal{A}$来攻击此 MAC:

攻击者先询问数据库长度为 2n 的串$m_1||m_1$，得到 tag：$\langle F_k(m_1), F_k(F_k(m_1))\rangle$。接着伪造输入为$F_k(m_1)||m_1$的 tag 为$\langle F_k(F_k(m_1)), F_k(F_k(m_1))\rangle$并将其输出。其成功的概率为：

$Pr[Macforge_{\mathcal{A},\Pi}(2n)=1 \,|m_1 \neq F_k(m_1)] \cdot X + Pr[Macforge_{\mathcal{A},\Pi}(2n)=1 \,|m_1 = F_k(m_1)] \cdot \bar{X}$

其中$X = Pr[m_1 \neq F_k(m_1)]$。由于后一项我们无法知道其概率大小但是其一定大于等于 0，所以我们取前面的一项，成功的概率肯定大于它。

由于当$m_1 \neq F_k(m_1)$时伪造成功的概率为 1。所以伪造成功的概率大于：$1 \cdot Pr[m_1 \neq F_k(m_1)] = 1 - negl(n)$，所以$Pr[Macforge_{\mathcal{A},\Pi}(2n)=1] > negl(n)$。所以此 MAC 不具有在适应性 CMA 下的存在性不可伪造性，是不安全的。

Problem 2：

证明:

我们对其进行规约，假设我们有对$\hat{H}$的攻击者$\mathcal{A}$，我们利用$\mathcal{A}$构造攻击者D来攻击$\mathcal{H}$，则D能成功破解$\mathcal{H}$当且当$\mathcal{A}$能成功实现对$\hat{H}$的攻击。

首先D收到生成的哈希函数的 key s，接着将其输入到攻击者$\mathcal{A}$中，$\mathcal{A}$会输出两个不同的输出满足：$H^s(H^s(x_1)) = H^s(H^s(x_2)), x_1 \neq x_2$。由于给定 key 的哈希函数是确定，所以函数给定相同的输入时输出相同。我们构造D的输出如下：

1. 若$H^s(x_1) = H^s(x_2)$那么我们直接输出x_1, x_2即可满足。
2. 若$H^s(x_1) \neq H^s(x_2)$那么我们输出$H^s(x_1), H^s(x_2)$即可满足。

假设$\mathcal{H}$是防碰撞的哈希函数我们可以得到$Pr[Hashcoll_{D,\Pi}(n)=1] \leq negl(n)$，所以我

们的对$\hat{H}$攻击满足：$Pr\left[Hashcoll_{\mathcal{A},\hat{\Pi}}(n)=1\right]\leq negl(n)$，所以我们可以得到$\hat{H}$也是防碰撞的。

■

Problem 3：

1. 不是防碰撞的。例如：假设h^s的输入长度为 n，我们构造长为 n+1 的串$x||0$，以及一个长为 n+2 的串$x||00$。由于我们构造的新 transform 无需使用长度我们得到二者的结果均为：$h^s(h^s(IV||x)||0^n)$，所以其不是防碰撞的哈希函数。
2. 是防碰撞的，证明如下：

   由于其最后一个块的输出为$z_B||L$，所以如果两个输入的长度不同最终得到的结果肯定不同，无法发生碰撞。

   所以我们只需要证明输入长度相同下的不同输入的碰撞即可，此时碰撞只可能发生在前 B 个块，我们假设这种情况出现：

   那么从后向前分析：

   1. $x_B\neq x'_B\ or\ z_{B-1}\neq z'_{B-1}$，此时第 B 个块发生碰撞。
   2. $x_B=x'_B\ and\ z_{B-1}=z'_{B-1}$此时碰撞发生于前 B-1 个块。

   由于$IV=IV'\ and\ x\neq x'$所以按照这样的推导，肯定会在某个前 B 个块发生碰撞，而我们根据 h 是防碰撞的得出这不可能，所以存在矛盾，即假设错误，碰撞不会发生。

   ■

3. 是防碰撞的，与上面的证明类似只简述不同：

   证明：

   首先这种情况下如果长度不同，我们可以得到两个输入的最后一块 h 的输入$z_B||L$是不同的，所以此时最后一块发生了碰撞，但是这在 h 是防碰撞时是不可能的。

   当长度相同时，与上面的证明相同，只不过若一直推到碰撞发生在第一个块时我们可以得到$x_1\neq x'_1$（因为之前的块中满足$x_i=x'_i\ and\ z_{i-1}=z'_{i-1}$）且$z_1=z'_1$而我们知道这是不可能的因为$z_1=x_1$，所以碰撞不可能发生。

因此在这种 transform 下碰撞不可能发生。

■

4. 不是防碰撞的，假设我们构造如下的单向函数，假设$g:\{0,1\}^{2n}\to\{0,1\}^{n-1}$且 g 是防碰撞的单向函数。根据提示的思想构造一个新的单向函数$h:\{0,1\}^{2n}\to\{0,1\}^{n}$:

$$h(x)=\begin{cases} l & x=(2n)_2||x_1 \\ g(x)||0 & else \end{cases} \qquad x\in\{0,1\}^{2n} \tag{1.1}$$

其中l为表示 n 这个数的二进制串，其且长度为 n（不满 n 在前面补零），上面的条件是当 x 等于表示 2n 的数的二进制串（其长度为 n，构造方法同上）与长为 n 的一个串x_1连接。

此时我们构造两个输入使其碰撞：$x_1||x_2,x_2$。其中$x_1,x_2\in\{0,1\}^n$。当输入$x_1||x_2$时首先第一个块中输入为$(2n)_2||x_1$（前面为附加的 L）所以输出为$z_1=l$，与第二个块的输入x_2综合得出结果为$g(x_2)||0$。同样的我们可以得到输入x_2时结果为：$g(x_2)||0$发生碰撞，所以其不是防碰撞的。

总结一下其构造思想是根据防碰撞哈希函数的性质构造一个新的哈希函数。两个长度相差 1 个块的大小，及$len(m)-len(m')=n$，但是除第一部分外二者组成相同的输入值输入哈希函数，会因为构造的原因导致$z_1=len(m')=z_0'$，因此输出相同，所以其不防碰撞。

■

Problem 4:

（1）我认为其是 CCA 安全的：

证明：

我们证明它通过将其归约到证明强伪随机置换与随机置换不可区分上，假设我们构造攻击者$\mathcal{A}$攻击此加密策略，同时利用它构造攻击者$\mathcal{D}$来攻击强伪随机置换。

开始输入加密与解密函数$\mathcal{O},\mathcal{O}^{-1}$其可能是强伪随机置换也可能是随机置换，我们用它来回答$\mathcal{A}$的询问，我们有：

$$Pr[PrivK^{cca}_{\mathcal{A},\Pi}(n)=1]=Pr[D^{F_k(\cdot),F_k^{-1}(\cdot)}(n)=1]=\varepsilon(n)+\frac{1}{2} \tag{1.2}$$

我们接下来分析当输入的加密函数为随机置换函数时发生的情况：

首先攻击者会向加密数据库与解密数据库询问得到原文与密文对，这里我们假设其采取最优的策略及尽量得到与m_1,m_2相关的明文密文对来便于攻击。、

首先分析向加密数据库分析的情况：在 D 发送密文前后我们都只进行m_1,m_2的询问并将结果的密文与对应的 m 存储于 E 中，容易知道其询问数量必然是多项式次用$q(n)$次表示，最佳情况每次加密用的随机串 r 均不同，一般情况下满足：$|E|\leq q(n)$。

接着我们分析对解密数据库的询问，此时因为无论在 D 发送密文前还是后，无论询问什么密文得到的明文都是随机的，所以我们只能随机进行询问期望得到与m_1,m_2相关的信息，同样的此时询问了多项式$x(n)$次。此时由于是伪随机置换，用不同密文得到的明文信息必然是不同的，将得到的明文中与m_1,m_2相关的、对应的明文密文对存储于 H 中，最佳情况询问得到的明文均是与m_1,m_2相关的，所以有$|H|\leq x(n)$，

接下来我们分析两个集合组合起来可以得到多少与m_1,m_2相关的明文密文对：假设最不可能的情况我们有两个集合中的元素没有一个相同，那么我们有将两个集合做加法操作后得到的集合 K 有$|K|\leq x(n)+q(n)$。我们用集合 K 的信息回答质询c，假设 c 对应的明文为m_n可以得到：

$$\begin{aligned}Pr[PrivK^{cca}_{\mathcal{A},\Pi'}(n)=1]&=Pr[PrivK^{cca}_{\mathcal{A},\Pi'}(n)=1\,|\,(c,m_n)\in K]+Pr[PrivK^{cca}_{\mathcal{A},\Pi'}(n)=1\,|\,(c,m_n)\notin K]\\&\leq 1\cdot\frac{x(n)+q(n)}{2^{\frac{n}{2}+1}}+\frac{1}{2}\cdot\left(1-\frac{x(n)+q(n)}{2^{\frac{n}{2}+1}}\right)\\&<\frac{1}{2}+\frac{x(n)+q(n)}{2^{\frac{n}{2}+1}}=\frac{1}{2}+negl(n)\end{aligned}$$

这里当(c,x_n)不在 K 中时由于随机置换的定义我们知道其成功的概率为 1/2。所以我们有：

$$Pr[PrivK^{cca}_{\mathcal{A},\Pi'}(n)=1]=Pr[D^{f_k(\cdot),f_k^{-1}(\cdot)}(n)=1]=\frac{1}{2}+negl(n) \tag{1.3}$$

结合上面的式子（1.2）我们知道：

$$Pr(D^{F_k(\cdot),F_k^{-1}(\cdot)}(n)=1)-Pr[D^{f_k(\cdot),f_k^{-1}(\cdot)}(n)=1]=\varepsilon(n)-negl(n) \tag{1.4}$$

而由于 F 为强伪随机置换所以我们有$Pr[PrivK^{cca}_{\mathcal{A},\Pi}(n)=1]=\frac{1}{2}+\varepsilon(n)=\frac{1}{2}+negl(n)$

因此此加密方案满足 CCA 安全

■

（2）我不认为 CCA 安全就可以得出其实现了认证通信，我们以第一问的加密方案为例，由于其使用了强伪随机置换，所以我们向Dec_k输入的任何密文均会被解密且均有意义，不会输出$\perp$。所以我只需要输出任意的一个密文，其均有有意义的明文与其对应。因此满足：$Pr[Auth_{\mathcal{A},\Pi}(n)=1]=1>negl(n)$。所以其不满足认证通信，但由第一问可知其满足了 CCA 安全。

Problem 5：

我们利用安全的 MAC$\langle Mac,Vrfy\rangle$构造这样的数据传输策略：

$$\begin{cases} EncMac_k(m)=(Mac_k(m),m) \\ Dec_k(c_1,c_2)=\begin{cases} c_2 & Vrfy_k(c_2,c_1) \\ \perp & otherwise \end{cases} \end{cases} \tag{1.5}$$

我们用规约的方法证明其实现了认证通信：

首先我们还是假设攻击者$\mathcal{A}$攻击我们的认证通信，我们利用它构造攻击者$\mathcal{D}$来攻击 MAC，$\mathcal{D}$得到Mac_k的访问权，并且将$\mathcal{A}$的询问数据$(m_1,m_2,m_3,\cdots,m_n)$输入Mac_k得到输出后返回：

$((Mac_k(m_1),m_1),\cdots,(Mac_k(m_n),m_n))$，并且将$\mathcal{A}$的输出$(Mac_k(m_0),m_0)\quad m_0\notin\{m_1,\ldots,m_n\}$中的$Mac_k(m_0)$返回。

我们可以得到：

$$Pr[Auth_{\mathcal{A},\Pi}(n)=1]=Pr[Macforge_{\mathcal{A},\Pi}(n)=1] \tag{1.6}$$

所以我们的方法实现了认证通信，但是其将明文暴露了出来明显其不是 CCA 安全的。