

随机消息伪造攻击 PMAC 和 TMAC-V

陈 杰¹⁾ 胡予濮¹⁾ 韦永壮^{1),2)}

¹⁾(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)

²⁾(桂林电子工业大学通信与信息工程学院 广西 桂林 541004)

摘 要 消息认证码(MAC)是与密钥相关的单向 Hash 函数,不同的密钥会产生不同的 Hash 函数.因此接收者能在验证发送者的消息是否被篡改的同时,验证消息是由谁发送的. PMAC 是由 Black 和 Rogaway 在 2002 年欧密会上提出的一种基于分组密码的可并行工作的 MAC. 2005 年 Mitchell 在 TMAC 的基础上进行了改进提出了 TMAC-V. 文章利用模式的局部差分恒等原理,针对 PMAC 和 TMAC-V 两种工作模式,给出一种新的随机消息伪造攻击.该攻击可对随机消息的 PMAC 和 TMAC-V 进行伪造,伪造的成功概率均为 86.5%,高于已有分析结果的概率 63%.新方法对 PMAC 输出没有截断时的攻击复杂度为 $[0, 2^{n/2+1}, 1, 0]$, PMAC 输出有截断时的攻击复杂度为 $[0, 2^{n/2+1}, \lceil n/\tau \rceil, 2^{n-\tau}]$;对 TMAC-V 的伪造攻击复杂度为 $[0, 2^{n/2+1}, 1, 0]$.

关键词 消息认证码;分组密码;工作模式;伪造攻击;生日碰撞

中图法分类号 TN918

Forgery Attack on PMAC and TMAC-V with Random Message

CHEN Jie¹⁾ HU Yu-Pu¹⁾ WEI Yong-Zhuang^{1),2)}

¹⁾(Key Laboratory of Computer Networks & Information Security of Ministry of Education, Xidian University, Xi'an 710071)

²⁾(School of Information and Communication, Guilin University of Electronic Technology, Guilin, Guangxi 541004)

Abstract A Message Authentication Code (MAC) is a hash function with secret key, which satisfies that different keys can induce different hash functions. Therefore, receiver can verify whether the message is forged from sender. At the same time, receiver can also verify who send the message. PMAC, a fully parallelizable MAC scheme based on block cipher, is proposed by Black and Rogaway in Eurocrypt 2002. In 2005, Mitchell presented TMAC-V to improve the security of TMAC. This paper presents a new forgery attack on PMAC and TMAC-V with random message, which make use of the principle of differential identical in part of the mode. The new attack can forge the PMAC and TMAC-V of random message, with a probability of 86.5% higher than 63% in the known reference. The complexity of this new attack is $[0, 2^{n/2+1}, 1, 0]$ for PMAC where no truncation is performed. For PMAC where truncation is performed, the complexity of this attack is $[0, 2^{n/2+1}, \lceil n/\tau \rceil, 2^{n-\tau}]$. And the complexity of this attack is $[0, 2^{n/2+1}, 1, 0]$ for TMAC-V.

Keywords message authentication code; block cipher; mode of operation; forgery attack; birthday collision

收稿日期:2007-05-08;修改稿收到日期:2007-07-23. 本课题得到国家自然科学基金(60673072)、国家“八六三”高技术研究发展计划项目基金(2007AA01Z435)和陕西省自然科学基金基础研究计划项目基金(2007F37)资助. 陈 杰,女,1979 年生,博士研究生,主要研究方向为分组密码的设计与安全性分析. E-mail: jchen@mail. xidian. edu. cn. 胡予濮,男,1955 年生,博士,教授,博士生导师,主要研究领域为密码学与信息安全. 韦永壮,男,1976 年生,博士研究生,主要研究方向为密码函数与分组密码分析.

1 引言

1974 年, Gilbert 等人首次提出了认证码^[1]的概念, 并用有限几何构造了认证码; 20 世纪 80 年代, Simmons 等人系统地发展了认证码的理论^[2-4].

假设 M 是发送方 A 要发送的消息, K 是发送方 A 和接收方 B 共有的密钥, A 首先计算 $MAC = C_K(M)$, 其中 $C_K(\cdot)$ 是密钥控制的公开函数, 然后 A 将要发送的消息 M 和验证码 MAC 一起发送给 B , B 收到后与 A 作相同的计算, 求得一个新 MAC , 并与收到的 MAC 进行比较.

如果仅 A, B 知道 K , 且 B 计算得到的 MAC 与收到的 MAC 一致, 则这一系统就实现了以下功能:

(1) B 相信 A 发送的消息 M 未被篡改. 这是因为攻击者如果不知道密钥, 就不能够在篡改消息后再相应地篡改 MAC ; 而如果仅篡改消息, 则 B 计算的新 MAC 就与收到的 MAC 不同.

(2) B 相信 A 不是冒充的. 这是因为除 A, B 双方外再无其他人知道密钥, 因此其他人不可能对 A 发送的消息 M 计算出正确的 MAC .

上述过程中, 由于消息 M 本身在发送过程中是明文形式, 所以这一过程只提供认证性而未提供保密性. 为提供保密性, 可在 MAC 函数之后或之前进行一次加密, 而且加密密钥需要被收发双方共享.

分组密码的工作模式是以分组密码算法为基础来解决实际问题的方案, 它包括保密模式、认证模式和认证保密模式. 认证模式是基于分组密码构造 MAC , 基于分组密码构建各种 MAC 也成为近年来分组密码研究的热点之一.

CBC-MAC 工作模式^[5] 是基于分组密码构造 MAC 的典型代表之一. 基于 DES 的 CBC-MAC 是最早出现的, 先后被包含在许多标准文件中, 比如 FIPS Pub. 81 (US Federal Standard)、ANSI X9.19 (US Banking Standard)、ISO 8730、ISO 9807 和 ISO/IEC 9797-1. 由于 CBC-MAC 工作模式是基于 CBC 串联模式工作, 2002 年 Black 等人在文献^[6]中提出了一种新的并行工作模式即 PMAC. 2003 年, Kurosawa 等人在 CBC-MAC 工作模式和 XCBC^[7]的基础上提出了 TMAC^[8]; 此后 Mitchell 等人又提出了变形的 TMAC 工作模式^[9], 这里称为 TMAC-V.

2006 年, Lee 等人在文献^[10]中对固定消息的 PMAC 和 TMAC-V 进行了伪造攻击. 由于该攻击是针对固定消息, 局限性较大. 本文利用模式的局部

差分恒等原理, 针对 PMAC 和 TMAC-V 两种工作模式, 给出一种新的攻击方法——随机消息伪造攻击. 该攻击可对随机消息进行伪造, 伪造的成功概率为 86.5%, 高于文献^[10]中的成功概率 63%. 对 PMAC 输出无截断的攻击复杂度为 $[0, 2^{n/2+1}, 1, 0]$, 输出有截断的攻击复杂度为 $[0, 2^{n/2+1}, \lceil n/\tau \rceil, 2^{n-\tau}]$; 对 TMAC-V 的攻击复杂度为 $[0, 2^{n/2+1}, 1, 0]$.

本文第 2 节简单介绍 PMAC 和 TMAC-V 的结构; 第 3 节给出一种新的随机消息伪造攻击 PMAC; 第 4 节给出一种新的随机消息伪造攻击 TMAC-V; 最后给出本文的分析结果和已有结果的比较分析列表.

2 PMAC 和 TMAC-V 的结构介绍

随着通信中硬件设备的快速发展, 串联的工作模式已经成为网络通信中的瓶颈. 2002 年, Black 等人在欧密会上提出了一种可并行工作的工作模式 PMAC^[6]. 我们用 $E_k(\cdot)$ 表示一个分组密码算法, $E_k(x)$ 表示用密钥 k 加密明文 x , 分组密码算法明文长度为 n . 消息 M 填充至分组长度 n 的整数倍, 例如 rn 长, M 可以拆分为 $M[1], M[2], \dots, M[r]$, 共有 r 个 n 长的分组. PMAC 算法是将输入消息 M , 经过并行运算输出长度为 τ 的 tag. 其工作模式如算法 1 所示.

算法 1.

1. 用密钥 k 加密长度为 n 的全零序列 0^n , 并将值赋给 L : $L = E_k(0^n)$.
2. 如果消息 M 的长度大于 $n2^n$, 即 $|M| > n2^n$, 则返回长度为 τ 的全零序列 0^τ .
3. 将消息 M 按长度 n 进行分拆. 若分拆为 r 个块 $M[1], \dots, M[r]$, 其中前 $r-1$ 块长度均为 n .
4. 对于 $i=1$ 到 $i=r-1$ 做如下操作:
 - 4.1. $X[i] = M[i] \oplus \gamma_i \cdot L$, 其中 γ_i 为 Gray 码, 乘法运算都是定义在有限域 $GF(2^n)$ 上.
 - 4.2. $Y[i] = E_k(M[i])$.
 - 4.3. $\sum = Y[1] \oplus \dots \oplus Y[r-1] \oplus padding(M[r])$, 其中 $padding(M[r])$ 表示: 当 $|M[r]| < n$ 时, 在 $M[r]$ 后填充 1 个“1”和 $n - |M[r]| - 1$ 个“0”, 其值为 $M[r] \parallel 10^{n-|M[r]|-1}$; 当 $|M[r]| = n$ 时, $padding(M[r]) = M[r]$.
5. 如果第 r 块分组长度为 n , 即 $|M[r]| = n$, 则定义 $X[r] = \sum \oplus L \cdot x^{-1}$; 否则将 \sum 的值赋给 $X[r]$, 即 $X[r] = \sum$.
6. 定义 MAC 值是: $X[r]$ 由密钥为 k 的分组密码算法加密后输出的前 τ 比特. 当 $\tau < n$ 时, 输出有截断.

7. 输出 MAC 值.

2003 年, Kurosawa 对 XCBC 算法^[7]进行了改进, 提出 TMAC 算法^[8]. XCBC 共需要 $(k+2n)$ -bit 密钥, 其密钥是由 (K_1, K_2, K_3) 密钥三重组所构成. 而 TMAC 算法用 $(K, K' \cdot u, K')$ 来代替 XCBC 中的 (K_1, K_2, K_3) , 其中 u 是定义在 $GF(2^n)$ 的常数. TMAC 仅需两个密钥: k -bit 密钥 K 和 n -bit 密钥 K' , 共 $(k+n)$ -bit. 2005 年, Mitchell 分析 TMAC 算法时提出了一种变形的 TMAC 算法, 这里称为 TMAC-V 算法^[9]. 在 TMAC-V 算法中用密钥 K' 加密固定的 n -bit 串 S_2 来代替 TMAC 中的 $K' \cdot u$, 用密钥 K' 加密固定的 n -bit 串 S_3 来代替 TMAC 中的 K' . TMAC-V 工作模式如算法 2 所示.

算法 2.

1. 判断消息 M 的长度, 是否是分组密码算法对应长度 n 的整数倍.

1.1. 是整数倍时, 计算 $E_{K'}(S_2)$, 并把其值赋给 Z , 即 $Z = E_{K'}(S_2)$. 将消息 M 的值赋给 P , 即 $P = M$.

1.2. 不是整数倍时, 计算 $E_{K'}(S_3)$, 并把其值赋给 Z , 即 $Z = E_{K'}(S_3)$. 并将消息 M 填充至 n 的整数倍长再将其值赋给 P (填充方法和算法 1 一致), 即 $P = M \parallel 10^i$, 其中 $i = (n-1 - |M|) \bmod n$.

2. 将 P 分拆成长为 n 的 m 块, $P = P_1 \parallel P_2 \parallel \dots \parallel P_m$, 其中 $|P_1| = |P_2| = \dots = |P_m| = n$.

3. 将长度为 n 的全零序列赋给 C_0 , 即 $C_0 = 0^n$.

4. 对于 $i = 1$ 到 $i = m-1$ 做如下操作: $C_i = E_K(P_i \oplus C_{i-1})$.

5. 输出 MAC 值为 $E_K(P_m \oplus C_{m-1} \oplus Z)$.

其中 S_2 和 S_3 是 n 长的固定比特串.

3 PMAC 的随机消息伪造攻击

2006 年, Lee 等人对固定消息的 PMAC 进行了伪造攻击^[10]. 由于该攻击是针对固定消息, 局限性较大. 本节利用模式的局部差分恒等原理, 针对随机消息给出 PMAC 的一种新的随机消息伪造攻击方法. 下面首先给出生日碰撞概率的性质.

性质 1 (生日碰撞概率)^[11]. 集合 A 由 n 个不同的事件组成, 随机选取 d 个事件, 这 d 个事件中的每一个都可能是集合 A 中的任意一个事件, 其概率为 2^{-n} . 则这 d 个事件中至少存在两个事件相同的概率是 $p = 1 - e^{-n(n-1)/2d}$.

3.1 无输出截断时的随机消息伪造攻击

首先讨论 PMAC 没有输出截断时的随机消息伪造攻击, 即输出 tag 长度 $\tau = n$. 攻击过程由以下 6

步构成.

1. 随机选取 $2^{n/2+1}$ 个消息及对应的消息认证码 (MAC), 设消息 $M(i)$ 对应的 MAC 为 $T(i)$, $i = 1, \dots, 2^{n/2+1}$. 由生日碰撞概率性质可得: 在 $2^{n/2+1}$ 个消息中至少存在一个碰撞对的概率约为 $p = 1 - e^{-\frac{\frac{n}{2}+1}{2} \cdot \frac{\frac{n}{2}+1}{2^{n/2}}} \approx 1 - e^{-2} = 0.865$. 设 $M(i) = (M[1], \dots, M[q], X)$ 和 $M(j) = (M^*[1], \dots, M^*[p], Y)$ 是一对碰撞对, 即 $T(i) = T(j)$, 或 $PMAC_k(M(i)) = PMAC_k(M(j))$.

2. 以下分 3 种情况讨论这个碰撞对:

(1) 若碰撞对 $M(i)$ 和 $M(j)$ 的最后一个分组长度均为 n , 由算法 1 可得 $E_k(X \oplus \sum_{i=1}^q E_k(M[i] \oplus \gamma_i \cdot L) \oplus L \cdot x^{-1}) = E_k(Y \oplus \sum_{j=1}^p E_k(M^*[j] \oplus \gamma_j \cdot L) \oplus L \cdot x^{-1})$, 跳至步 3.

(2) 若碰撞对 $M(i)$ 和 $M(j)$ 的最后一个分组长度均小于 n , 则有 $E_k((X \parallel padding) \oplus \sum_{i=1}^q E_k(M[i] \oplus \gamma_i \cdot L)) = E_k((Y \parallel padding) \oplus \sum_{j=1}^p E_k(M^*[j] \oplus \gamma_j \cdot L))$, 跳至步 4.

(3) 若碰撞对 $M(i)$ 和 $M(j)$ 的最后一个分组仅有一个长度小于 n (假定为 $M(i)$), 则有 $E_k((X \parallel padding) \oplus \sum_{i=1}^q E_k(M[i] \oplus \gamma_i \cdot L)) = E_k(Y \oplus \sum_{j=1}^p E_k(M^*[j] \oplus \gamma_j \cdot L) \oplus L \cdot x^{-1})$, 跳至步 5.

3. 因为分组算法是一个置换, 相同的输出对应相同的输入. 当满足步 2 的情况 (1) 时, 即 $E_k(X \oplus \sum_{i=1}^q E_k(M[i] \oplus \gamma_i \cdot L) \oplus L \cdot x^{-1}) = E_k(Y \oplus \sum_{j=1}^p E_k(M^*[j] \oplus \gamma_j \cdot L) \oplus L \cdot x^{-1})$, 由分组算法的置换性质可得 $X \oplus \sum_{i=1}^q E_k(M[i] \oplus \gamma_i \cdot L) \oplus L \cdot x^{-1} = Y \oplus \sum_{j=1}^p E_k(M^*[j] \oplus \gamma_j \cdot L) \oplus L \cdot x^{-1}$. 再将等式两边同时异或差量串 Δ 可得 $(X \oplus \Delta) \oplus \sum_{i=1}^q E_k(M[i] \oplus \gamma_i \cdot L) \oplus L \cdot x^{-1} = (Y \oplus \Delta) \oplus \sum_{j=1}^p E_k(M^*[j] \oplus \gamma_j \cdot L) \oplus L \cdot x^{-1}$. 跳至步 6.

4. 当 $E_k((X \parallel padding) \oplus \sum_{i=1}^q E_k(M[i] \oplus \gamma_i \cdot L)) = E_k((Y \parallel padding) \oplus \sum_{j=1}^p E_k(M^*[j] \oplus \gamma_j \cdot L))$, 即步 2 的情况 (2) 时, 由分组算法的置换性质可得 $(X \parallel padding) \oplus \sum_{i=1}^q E_k(M[i] \oplus \gamma_i \cdot L) = (Y \parallel padding) \oplus \sum_{j=1}^p E_k(M^*[j] \oplus \gamma_j \cdot L)$. 再将等式两边同时异或差量串 Δ 可得 $((X \parallel padding) \oplus \Delta) \oplus \sum_{i=1}^q E_k(M[i] \oplus \gamma_i \cdot L) = ((Y \parallel padding) \oplus \Delta) \oplus \sum_{j=1}^p E_k(M^*[j] \oplus \gamma_j \cdot L)$. 跳至步 6.

5. 当 $E_k((X \parallel padding) \oplus \sum_{i=1}^q E_k(M[i] \oplus \gamma_i \cdot L)) = E_k(Y \oplus \sum_{j=1}^p E_k(M^*[j] \oplus \gamma_j \cdot L) \oplus L \cdot x^{-1})$, 即步 2 的情

况(3)时,由分组算法的置换性质可得 $(X \parallel padding) \oplus \sum_{i=1}^q E_k(M[i] \oplus \gamma_i \cdot L) = Y \oplus \sum_{j=1}^p E_k(M^*[j] \oplus \gamma_j \cdot L) \oplus L \cdot x^{-1}$. 再将等式两边同时异或差量串 Δ 可得 $((X \parallel padding) \oplus \Delta) \oplus \sum_{i=1}^q E_k(M[i] \oplus \gamma_i \cdot L) = (Y \oplus \Delta) \oplus \sum_{j=1}^p E_k(M^*[j] \oplus \gamma_j \cdot L) \oplus L \cdot x^{-1}$.

6. 截获一个新的消息 $(M[1], \dots, M[q], X \oplus \Delta)$, 对应的 MAC 记为 T^* , 则消息 $(M^*[1], \dots, M^*[p], Y \oplus \Delta)$ 所对应的 MAC 也为 T^* . 此时满足 $PMAC_k(M^*[1], \dots, M^*[p], Y \oplus \Delta) = T^* = PMAC_k(M[1], \dots, M[q], X \oplus \Delta)$.

由此,我们给出了一种 PMAC 输出无截断时的随机消息伪造攻击. 该攻击利用的是模式局部的差分恒等性质来伪造新的消息对. 当输出长度为 $\tau(\tau=n)$ 时,该攻击需要 $2^{n/2+1}$ 的随机消息和它对应的 MAC 对以及 1 个选择消息和它对应的 MAC 对,攻击复杂度为 $[0, 2^{n/2+1}, 1, 0]$. 此处复杂度的定义由文献[5]给出: $[a, b, c, d]$, a 表示离线工作的分组密码加密或解密次数, b 表示已知的消息和它对应 MAC 对的数目, c 表示选择消息和它对应的 MAC 对的数目, d 表示在线工作所需的 MAC 认证的次数.

3.2 有输出截断时的随机消息伪造攻击

下面讨论 PMAC 有输出截断时的随机消息伪造攻击, 即 $\tau < n$. 此时, 输出的 tag 存在两种碰撞——外部碰撞和内部碰撞. 外部碰撞是当消息对最后一个分组加密 $E_k(\cdot)$ 输出不同, 但选取前 τ 字节后相同. 若分组算法的数据长度为 n , 则外部碰撞共有 $2^{n-\tau}$ 个. 另一种是来自内部的碰撞, 即分组加密 $E_k(\cdot)$ 输出相同. 为了可以成功伪造任意消息, 攻击者希望可以从所有的外部碰撞中找到内部碰撞, 从而成功伪造 MAC. 攻击过程由以下 4 步构成:

1. 随机选取 $2^{n/2+1}$ 个消息及对应的消息认证码(MAC). 设 $M(i)$ 对应的 MAC 为 $T(i)$, $i=1, \dots, 2^{n/2+1}$. 设 $M(i) = (M[1], \dots, M[q], X)$ 和 $M(j) = (M^*[1], \dots, M^*[p], Y)$ 是一对碰撞对即 $T(i) = T(j)$ 或 $PMAC_k(M(i)) = PMAC_k(M(j))$.

2. 对这个碰撞对, 又可分为以下 3 种情况讨论:

(1) 若碰撞对 $M(i)$ 和 $M(j)$ 的最后一个分组长度均为 n , 由算法 1 可得 $E_k(X \oplus \sum_{i=1}^q E_k(M[i] \oplus \gamma_i \cdot L) \oplus L \cdot x^{-1}) = E_k(Y \oplus \sum_{j=1}^p E_k(M^*[j] \oplus \gamma_j \cdot L) \oplus L \cdot x^{-1})$, 跳至步 3.

(2) 若碰撞对 $M(i)$ 和 $M(j)$ 的最后一个分组长度均小于 n , 则有 $E_k((X \parallel padding) \oplus \sum_{i=1}^q E_k(M[i] \oplus \gamma_i \cdot L)) = E_k((Y \parallel padding) \oplus \sum_{j=1}^p E_k(M^*[j] \oplus \gamma_j \cdot L))$, 跳至步 3.

(3) 若碰撞对 $M(i)$ 和 $M(j)$ 的最后一个分组仅有一个

的长度小于 n (假定为 $M(i)$), 则有 $E_k((X \parallel padding) \oplus \sum_{i=1}^q E_k(M[i] \oplus \gamma_i \cdot L)) = E_k(Y \oplus \sum_{j=1}^p E_k(M^*[j] \oplus \gamma_j \cdot L) \oplus L \cdot x^{-1})$, 跳至步 3.

3. 下面只分析步 2 中的第(1)种情况, 另外两种情况分析方法类似, 结论一致.

如果该碰撞是内部碰撞, 由分组算法的置换性质可得 $X \oplus \sum_{i=1}^q E_k(M[i] \oplus \gamma_i \cdot L) \oplus L \cdot x^{-1} = Y \oplus \sum_{j=1}^p E_k(M^*[j] \oplus \gamma_j \cdot L) \oplus L \cdot x^{-1}$. 再将等式两边同时异或差量串 Δ 可得 $(X \oplus \Delta) \oplus \sum_{i=1}^q E_k(M[i] \oplus \gamma_i \cdot L) \oplus L \cdot x^{-1} = (Y \oplus \Delta) \oplus \sum_{j=1}^p E_k(M^*[j] \oplus \gamma_j \cdot L) \oplus L \cdot x^{-1}$. 为了找到正确的内部碰撞, 攻击者选择一个差量串 Δ , 并得到一个消息 $(M[1], \dots, M[q], X \oplus \Delta)$ 对应的 MAC 值记为 T^* , 验证 $(M^*[1], \dots, M^*[p], Y \oplus \Delta)$ 所对应的 MAC 值是否也为 T^* . 如果通过验证, 把这组碰撞作为候选, 再选取不同的差量串 Δ 进行测试. 否则, 丢弃这组碰撞值, 这组碰撞只是外部碰撞, 再寻找另一碰撞对.

4. 如果有 $2^{n-\tau}$ 个外部碰撞, 那么一次验证后剩下的可能的内部碰撞有 $2^{n-2\tau}$ 个. 经过选取不同差量串 Δ 进行 $\lceil n/\tau \rceil$ 次验证, 可以得到所需的内部碰撞, 从而得到正确的候选值. 如果正确的候选碰撞对为 $M(i) = (M[1], \dots, M[q], X)$ 和 $M(j) = (M^*[1], \dots, M^*[p], Y)$, 截获一个新的消息 $(M[1], \dots, M[q], X \oplus \Delta)$ 对应的 MAC 记为 T^* , 则 $(M^*[1], \dots, M^*[p], Y \oplus \Delta)$ 所对应的 MAC 也为 T^* , 此时满足 $PMAC_k(M^*[1], \dots, M^*[p], Y \oplus \Delta) = T^* = PMAC_k(M[1], \dots, M[q], X \oplus \Delta)$.

由此, 我们给出了当 PMAC 输出有截断时的随机消息伪造攻击. 当输出长度为 $\tau(\tau < n)$ 时, 该攻击需要 $2^{n/2+1}$ 的随机消息和它对应的 MAC 对以及 $\lceil n/\tau \rceil$ 个选择消息和它对应的 MAC 对, 此外还需要至多 $2^{n-\tau} + 2^{n-2\tau} + \dots + 2^{n-\lceil n/\tau \rceil \cdot \tau} \approx 2^{n-\tau}$ MAC 认证次数, 攻击复杂度为 $[0, 2^{n/2+1}, \lceil n/\tau \rceil, 2^{n-\tau}]$.

4 TMAC-V 的随机消息伪造攻击

下面讨论 TMAC-V 的随机消息伪造攻击. 攻击过程由以下 6 步构成:

1. 随机选取 $2^{n/2+1}$ 个消息及对应的消息认证码(MAC), 设 $M(i)$ 对应的 MAC 为 $T(i)$, $i=1, \dots, 2^{n/2+1}$. 由生日碰撞概率性质可得: 在 $2^{n/2+1}$ 个消息中至少存在一个碰撞对的概率约为 $p = 1 - e^{-\frac{\frac{n}{2}+1}{2 \cdot 2^n} \cdot \frac{\frac{n}{2}+1}{2} - 1} \approx 1 - e^{-2} = 0.865$. 设 $M(i) = (M[1], \dots, M[q], X)$ 和 $M(j) = (M^*[1], \dots, M^*[p], Y)$ 是一对碰撞对, 即 $T(i) = T(j)$ 或 $TMAC-V_k(M(i)) = TMAC-V_k(M(j))$.

2. 以下分 3 种情况讨论这个碰撞对:

(1) 若碰撞对所对应消息的最后一个分组长度均为 n ，则有 $E_k(X \oplus E_{k'}(S_2) \oplus C(i)^{(q)}) = E_k(Y \oplus E_{k'}(S_2) \oplus C(j)^{(p)})$. $C(i)^{(q)}$ 表示消息 $M(i)$ 在 TMAC-V 算法中的第 q 个分组的输出，即 $t=1$ 到 $t=q$ 时做如下操作： $C(i)^t = E_k(M[t] \oplus C(i)^{t-1})$ ，其中 $C(i)^0 = 0^n$. $C(j)^{(p)}$ 表示消息 $M(j)$ 在 TMAC-V 算法中的第 p 个分组的输出，即 $t=1$ 到 $t=p$ 时做如下操作： $C(j)^t = E_k(M^*[t] \oplus C(j)^{t-1})$ ，其中 $C(j)^0 = 0^n$. 跳至步 3.

(2) 若碰撞对所对应消息的最后一个分组长度均小于 n ，则有 $E_k((X \parallel padding) \oplus E_{k'}(S_3) \oplus C(i)^{(q)}) = E_k((Y \parallel padding) \oplus E_{k'}(S_3) \oplus C(j)^{(p)})$ ，跳至步 4.

(3) 若碰撞对所对应消息的最后一个分组有一个的长度小于 n (假定为 $M(i)$)，则有 $E_k((X \parallel padding) \oplus E_{k'}(S_3) \oplus C(i)^{(q)}) = E_k(Y \oplus E_{k'}(S_2) \oplus C(j)^{(p)})$ ，跳至步 5.

3. 因为分组算法是一个置换，相同的输出对应相同的输入. 当满足步 2 的情况 (1) 时，即 $E_k(X \oplus E_{k'}(S_2) \oplus C(i)^{(q)}) = E_k(Y \oplus E_{k'}(S_2) \oplus C(j)^{(p)})$ ，由分组算法的置换性质可得 $X \oplus E_{k'}(S_2) \oplus C(i)^{(q)} = Y \oplus E_{k'}(S_2) \oplus C(j)^{(p)}$. 再将等式两边同时异或差量串 Δ 可得 $(X \oplus \Delta) \oplus E_{k'}(S_2) \oplus C(i)^{(q)} = (Y \oplus \Delta) \oplus E_{k'}(S_2) \oplus C(j)^{(p)}$. 跳至步 6.

4. 当 $E_k((X \parallel padding) \oplus E_{k'}(S_3) \oplus C(i)^{(q)}) = E_k((Y \parallel padding) \oplus E_{k'}(S_3) \oplus C(j)^{(p)})$ ，即步 2 的情况 (2) 时，可得 $(X \parallel padding) \oplus E_{k'}(S_3) \oplus C(i)^{(q)} = (Y \parallel padding) \oplus E_{k'}(S_3) \oplus C(j)^{(p)}$. 再将等式两边同时异或差量串 Δ 可得 $((X \parallel padding) \oplus \Delta) \oplus E_{k'}(S_3) \oplus C(i)^{(q)} = ((Y \parallel padding) \oplus \Delta) \oplus E_{k'}(S_3) \oplus C(j)^{(p)}$. 跳至步 6.

5. 当 $E_k((X \parallel padding) \oplus E_{k'}(S_3) \oplus C(i)^{(q)}) = E_k(Y \oplus E_{k'}(S_2) \oplus C(j)^{(p)})$ 即步 2 的情况 (3) 时，可得 $(X \parallel padding) \oplus E_{k'}(S_3) \oplus C(i)^{(q)} = Y \oplus E_{k'}(S_2) \oplus C(j)^{(p)}$. 再将等式两边同时异或差量串 Δ 可得 $((X \parallel padding) \oplus \Delta) \oplus E_{k'}(S_3) \oplus C(i)^{(q)} = (Y \oplus \Delta) \oplus E_{k'}(S_2) \oplus C(j)^{(p)}$.

6. 截获一个新的消息 $(M[1], \dots, M[q], X \oplus \Delta)$ 对应的 MAC 值记为 T^* ，则 $(M^*[1], \dots, M^*[p], Y \oplus \Delta)$ 所对应的 MAC 值也为 T^* ，即 $TMAC-V_k(M^*[1], \dots, M^*[p], Y \oplus \Delta) = T^* = TMAC-V_k(M[1], \dots, M[q], X \oplus \Delta)$.

由此，我们给出了 TMAC-V 的随机消息伪造攻击. 该攻击利用的是模式局部的差分恒等性质来伪造新的消息对. 该攻击需要 $2^{n/2+1}$ 的随机消息和它对应的 MAC 对以及 1 个选择消息和它对应的 MAC 对，攻击复杂度为 $[0, 2^{n/2+1}, 1, 0]$.

5 比较和结论

本文利用模式的局部差分恒等原理，针对 PMAC 和 TMAC-V 两种工作模式，给出一种新的随机消息伪造攻击. 该攻击可对随机消息的 PMAC 和 TMAC-V 进行伪造，伪造的成功概率均为 86.5%，

高于文献[10]中的成功概率 63%. 对 PMAC 输出无截断的攻击复杂度为 $[0, 2^{n/2+1}, 1, 0]$ ，输出有截断的攻击复杂度为 $[0, 2^{n/2+1}, \lceil n/\tau \rceil, 2^{n-\tau}]$ ；对 TMAC-V 的攻击复杂度为 $[0, 2^{n/2+1}, 1, 0]$. 本文和文献[10]的分析结果和碰撞条件如表 1 所示.

表 1 PMAC 和 TMAC-V 攻击复杂度比较

方案	消息碰撞条件	复杂度	文献
PMAC 输出无截断	固定选取	$[0, 0, 2^{n/2+1}, 0]$	文献[10]
PMAC 输出有截断	固定选取	$[0, 0, 2^{n/2+1}, 2^{n-\tau}]$	文献[10]
PMAC 输出无截断	随机选取	$[0, 2^{n/2+1}, 1, 0]$	本文
PMAC 输出有截断	随机选取	$[0, 2^{n/2+1}, \lceil n/\tau \rceil, 2^{n-\tau}]$	本文
TMAC-V	固定选取	$[0, 0, 2^{n/2+1}, 0]$	文献[10]
TMAC-V	随机选取	$[0, 2^{n/2+1}, 1, 0]$	本文

由以上的参数比较，我们知道该新攻击利用的是随机消息伪造攻击，其中所需要的消息碰撞条件是很宽松的，而且伪造成功的概率也高于文献[10]中的结论. 因此，该伪造方法更为实用和新型有效.

参 考 文 献

[1] Gilbert E N, MacWilliams F J, Sloane N J. Codes which detect deception. Bell System Technical Journal, 1974, 53: 405-424

[2] Simmons G J. A game theory model of digital message authentication//Proceedings of the 11th Annual Conference on Numerical Mathematics and Computing, University of Manitoba, Winnipeg, Canada, 1982, 34: 413-424

[3] Simmons G J. A system for verifying user identity and authorization at the point-of-sale or access. Cryptologia, 1984, 8(1): 1-21

[4] Simmons G J. A Cartesian product construction for unconditionally secure authentication codes that permit arbitration. Journal of Cryptology, 1990, 2(2): 77-104

[5] ISO/IEC 9797-1. Information technology-security techniques—Message Authentication Code (MACs) — Part 1: Mechanism using a block cipher, international organization for standardization. Geneve, Switzerland, 1999

[6] Black J, Rogaway P. A block-cipher mode of operation for parallelizable message authentication//Proceedings of the Eurocrypt'02. Amsterdam, The Netherlands, 2002: 384-397

[7] Gligor V, Donescu P. Fast encryption and authentication: XCBC encryption and XECB authentication modes//Proceedings of the FSE'01. Yokohama, Japan, 2002: 92-108

[8] Kurosawa K, Iwata T. TMAC: Two-key CBC-MAC//Proceedings of the CT-RSA 2003. San Francisco, CA, USA, 2003: 33-49

[9] Mitchell C. Partial key recovery attack on XCBC, TMAC, and OMAC//Proceedings of the 10th IMA International Conference—CCC 2005. Cirencester, UK, 2005: 155-167

[10] Lee Changhoon, Kim Jongsung, Sung Jaechul et al. Forgery and key recovery attacks on PMAC and Mitchell's TMAC variant//Proceedings of the 11th Australasian Conference ACISP 2006. Lecture Notes in Computer Science 4058. Melbourne, Australia, 2006; 421-431

[11] Menezes A, Oorschot P C, Vanstone S. Handbook of Applied Cryptography. New York: CRC Press, 1997



CHEN Jie, born in 1979, Ph. D. candidate. Her current research interests include design and analysis of block cipher.

HU Yu-Pu, born in 1955, Ph. D. , professor and Ph. D. supervisor. His current research interests include cryptology and information security.

WEI Yong-Zhuang, born in 1976, Ph. D. candidate. His current research interests include analysis of cryptographic functions and block cipher.

Background

This research is supported by the National Natural Science Foundation of China under grant No. 60673072, and the National High Technology Research and Development Program (863 Program) of China (2007AA01Z435), and the Natural Science Basic Research Plain in Shaanxi Province of China (Program No. 2007F37).

This paper focuses on the field of forgery attacks on MACs which based on block cipher. The research group has done much research work in the design and analysis of block ciphers and other related work of block ciphers. A Message Authentication Code (MAC) is a hash function with secret key, which satisfies that different keys can induce different hash functions. Therefore, receiver can verify whether the message is forged from sender. At the same time, receiver can also verify who send the message. MAC algorithms have two forms that based on block cipher and based on hash function. This paper research MACs based on block cipher, which are PMAC and TMAC-V. PMAC, a fully parallelizable MAC scheme based on block cipher, is proposed by

Black and Rogaway in Eurocrypt 2002. In 2005, Mitchell presented TMAC-V to improve the security of TMAC. A MAC is secure if for an adversary who does not know the secret key K, it is computationally infeasible to perform an existential forgery under an adaptive chosen text attack. In the conference of ACISP 2006, Lee et al. devised forgery attack on PMAC and TMAC-V. But their method need fixed message, with a probability of 63%. This paper presents a new forgery attack on PMAC and TMAC-V with random message, which make use of the principle of differential identical in part of the mode. The new attack can forge the PMAC and TMAC-V of random message, with a probability of 86.5% higher than 63% in the known reference. The complexity of this new attack is $[0, 2^{n/2+1}, 1, 0]$ for PMAC where no truncation is performed. For PMAC where truncation is performed, the complexity of this attack is $[0, 2^{n/2+1}, \lceil n/\tau \rceil, 2^{n-\tau}]$. And the complexity of this attack is $[0, 2^{n/2+1}, 1, 0]$ for TMAC-V.