第35卷 第22期 计 算 机 工 程 2009年11月
Vol.35 No.22 Computer Engineering November 2009
·安全技术· 文章编号：1000—3428(2009)22—0150—03 文献标识码：A 中图分类号：TN918.1

PMAC模式的消息伪造攻击

刘彦宾[1]，韦永壮[2,3]
(1. 遵义师范学院计算机科学系，遵义 563002；2. 桂林电子科技大学信息与通信学院，桂林 541004；
3. 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)

摘 要：针对PMAC工作模式，利用模式局部差分恒等原理，给出一种消息伪造攻击方法，指出新攻击下PMAC工作模式是脆弱的。利用该方法可以成功地进行消息和其MAC的伪造。与已有的攻击方法相比，该新攻击所需的碰撞条件更为宽松，并使得实施攻击更为灵活、有效。

关键词：分组密码；消息认证码；PMAC模式；消息伪造攻击

Message Forgery Attack on PMAC Mode

LIU Yan-bin[1], WEI Yong-zhuang[2,3]
(1. Department of Computer Science, Zunyi Normal University, Zunyi 563002;
2. School of Information and Communication, Guilin University of Electronic Technology, Guilin 541004;
3. Key Laboratory of Computer Networks & Information Security, Ministry of Education, Xidian University, Xi'an 710071)

【Abstract】 This paper proposes a message forgery attack on PMAC mode by using the property of differential equivalent of local operation mode. It shows that PMAC mode is vulnerable to the new message forgery attack, where new message and corresponding MAC code can be forged successfully. Compared with the previously works, it shows that the new forgery attack is more flexible and effective, and the collision condition is much looser.

【Key words】 block cipher; message authentication code; PMAC mode; message forgery attack

1 概述

基于分组密码构建各种消息认证码(MAC)是目前的研究热点之一[1]。CBC-MAC模式[2]是基于分组密码构造MAC最典型的代表之一。由于CBC-MAC模式是基于串联模式工作的，文献[3]提出了一种新的并联工作模式，即PMAC，并声称在假设分组密码算法为伪随机置换条件下该工作模式是可证明安全的。文献[4]针对PMAC提出了一种消息伪造攻击方法。本质上，这种攻击的最大缺点是每次攻击时都需要获取2个长度固定且相等的消息集和对应的MAC码集。文献[5]针对PMAC给出了一种新的随机消息伪造方法。该方法避免了文献[4]攻击方法的缺点，然而不足之处是需要更多的在线选择消息串和对应MAC码。

如何提出灵活的、新型有效的攻击方法，特别是减少攻击所需的数据量(如在线选择消息串和对应 MAC 码)是当前的研究重点。

针对PMAC工作模式，本文提出了一种新的随机消息伪造攻击方法。该攻击有效地降低了攻击所需的数据量，特别是减少了在线选择消息串和对应MAC码的数量。

2 准备知识

本节回顾PMAC工作模式及相关定义。

(1)PMAC工作模式介绍[3]

$\mathrm{PMAC}_k(M)$
$L \leftarrow E_k(0^n)$
if $|M| > n2^n$ then return 0^τ
Partition M into M[1], M[2],…, M[r]
for i ← 1 to r-1 do
$X[i] \leftarrow M[i] \oplus \gamma_i \cdot L$
$Y[i] \leftarrow E_k(M[i])$
$\Sigma \leftarrow Y[1] \oplus Y[2] \oplus \cdots \oplus Y[r-1] \oplus \mathrm{pad}(M[r])$
if $|M[r]| = n$ then return $X[r] = \Sigma \oplus L \cdot x^{-1}$, else $X[r] \leftarrow \Sigma$
MAC= truncation of first τ bits of $(E_k(X[r]))$
return MAC

其中，γ_i 为Gray码。

实际上，PMAC工作模式利用的是一个密钥信息 k 和任意长度消息串 M，其输出是 τ bit MAC码。

(2)定义与注记

定义1(τ-消息对)[6] 如果2个消息串的整体长度一样，在工作模式下分组时，仅有最后一个数据块的值是不同的，则称这2个消息串是 τ-消息对。

例如 2个消息串的整体长度一样 $M=(M[1], M[2],\cdots,M[q], X)$，$M^*=(M[1], M[2],\cdots, M[q], Y)$。其中，$M[1], M[2],\cdots, M[q], X, Y$ 都是对应模式下的数据分组，且 $X \neq Y$，则 M 与 M^* 是 τ-消息对。

定义2(t-消息集) 如果 t 个消息串的整体长度一样，在工作模式下分组时，仅有最后一个数据块的值是不同的，则称这 t 个消息串是 t-消息集。

实际上，τ-消息对就是2-消息集。

注记：$|X|$表示比特串 X 的长度。

基金项目：国家自然科学基金资助项目(60673072)
作者简介：刘彦宾(1966－)，男，副教授、硕士，主研方向：信息安全；韦永壮，讲师、博士研究生
收稿日期：2009-05-23 **E-mail：**walker_wyz@tom.com

3 PMAC 工作模式的一种新的消息伪造攻击方法

本节介绍 PMAC 工作模式的一种新的消息伪造攻击方法，并指出新攻击下 PMAC 工作模式是脆弱的。

利用本文的新方法可以成功地进行消息和其 MAC 码的伪造。

算法 1 输出长度$|T|=\tau=n$。

Step1 随机获得 $2^{n/2-1}$ 个不同的 τ-消息对及对应的 MAC 码；设 τ-消息对(M_1^i,M_2^i)对应的 MAC 为$(T_1^i,\ T_2^i)$, i=1, 2,…,$2^{n/2-1}$；注意这些 τ-消息对的数据分组长度并不固定，可以随机选择。

Step2 随机获得 $2^{n/2}$ 个不同的消息及对应的 MAC 码；设 $M(i)$对应 $T(i)$, i=1,2,…,$2^{n/2}$；注意这些消息的数据分组长度并不固定，都可以随机选择。

Step3 利用生日碰撞定理，在 $2^{n/2+1}$ 个消息中约以 63%概率至少存在一个碰撞对。也就是消息集(M_1^i,M_2^i), i=0,1,…, $2^{n/2-1}$以 63%概率至少存在一个消息 M与消息集 $M(i)$, i=0,1,…, $2^{n/2}$ 中的一个消息 M^*所产生的 MAC 码是碰撞的，即 $\mathrm{PMAC}_k(M)=\mathrm{PMAC}_k(M^*)$。

设 $M=M_1^{i*}=(M[1],M[2],\cdots,M[q],X)$和 $M^*=(M^*[1],M^*[2],\cdots, M^*[p],Y)$是一对碰撞对，即 $\mathrm{PMAC}_k(M)=\mathrm{PMAC}_k(M^*)$。

由 PMAC 的算法特点，知道这个碰撞对有以下 3 种情形：

(1)若碰撞对所对应消息的最后一个分组长度均为 n，即 $|X|=|Y|=n$，则

$$E_k(X\oplus\sum_{i=1}^{q}E_k(M[i])\oplus L\cdot x^{-1})=E_k(Y\oplus\sum_{j=1}^{p}E_k(M^*[j])\oplus L\cdot x^{-1})$$

(2)若碰撞对所对应消息的最后一个分组长度均小于 n，即 $|X|<n,|Y|<n$，则

$$E_k((X\,\|\,padding)\oplus\sum_{i=1}^{q}E_k(M[i])\oplus 0^n)=$$
$$E_k((Y\,\|\,padding^*)\oplus\sum_{j=1}^{p}E_k(M^*[j])\oplus 0^n)$$

(3)若碰撞对所对应消息的最后一个分组仅有一个长度小于 n(假定为 $M(i)$)，即 $|X|<n,|Y|=n$，则

$$E_k((X\,\|\,padding)\oplus\sum_{i=1}^{q}E_k(M[i])\oplus 0^n)=$$
$$E_k(Y\oplus\sum_{j=1}^{p}E_k(M^*[j])\oplus L\cdot x^{-1})$$

Step4 以下仅讨论第一种情形，其他 2 种情形类似：若碰撞对所对应消息的最后一个分组长度均为 n，即 $|X|=|Y|=n$，则

$$E_k(X\oplus\sum_{i=1}^{q}E_k(M[i])\oplus L\cdot x^{-1})=E_k(Y\oplus\sum_{j=1}^{p}E_k(M^*[j])\oplus L\cdot x^{-1})$$

进一步地：

$$X\oplus\sum_{i=1}^{q}E_k(M[i])\oplus L\cdot x^{-1}=Y\oplus\sum_{j=1}^{p}E_k(M^*[j])\oplus L\cdot x^{-1}$$

由此有：

$$X\oplus\Delta\oplus\sum_{i=1}^{q}E_k(M[i])\oplus L\cdot x^{-1}=Y\oplus\Delta\oplus\sum_{j=1}^{p}E_k(M^*[j])\oplus L\cdot x^{-1}$$

其中，Δ为任意非零串，且$|\Delta|=n$。

注意到，在 τ-消息对内 $M=M_1^{i*}=(M[1], M[2],\cdots, M[q], X)$所对应的另一个消息是 $M_2^{i*}=(M[1],\ M[2],\cdots,\ M[q],\ X^*)$，其中，$X\neq X^*$；记 M_2^{i*}所对应的 MAC 码为 $T_2^{i*}=T^*$。令 $\Delta=X\oplus X^*$，则 $(M^*[1],\ M^*[2],\cdots,\ M^*[p], Y\oplus\Delta)$所对应的 MAC 也为 T^*，即

$$PMAC_k(M^*[1], M^*[2],\cdots, M^*[p], Y\oplus\Delta)=$$
$$PMAC_k(M[1], M[2],\cdots, M[q], X\oplus\Delta)=$$
$$PMAC_k(M[1], M[2],\cdots, M[q], X^*)=T_2^{i*}=T^*$$

因此，可以伪造出新的消息和它所对应的 MAC 码：$(M^*[1], M^*[2],\cdots, M^*[p],\ Y\oplus\Delta)$与 T^*。

算法 2 输出长度$|T|=\tau<n$。

Step1 令 $t=\lceil n/\tau\rceil+2\approx 2^{\lambda}$，随机获得 $2^{(n/2-\lambda)}$ 个不同的 t-消息集及对应的 MAC 码；注意这些 t-消息集的分组长度并不固定，可以是随机长度。

Step2 随机获得 $2^{n/2}$ 个不同的消息及对应的 MAC 码；设 $M(i)$对应 $T(i)$, i=1,2,…,$2^{n/2}$；注意这些消息的数据分组长度并不固定，都可以随机选择。

Step3 利用生日碰撞定理，在 $2^{n/2+1}$ 个消息中约以概率 63%存在 $2^{n-\tau}$ 个碰撞对，即存在 $2^{n-\tau}$ 个消息对 $M(1)^{*(l)}=(M[1], M[2],\cdots,M[q^{(l)}],\ X^*(l))$和 $M(2)^{*(l)}=(M[1],\ M[2],\cdots,M[p^{(l)}],Y^*(l))$的 MAC 是碰撞的，其中，$1\le l\le 2^{n-\tau}$。由 PMAC 的算法特点，知道这些碰撞对有以下 3 种情形：

(1)若碰撞对所对应消息的最后一个分组长度均为 n，即 $|X(l)|=|Y(l)|=n$，则

$$(X(l)\oplus\Delta)\oplus\sum_{i=1}^{q^{(l)}}E_k(M[i])\oplus L\cdot x^{-1}=(Y(l)\oplus\Delta)\oplus\sum_{j=1}^{p^{(l)}}E_k(M^*[j])\oplus L\cdot x^{-1}$$

(2)若碰撞对所对应消息的最后一个分组长度均小于 n，即 $|X(l)|<n,|Y(l)|<n$，则

$$(X(l)\,\|\,padding)\oplus\Delta\oplus\sum_{i=1}^{q^{(l)}}E_k(M[i])\oplus 0^n=$$
$$(Y(l)\,\|\,padding^*)\oplus\Delta\oplus\sum_{j=1}^{p^{(l)}}E_k(M^*[j])\oplus 0^n$$

(3)若碰撞对所对应消息的最后一个分组仅有一个的长度小于 n，即 $|X(l)|<n,|Y(l)|=n$，则

$$(X(l)\,\|\,padding)\oplus\Delta\oplus\sum_{i=1}^{q^{(l)}}E_k(M[i])\oplus 0^n=$$
$$Y(l)\oplus\Delta\oplus\sum_{j=1}^{p^{(l)}}E_k(M^*[j])\oplus L\cdot x^{-1}$$

Step4 以下仅讨论第(1)种情形，其他 2 种情形类似：在碰撞消息集 $M(1)^{*(l)}=(M[1],\ M[2],\cdots,M[q^{(l)}],\ X^*(l))$中，考虑每个消息所对应的 t-消息集。在每个$(M[1],\ M[2],\cdots,M[q^{(l)}],\ X^*(l))$所在的 t-消息集中，任选一个消息即$(M[1],\ M[2],\cdots,M[q^{(l)}],\ X^{**}(l,i))$，其中，$1\le l\le 2^{n-\tau}, i=1,2,\cdots,t-1$。令 $\Delta^{(l)}=X^*(l)\oplus X^{**}(l,i)$。要求验证 $2^{n-\tau}$ 个消息 $M(2)^{*(l)}=(M[1],\ M[2],\cdots,\ M[p^{(l)}],\ \Delta^{(l)}\oplus Y^*(l))$的 MAC 码，并判断该 MAC 码是否等于$(M[1],\ M[2],\cdots,M[q^{(l)}],\ X^{**}(l,i))$的 MAC 码，其中，$1\le l\le 2^{n-\tau},\ i=1,2,\cdots,t-1$。若相等，则这个碰撞消息$(M[1],\ M[2],\cdots,\ M[q^{(l)}],\ X^*(l))$能通过。这一步能通过的碰撞消息集$(M[1],M[2],\cdots,\ M[q^{(l)}],\ X^*(l))$大约有 $2^{n-2\tau}$ 个。

Step5 重复 Step4 $\lceil n/\tau\rceil$ 次，最终能通过的碰撞消息为 $2^{n-\lceil n/\tau\rceil\cdot\tau}\approx 1$个，记为$(M[1],\ M[2],\cdots,\ M[q^{(l^*)}],\ X^*(l^*))$。这说明：在$(M[1],\ M[2],\cdots,\ M[q^{(l^*)}],\ X^*(l^*))$所在的 t-消息集中，任选一个消息即$(M[1],\ M[2],\cdots,\ M[q^{(l^*)}],\ X^{**}(l^*,i))$, $i=1,2,\cdots,t-1$，令 $\Delta^{(l^*)}=X^*(l^*)\oplus X^{**}(l^*,i)$，则均有

$$PMAC(M[1],\ M[2],\cdots,\ M[p^{(l^*)}],\ \Delta^{(l^*)}\oplus Y^*(l^*))=$$
$$PMAC(M[1],\ M[2],\cdots,\ M[q^{(l^*)}],\ X^{**}(l^*,i))$$

Step6 注意到，t-消息集中含有 t 个消息；而 Step5 重复 Step4 共$\lceil n/\tau\rceil=t$-2 次，故至少有一个消息$(M[1],\ M[2],\cdots,\ M[q^{(l^*)}],\ X^{**}(l^*,i^*))$没有参与 Step5 的验证。类似于算法 1 的 Step4，令 $\Delta^{(l^*)}=X^*(l^*)\oplus X^{**}(l^*,i^*)$，则

$PMAC(M[1], M[2],\cdots,M[p^{(l^*)}], \Delta^{(l^*)} \oplus Y^*(l^*))=$

$PMAC(M[1], M[2],\cdots, M[q^{(l^*)}], X^{**}(l^*,i^*))= T^*$

因此，可以伪造出新的消息和对应的 MAC 码。其中，攻击所需的已知消息串为 $2^{n/2+1}$，所需的 MAC 验证为 $2^{n-\tau}+2^{n-2\tau}+\cdots+2^{n-\lceil n/\tau\rceil\tau}\approx 2^{n-\tau}$ 次。

由此，给出了 PMAC 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。

4 结果比较

本节对 PMAC 工作模式的已有攻击结果进行比较。

其中，复杂度一项[a ,b ,c, d]：a 表示离线分组加/解密的次数；b 表示已知消息串和对应 MAC 的数量；c 表示在线选择消息串和对应 MAC 的数量；d 表示在线 MAC 码确认的次数。

由表 1 的参数比较可知：已有的攻击方法需要获取长度固定且相等的消息集和对应的 MAC 码集[4]，或是需要在线选择消息串和对应 MAC 码[5]；而本文的新攻击利用的是随机消息伪造攻击，攻击时仅需要获取随机长度消息集和对应的 MAC 码集，不需要在线选择消息串和对应 MAC 码，即所需的消息碰撞条件更为宽松。因此，该伪造攻击方法更为灵活和新型有效。

表 1　PMAC 工作模式的已有攻击结果比较

消息碰撞条件	输出截断	攻击复杂度	文献
长度固定	否	$[0,2^{n/2+1},0,0]$	文献[4]
长度固定	是	$[0,2^{n/2+1},0,2^{n-\tau}]$	文献[4]
随机长度	否	$[0,2^{n/2+1},1,0]$	文献[5]
随机长度	是	$[0,2^{n/2+1},\lceil n/\tau\rceil, 2^{n-\tau}]$	文献[5]
随机长度	否	$[0,2^{n/2+1},0,0]$	本文
随机长度	是	$[0,2^{n/2+1},0,2^{n-\tau}]$	本文

5 结束语

本文利用模式局部差分恒等原理，给出了 PMAC 模式的一种新攻击方法。与已有的各种攻击结果相比较，发现这种新攻击具有以下优点：(1)所需要的消息碰撞条件更为宽松，这使得实施攻击更为灵活、有效；(2)有效地降低了攻击所需的数据量，特别是减少了在线选择消息串和对应 MAC 码。值得注意的是：如何利用类似的攻击方法，针对 OMAC, XCBC 等模式进行分析，仍有待进一步深入研究。

参考文献

[1] 袁署光, 戴宏跃, 赖声礼. 基于 Hash 函数的 RFID 认证协议[J]. 计算机工程, 2008, 34(12): 141-143.

[2] International Organization for Standardization. ISO/IEC 9797-1-199 Information Technology Security Techniques Message Authentication Code(MACs)——Part 1: Mechanism Using a Block Cipher[S]. 1999.

[3] Black J, Rogaway P. A Block-cipher Mode of Operation for Parallelizable Message Authentication[C]//Proc. of International Conference on the Theory and Applications of Cryptographic Techniques. Amsterdam, Holland: Springer-Verlag, 2002: 384-397.

[4] Changhoon L, Jongsung K, Jaechul S, et al. Forgery and Key Recovery Attack on PMAC and Mitchell's TMAC Variant[C]//Proc. of the 11th Australasian Conference. Melbourne, Australia: Springer-Verlag, 2006: 421-431.

[5] 陈　杰, 胡予濮, 韦永壮. 随机消息伪造攻击 PMAC 和 TMAC-V[J]. 计算机学报, 2007, 30(10): 1827-1832.

[6] 韦永壮, 胡予濮, 陈　杰. TMAC-V 模式新的消息伪造攻击[J]. 信息安全与通信保密, 2007, 8(8): 48-50.

编辑　任吉慧

(上接第 149 页)

策略一：FLS 范式

典型应用出现在 BPK 协议[3]，验证方在私钥 SK 的 3 轮证据不可区分的知识证明中应用 KLS 范式，合并了关于证明方发送的随机串 v 的单向函数逆元 $u = f^{-1}(v)$ 作为与 SK 不可区分的二选一证据，通过破解单向函数获得 u 作为知识证明的证据。

策略二：Oracle 模型

在 cPK 协议中，验证方使用的签名协议 SS 的不可锻造性是基于 Oracle 模型的：通过询问 Oracle 可获得对证明方发送消息的签名作为验证方的消息(V 用私钥 SK 完成签名)。

在 WPK 协议中，验证方使用的可验证的随机函数族 VRF 的剩余伪随机性也是基于 Oracle 模型的：通过询问 Oracle 可获得对 x 及 VRF 的伪随机输出及正确性证明作为验证方的消息(V 的私钥 SK 由 VRF 的密钥发生器产生)。

4 结束语

本文比较全面地探讨了弱公钥模型集的特性，提出了该模型集下具有最优轮数的并发健壮的可重置零知识系统的 2 种通用构造模式，并就可重置、零知识、并发、健壮性等一系列安全性要求的实现技术分别进行了分析。

目前弱公钥模型集下的零知识系统改进的方向主要有：应用非黑盒模拟技术，以改进协议的轮数，健壮性和模拟时间；定义和构造新的基于弱假设的弱公钥模型集，以替代计数器的配置；开发有别于复杂性杠杆的技术进行协议的健壮性证明，以消除对亚指数计算攻击安全的限定；从论证系统到证明系统的改进；提高协议某些安全构件的性能，在不降低原有安全性的基础上引入新的安全特性。

参考文献

[1] Canetti R, Goldreich O, Coldwasser S, et al. Resettable Zero-knowledge[C]//Proc. of the 32nd Annual ACM Symposium on Theory of Computing. Portland, Oregon, USA: [s. n.], 2000.

[2] Micali S, Reyzin L. Soundness in the Public-key Model[C]//Proc. of the 21st Annual International Cryptology Conference on Advances in Cryptology. London, UK: Springer-Verlag, 2001: 542-565.

[3] Di Crescenzo G, Persiano G, Visconti I. Constant-round Resettable Zero Knowledge with Concurrent Soundness in the Public-key Model[C]//Proc. of the Annual International Cryptology Conference. Santa Barbara, USA: [s. n.], 2004: 237-253.

[4] Micali S, Reyzin L. Min-round Resettable Zero Knowledge in the Public-key Model[C]//Proc. of EUROCRYPT'01. Innsbruck, Austria: [s. n.], 2001: 373-393.

[5] Crescenzo G D, Persiano G, Visconti I. Improved Setup Assumptions for 3-round Resettable Zero Knowledge[C]//Proc. of ASIACRYPT'04. Jeju Island, Korea: [s. n.], 2004: 530-544.

[6] Zhao Yunlei, Deng Xiaotie, Lee C H, et al. Resettable Zero Knowledge in the Weak Public-key Model[C]//Proc. of the International Conference on the Theory and Applications of Cryptographic Techniques. Warsaw, Poland: [s. n.], 2003: 123-139.

编辑　任吉慧