iPMAC及VPMAC的伪造攻击

田玉丹[1] 韦永壮[2,3]
(广西信息科学实验中心(桂林电子科技大学) 桂林 541004)[1]
(广西无线宽带通信与信号处理重点实验室(桂林电子科技大学) 桂林 541004)[2]
(广西云计算与大数据协同创新中心(桂林电子科技大学) 桂林 541004)[3]

摘 要 消息认证码(MAC)是保证信息完整性传输的重要手段,目前已广泛应用于各种安全系统中。iPMAC和VPMAC由于其平行的结构模式成为了消息认证码的典型代表。而iPMAC和VPMAC是否存在新的安全性问题,是目前业界讨论的热点问题之一。根据iPMAC输入参数的可变性,利用碰撞的基本思想提出了针对iPMAC的伪造攻击。该攻击在已知输入输出对应关系的基础上寻找出一组新的对应关系。结果表明,该攻击经一次解密模型访问后成功伪造的概率为0.5。这一攻击同样适用于VPMAC。

关键词 消息认证,iPMAC,伪造攻击,VPMAC,认证加密
中图法分类号 TP309.7 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.03.041

Forgery Attack on Authenticated Cipher Mode iPMAC and VPMAC

TIAN Yu-dan[1] WEI Yong-zhuang[2,3]
(Guangxi Experiment Center of Information Sciences(Guilin University of Electronic Technology),Guilin 541004,China)[1]
(Guangxi Key Laboratory of Wireless Wideband Communication and Signal Processing
(Guilin University of Electronic Technology),Guilin 541004,China)[2]
(Guangxi Cooperative Innovation Center of Cloud Computing and Big Data(Guilin University of Electronics Technology),Guilin 541004,China)[3]

Abstract Message authentication has received the wide spread attention after being proposed. iPMAC and VPMAC become the representative of message authentication due to its parallel structure model. Whether iPMAC and VPMAC are secure become a research focus. Based on the variable parameter Γ and Λ, we put forward a new forgery attack by making use of the basic idea of the collision. Based on known relations, we found out a new set of corresponding relations. We created a successful forgery by making only one query to the decryption oracle with probability 0.5. This attack process also applies to VPMAC.

Keywords Message authentication, iPMAC, Forgery attack, VPMAC, Authenticated encryption

1 引言

1974年Gilbert等人首次提出了消息认证码[1](MAC)的概念,从而实现了消息完整性的认证。随后消息认证技术得到进一步发展,其中常见的构造方式有:基于流密码算法构造MAC、基于Hash函数构造MAC[2-3]、基于分组密码构造MAC[4](即CBC-MAC模式[5],CBC表示Cipher Block Chaining)。注意到,CBC-MAC模式只有计算出C_{i-1}后才能计算C_i(第i个密文分组),该模式的这一特点成为追求高速率的一个缺陷。2002年,为了克服CBC-MAC模式的缺陷,Black等人基于扭曲分组加密(TBC)体制提出了完全平行算法PMAC[6]。2009年,Sarkar在文献[7]中改进PMAC提出PMAC模式,VPMAC模式和PAE算法,其提出的模式采用面向字的混淆参数,比PMAC的效率更高。2013年,认证工作模式在CAESAR征集活动中得到广泛使用[8-10]。2015年,Debrup等人在文献[11]中提出了对PAE的攻击,分析表明:经一次解密模块访问成功实现伪造攻击的概率为0.5。那么iPMAC和VPMAC是否同样存在安全性问题成为了当前密码学界研究的热点。

本文通过分析iPMAC的基本模型,将输入参数作为突破口,利用碰撞的基本思想提出了针对iPMAC的伪造攻击。该攻击在已知输入输出对应关系(明文1、公开变量1、密文1、Tag)的基础上,删除最后的一个明文分组,使得参数(Γ和Λ)发生碰撞,寻找出一组新的有效对应关系(明文2、公开变量2、密文2、Tag')。结果表明:该攻击成功的概率为0.5,共使用一次解密模块访问。这一攻击过程同样适用于VPMAC。

到稿日期:2015-11-02 返修日期:2016-01-08 本文受国家自然科学基金项目(61572148),广西自然科学基金项目(2015GXNSFGA139007),广西高等学校优秀中青年骨干教师培养工程(第二期),桂林电子科技大学研究生创新项目(YJCXS201525)资助。
田玉丹(1990—),女,硕士生,主要研究方向为信息安全;韦永壮(1976—),男,博士,教授,主要研究方向为信息安全,E-mail:walker_wei@msn.com。

本文第 2 节对 iPMAC 的加密过程进行介绍；第 3 节简述伪造攻击的基本思想；第 4 节针对 iPMAC 提出伪造攻击；最后总结全文。

2　iPMAC 介绍[7]

2.1　iPMAC 参数介绍

π：$\{0,1\}^n$ 上均匀分布的矩阵；

ϕ：自定义线性映射，其输入为域 IF_{2^n} 上的变量，输出为域 IF_{2^n} 上的变量，并且该映射函数的最小多项式代数次数为 n；

N：n 位随机数；

Γ_i：混淆参数，$\Gamma_i=\phi_\gamma(i)$；

n：一个分组的字节长度；

r：明文最后一个分组的字节长度；

$len(x)$：二进制字符串 x 的长度；

$First_{n-1}(x)$：x 的前 $n-1$ 位；

Λ：若明文的最后一个分组为满分组，$\Lambda=0^n$；若明文的最后一个分组不是满分组，$\Lambda=\phi_\gamma(i)$；

$\gamma=\pi(N)$；

$\delta=\pi(\gamma)$。

2.2　Format(x,n)

函数 $Format(x,n)$：给定的明文字符串 x 经填充、转化后输出成 m 个 n 位分组，其中 $n\geqslant 1$，m 和 r 的值由 $len(x)$ 和 n 决定，具体步骤如下：

Format(x,n)

1. write len(x)=(m−1)n+r, where $1\leqslant r\leqslant n$;
2. if r<n, then set pad(x)=x ‖ 10^{n-r-1};
3. else set pad(x)=x;
4. format pad(x) into m blocks $x_1,\cdots,x_m$ each of length n;

return $(x_1,\cdots,x_m)$.

2.3　iPMAC 的模式描述

设 x 为二进制字符串(其中 $len(x)>n$)，$Format(x,n)$ 的输出为 $(P_1,\cdots P_m)$，将 $iPMAC_\pi$ 表示为映射：$iPMAC_\pi: x\mapsto C_m$。其具体过程如下：

$iPMAC_\pi(P)$：

1. $(N,P_1,\cdots,P_m)$=Format(P,n);
2. $\gamma=\pi(N)$;
3. for i=1,⋯,m, $\Gamma_i=\varphi_\gamma(i)$;
4. $(C_1,\cdots,C_{m-1})=ECB_\pi(P_1\oplus\Gamma_1,\cdots,P_{m-1}\oplus\Gamma_{m-1})$;
5. sum=$C_1\oplus\cdots\oplus C_{m-1}\oplus P_m$;
6. if(r<n)then sum=sum $\oplus\Gamma_m$;
7. if m=1, then
8. $\delta=\pi(\gamma)$; sum=sum $\oplus\delta$;
9. Tag=π(sum);
10. return Tag.

引理 1　设进行两次加解密模块访问：$iPMAC_\pi(N_1,P_1)$ 和 $iPMAC_\pi(N_2,P_2)$，如果这两次加密过程中使用相同的随机数 N，即 $N_1=N_2$，那么这两次加密过程中相同索引值 i 所对应的可变参数 Γ_i 相同。

证明：根据第 1 节对算法 $iPMAC_\pi$ 的描述可知，$\gamma=\pi(N)$，$\Gamma_i=\phi_\gamma(i)$。因此 $iPMAC_\pi(N_1,P_1)$ 对应的 $\Gamma_i=\phi_\gamma(i)=\phi_{\pi(N_1)}(i)$，$iPMAC_\pi(N_2,P_2)$ 对应的 $\Gamma_i=\phi_\gamma(i)=\phi_{\pi(N_2)}(i)$，又因为 $N_1=N_2$，所以两次加密过程具有相同的 Γ_i，且与明文无关。

3　伪造攻击的基本思想

2001 年，Brincat 等人在文献[12]中提出了一种攻击方法，即伪造攻击[13-14]，并给出了 3 种形式的伪造方式，其基本思想归纳为：在未知密钥情况下，假设攻击者已经知道某一对应关系，输入(明文 1、公开变量 1、相关数据 1)与输出(密文 1、认证标签 1)有效对应。那么，如果能够找到另一输入(明文 2、公开变量 2、相关数据 2)与输出(密文 2、认证标签 2)有效对应，而新的对应关系在已知对应关系的基础上没有增加新的未知变量，那么就称该伪造攻击有效。

4　对 iPMAC 的伪造攻击

设明文 P 可划分为 $m+1$ 个分组块，当加密 P_1-P_m 这 m 个明文时，根据第 1 节对 iPMAC 的介绍可知，可变参数 Γ_i 是由分组索引 i 和参数 γ 确定的，即 $\Gamma_i=\phi_\gamma(i)$；当加密最后一个分组 P_{m+1} 时，可变参数为 Λ，若明文的最后一个分组为满分组，则 $\Lambda=\phi_\gamma(i)$。由此可知存在 Γ_i 与 Λ 相等的可能性。根据模式的这种特性，本文设计攻击过程如下。

Step1　设明文 P 可划分为 $m+1$ 个分组，其加密过程如图 1 所示。设随机数为 N，输入明文 $P=(P_1\parallel\cdots\parallel P_{m-1}\parallel P_m\parallel P_{m+1})$(其中 $\Gamma_i=\phi_\gamma(i)$，$1\leqslant i\leqslant m$)，经 iPMAC 加密后输出为 (C,Tag)，其中 $C=(C_1\parallel\cdots\parallel C_{m-1}\parallel C_m\parallel C_{m+1})$。

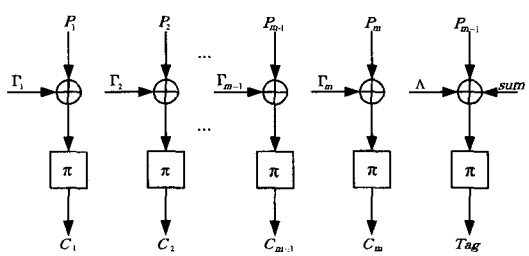

图 1　Step1 加密 $m+1$ 个明文的分组

Step2　如图 2 所示，N 保持不变，伪造 m 个分组的明文：$P'=(P_1\parallel P_2\parallel\cdots\parallel P_{m-1}\parallel First_{n-1}(C_1\oplus C_2\oplus\cdots\oplus C_{m-1}))$($P'$ 与 P 的前 $m-1$ 个分组相同，$\Gamma_i=\phi_\gamma(i)$，$1\leqslant i\leqslant m-1$)。那么，输出值为 (C',Tag')，其中 $C'=(C_1\parallel\cdots\parallel C_{m-1})$，$Tag'=C_m$。

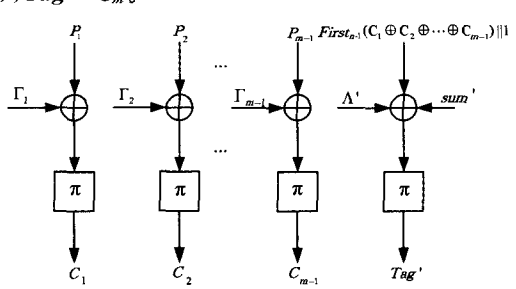

图 2　Step2 加密 m 个明文的分组

正确性分析如下。

根据第 1 节 $Format(x,n)$ 的生成原理可知，P 和 P' 生成的前 $m-1$ 个明文分组相同。Step1 和 Step2 这两次加密所使

用的随机数 N 相同，由引理 1 可知，所对应的 Γ_i（$1\leqslant i\leqslant m-1$）相同。综合以上两个条件可知，图 1 和图 2 这两次加密过程中前 $m-1$ 个分组的加密过程完全相同，因此所得到的密文 C_i 对应相同，即 $C'=(C_1\parallel\cdots\parallel C_{m-1})$。

在 Step2 中，因为 P 的最后一个明文分组只有 $n-1$ 位（不是满分组），根据第 1 节对参数 Λ 的介绍可知，$\Lambda'=\phi_\gamma(m)$，又因为 Step1 中 $\Gamma_m=\phi_\gamma(m)$，因此 $\Gamma_m=\Lambda'$。

由 Step1 可知：$C_m=\pi(\Gamma_m\oplus P_m)$。

由 Step2 和 $Format(x,n)$ 的填充原理得：

$$\begin{aligned}Tag'&=\pi(\Lambda'\oplus(First_{n-1}(C_1\oplus C_2\oplus\cdots\oplus C_{m-1})\parallel 1)\oplus sum')\\&=\pi(\Lambda'\oplus(First_{n-1}(C_1\oplus C_2\oplus\cdots\oplus C_{m-1})\parallel 1)\oplus P_m\oplus C_1\oplus C_2\oplus\cdots\oplus C_{m-1})\end{aligned}$$

假设 $P_m\oplus C_1\oplus C_2\oplus\cdots\oplus C_{m-1}$ 的最后一位为 1，那么根据 iPMAC 模式的结构原理可知：

$$\begin{aligned}Tag'&=\pi(\Lambda'\oplus(First_{n-1}(C_1\oplus C_2\oplus\cdots\oplus C_{m-1})\parallel 1)\oplus sum')\\&=\pi(\Lambda'\oplus(C_1\oplus C_2\oplus\cdots\oplus C_{m-1})\oplus P_m\oplus C_1\oplus C_2\oplus\cdots\oplus C_{m-1})\\&=\pi(\Lambda'\oplus P_m)\end{aligned}$$

因为 $\Gamma_m=\Lambda'$，所以 $Tag'=\pi(\Gamma_m\oplus P_m)=C_m$。

$C_1\oplus C_2\oplus\cdots\oplus C_{m-1}$ 的最后一位为 1 的概率为 0.5，因此该伪造攻击成功的概率为 0.5，共使用一次解密访问。证毕。

因为 iPMAC 和 VPMAC 具有相同的结构特点，所以以上攻击方法同样适用于 VPMAC。

结束语 针对 iPMAC 模式的结构特点提出伪造攻击。iPMAC 的输入使用可变参数 Γ 和 Λ，在一定程度上增强了模式的安全性。控制随机数 N 不变，利用 Γ 和 Λ 在一定情况下相等这一特点提出攻击，使得可变参数相互抵消，得到一组新的有效对应关系（明文，密文，标签）。通过一次解密模块访问，即可实现对 iPMAC 的伪造攻击，成功伪造的概率为 0.5。因为 iPMAC 和 VPMAC 使用相同的加密模型，所以本文提出的伪造攻击过程同样适用于 VPMAC。

参 考 文 献

[1] GILBERT E, MACWILLIAMS F, SLOANE N. Codes which detect deception[J]. Bell System Technical Journal, 1974, 53(3): 405-424.

[2] PRENEEL B, VAN P Oorschot. MD-x MAC and building fast MACs from hash functions[C]// Advances in Cryptology-Crypto 95 Proceedings. Lecture Notes in Computer Science, Vol. 963, D. Coppersmith ed., Springer-Verlag, 1995.

[3] "Secure Hash Standard". Federal Information Processing Standards Publication 180-1[J]. Us Dept of Commerce/nist National Technical Information Service, 1995.

[4] WANG P, FENG D G. To construct the MAC based on block cipher [J]. Graduate School of Chinese Academy of Sciences Journa, 2005, 22(6): 746-750. (in Chinese)
王鹏，冯登国. 基于可调分组密码的 MAC 构造[J]. 中国科学院研究生院学报，2005，22(6)：746-750.

[5] ISO/IEC 9797-1. Information technology-security techniques message authentication code (MACs)-part 1: Mechanism using a block cipher[S]. International organization for standardization. geneve, swizerland, 1999.

[6] BLACK J, ROGAWAY P. A block-cipher mode of operation for parallelizable message authentication[M] // Lecture Notes in Computer Science 2332: Advances in cryptology-eurocrypt. 2002: 384-397.

[7] SARKAR P. Pseudo-random functions and parallelizable modes of operations of a block cipher[J]. IEEE Transactions on Information Theory, 2010, 56(8): 4025-4037.

[8] CAESAR-competition for authenticated encryption: security, applicability, and robustness[OL]. http://competitions.cr.yp.to/caesar.html.

[9] NASOUR B, JAVAD A, MOHAMMAD R. A single query forgery on avalanchev1[R]. Cryptographic Competitions Mailing List, 2014.

[10] GUY B. Forgery on stateless cmcc[OL]. http://eprint.iacr.org.

[11] CHAKRABORTY D, NANDI M. Attacks on the authenticated encryption mode of operation PAE[J]. IEEE Transaction on Information Theory, 2015, 61(10): 5636-5642.

[12] BRINCAT K, MITCHELL C. New CBC-MAC forgery attacks [C]// varadharajan, V, Mu, Y. (eds.) ACISP 2001. LNCS, Springer, Heidelberg, 2119: 3-14.

[13] CHEN J, HU Y P, WEI Y Z. A random message forgery attack on PMAC and TMAC-V[J]. Chinese Journal of Computers, 2007, 30(10): 1827-1832. (in Chinese)
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.

[14] CHAO S D, ZHANG Z L, TIAN H, et al. Improved PMAC and security analysis[J]. Computer Engineering and Applications, 2009, 45(21): 77-78. (in Chinese)
晁仕德，张绍兰，田华，等. 改进的 PMAC 及安全性分析[J]. 计算机工程与应用，2009，45(21)：77-78.

（上接第 181 页）

[12] YIN X L, QI W D. LiteST: a lightweight secure time synchronization protocol for wireless sensor networks [J]. Journal on Communations, 2009, 30(4): 74-85. (in Chinese)
尹香兰，齐望东. LiteST：一种无线传感器网络轻量级安全时间同步协议[J]. 通信学报，2009，30(4)：74-85.

[13] GANERIWAL S, PÖPPER C, ČAPKUN S, et al. Secure time synchronization in sensor networks[J]. ACM Transactions on Information and System Security (TISSEC), 2008, 11(4): 23.

[14] THUBERT P, WATTEYNE T, PALATTELLA M R, et al. IETF 6TSCH: Combining IPv6 Connectivity with Industrial Performance[J]. Seventh International Conference on Innovative Mobile & Internet Services in Ubiquitous Computing, 2013, 395(6): 541-546.

[15] LUO J, LIU X, FAN M. A trust model based on fuzzy recommendation for mobile ad-hoc networks[J]. Computer Networks, 2009, 53(14): 2396-2407.