文章编号：1008-0562(2006)05-0741-03

基于 Logistic 映射和 Rijndael 改进型 MAC 算法

刘鸿雁，吴恒柏

（鞍山科技大学 电子与信息工程学院 ，辽宁 鞍山 114044）

摘 要：为增强消息认证码（MAC）算法的安全性，将 Rijndael 作为消息认证码的反馈分组加密算法,取代原有的 DES。该算法用 Logistic 映射初值作为种子密钥生成混沌序列，对该序列进行域值量化得到二进制密钥流，对其分组作为 Rijndael 算法的初始密钥，给出了改进型 MAC 算法模型，经分析可知，该算法减少了密钥种子字节数，实现了一次一密，增加了攻击 MAC 的困难程度，可以提供更安全的认证功能。

关键词：Logistic 映射；Rijndael；MAC；算法

中图分类号：TP 273; O 244 **文献标识法**：A

Improved MAC algorithm based on Logistic map and Rijndael

LIU Hong-yan，WU Heng-bai

(School of Electronic and Information Engineering,Anshan University of Science and Technology, Anshan 114044,China)

Abstract: In order to strengthen the security of Message Authentication Code (MAC) algorithm, Rijndael algorithm is applied as the feedback and block encryption algorithm of MAC instead of the DES. By using initial values of Logistic Map as the CipherKey seeds to create chaotic sequences and then carrying on quantification with its proper region value, the binary system CipherKey streams can be obtained. The initial CipherKey of Rijndael can be produced by dividing the binary streams into groups. The improved MAC algorithm model is described. By analysis, the number of bytes of Rijndael CipherKey seeds is decreased, one-time-pad is realized with the algorithm. It can offer safer authentification and make attacking of MAC more difficult.

Key words: logistic map; Rijndael; MAC; algorithm

0 引 言

认证（Authentication）又称鉴别、确认，它是证实某事是否名副其实或是否有效的一个过程，认证往往是许多应用系统中安全保护的第一道防线。消息认证是用以确保报文发送者和接收者的真实性以及报文的完整性，阻止对手的主动攻击，如冒充、篡改、重播等。消息认证码(Message Authentication Code，简称 MAC)是通信双方报文内容认证的一个重要方法，通过验证 MAC,能使接收方确认报文内容的真实性。Rijndael 是 2001 年美国新的高级加密标准(AES)，它的密钥建立时间短，灵敏性好。Rijndael 对内存需求低[1]，对恶意攻击和时间选择攻击抵抗能力强，目前不可破解[1]。混沌现象是非线性动态系统中出现的确定的伪随机过程，对初始条件极端敏感，用混沌系统调制的数据具有高度的保密性。本文研究将 Rijndael 及 Logistic 映射生成初始密钥应用于 MAC 算法之中，提高 MAC 算法的认证功能。

1 消息认证码

消息认证码（MAC）是消息内容和秘密钥的公开函数，其输出是固定长度的短数据块

$$MAC = C(M, K) \qquad (1)$$

假定通信双方共享秘密钥为 K。若发送方 A 向接收方 B 发送报文 M 和 MAC，接收方 B 按秘密钥和公开函数自行计算 MAC，并将其与接收到的 MAC 进行比较。若两者相等，则接收方 B 可以相信报文未被修改，并且报文来自认定的发送方 A。如果报文 M 被其恶意篡改，接收方 B 根据接收到的信息计算产生的 MAC 必定会发生改变，接收方 B 可认定报文已被篡改。

收稿日期：2005-10-26

基金项目：国家自然科学基金资助项目（50574048）

作者简介：刘鸿雁（1963-），女，博士研究生，教授，主要从事数据挖掘、信息安全、人工智能方面的研究。**本文编校**：杨瑞华

从理论上讲，对不同报文 M，产的认证码 MAC 也不同。实际应用时要求函数 C 具有以下性质：

（1）对已知报文 M_1 和 $C(M_1,K)$，构造满足 $C(M_2,K)=C(M_1,K)$ 的报文 M_2 在计算上是不可行的；

（2）$C(M,K)$ 应是均匀分布的，即对任何随机选择的报文 M_1 和 M_2，$C(M_1,K)=C(M_2,K)$ 的概率是 2^{-n}，其中 n 是 MAC 的位数；

（3）设 M_2 是 M_1 的某个已知的变换，即 $M_2=f(M_1)$，那么 $C(M_1,K)=C(M_2,K)$ 的概率是 2^{-n}。

2 构架基于 Rijndael 的 MAC 算法

基于数据加密标准 DES 的 MAC 算法是目前广泛使用的消息认证码算法之一。DES 作为 20 世纪 70 年代的加密标准，其加密强度越来越不能满足人们的要求。DES 的密钥长度只有 56 bit，随着计算能力的不断提高，利用穷搜索的方法攻击 DES 是完全可能的。特别是在政府或者组织的支持下，设计专门的硬件来攻击 DES 已经是容易的事情，基于 DES 的 MAC 算法安全性受到前所未有的威胁。Rijndael 算法是取代 DES 的新一代高级加密标准，它具有极高的安全性，对各种攻击有很强的免疫力。构建基于 Rijndael 的 MAC 算法，可以满足上面函数 C 的性质，为报文提供更安全的认证功能。用 Rijndael 运算的密文反馈分组链接(CBC)方式[2]，需认证的数据可按分组加密算法分成若干个大小为 128 位的数据块 $D_1\|D_2\|\ldots\|D_N$，若最后分组不足 128 位，则在其后填 0 补足。

Rijndael 算法的子密钥前 16 个字节是完全由种子密钥填充而成的，这样虽然提高了密钥的离散性，但是雪崩效应相应减弱，同时它的轮密钥是通过递归运算生成的，即可由前一轮或几轮的密钥推出某一轮的密钥。当密钥信息的泄漏达到一定的临界线时，其他的种子密钥有极大的概率通过某种攻击法获得，进而获得全部轮子密钥，从而可以译出明文。用 Logistic 映射初值作为种子密钥生成混沌序列，并进行量化得到初始密钥，可减少生成初始密钥的种子密钥字节数，增加密钥安全性。

3 映射初值作密钥种子产生初始密钥

混沌现象是一种确定性的、类随机过程，对初始状态具有蝴蝶效应，即初始状态有微小变化，两个同构混沌系统就会产生两组完全不同的混沌序列。混沌序列具有天然随机性，蕴含大量不稳定的周期信号，使其可以被利用作为具有很高安全性的序列密码。混沌系统对初始状态具有极端敏感性，可以提供数量庞大的初始密钥。所以可以利用混沌系统产生序列密钥作为 Rijndael 的初始密钥[3-4]。

Rijndael 算法中初始密钥是固定不变的，对每组明文都采用相同的初始密钥进行加密。如果希望变换初始密钥以增强抗破译性，接收端和发送端的初始密钥同步将会存在问题。利用 Logistic 映射生成的密钥流作为初始密钥可以解决这个问题。

Logistic 映射是一个离散混沌系统，它的映射关系为：$x_{n+1}=ux_n(1-x_n)$。其中 u 为控制参量且 $u\in(0,4)$，若初始条件 $x_0\in[0,1]$。当 $0<u\leqslant 3$ 时，迭代后的值为稳定不动点；当 u 逐渐增大时，出现倍周期分岔现象，当 $3.569945673<u\leqslant 4$ 时，该映射处于混沌状态，所以可以选择 u 在这个范围内的一个值产生混沌序列 $\{x_n,n=0,1,2,3\ldots\}$[6]。

定义一个域值函数 θ，对 Logistic 产生的混沌序列 $\{x_n,n=0,1,2,3\ldots\}$ 进行量化，得到二进制密钥流序列：

$$\theta(x_n)=\begin{cases}0, 0\leq x_n<0.5\\ 1, 0.5\leq x_n\leq 1\end{cases} \qquad (2)$$

则二进制序列 $\{\theta(x_n),n=0,1,2,3\ldots\}$ 经分组可作为 Rijndael 算法的初始密钥。这里我们把二进制序列按 128 位分组来构造 Rijndael 算法的初始密钥 $K_i(1\leqslant i\leqslant N)$，其中 N 为正整数。采用 Logistic 映射后，只要已知 2 个初值的密钥种子（x_0 和 u），就可以产生足够多的初始密钥，初始密钥不再由密钥种子填充。若不用 Logistic 映射，每次加密需要选取 16 字节的密钥种子，此时密钥种子就是初始密钥，变换初始密钥以增强抗破译性时就需要更多的密钥种子。Logistic 映射产生的混沌序列作初始密钥可实现一次一密的思想。该混沌序列使密钥具有不规则性和难以预测性，克服了 Rijndael 算法容易暴露子密钥的缺点，起到了隔离作用，具备抵抗线性、差分和穷举攻击的能力。采用这种方案的 MAC 算法具有更高的密钥安全性。

4 改进的 MAC 算法描述

在接收端和发送端构造参数相同的 Logistic 映射，只要初始值相同，映射产生的混沌序列也相同。

对相同初值产生混沌序列进行量化即可得到相同的初始密钥，使接收端和发送端的初始密钥同步。

改进的 MAC 中，每轮都是截取二进制序列流 $\{x_n, n=0,1,2,3...\}$ 的 128 位作为 Rijndael 的初始密钥，并重新扩展 10 轮 Rijndael 的子密钥对报文加密。改进的 MAC 函数可描述如下

$$MAC = C(M, x_0, u) \qquad (3)$$

式中，x_0 和 u 是双方共享的秘密钥种子，也是 Logistic 映射的初始输入量。图 1 给出基于 Rijndael 的消息认证码的计算流程，其中 IV 为初始向量，此处可取为 0。

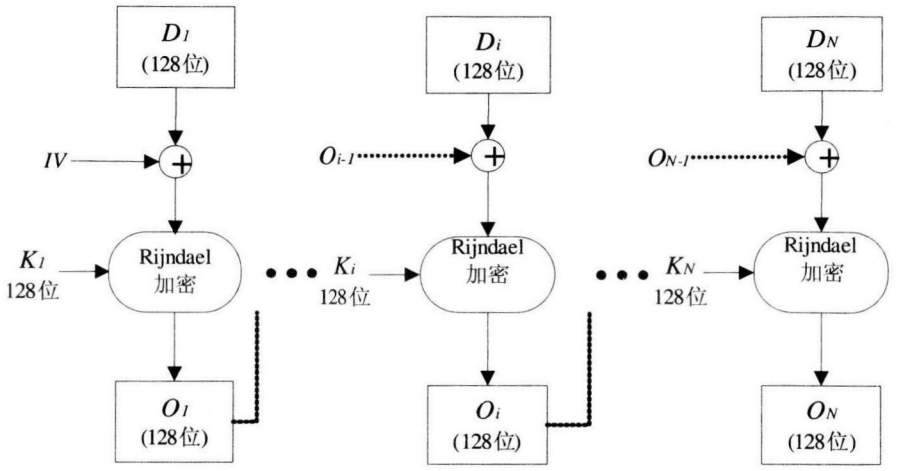

图 1　基于 Logistic 映射和 Rijndael 的改进型 MAC 算法

Fig.1 improved MAC algorithm based on Logistic map and Rijndael

该 MAC 算法的 128 位密钥输入 K，（$1 \leqslant I \leqslant N$）被分为 16 个字节，作为 MAC 每轮的 128 位密钥输入。

改进型 MAC 中，初始密钥由种子密钥经过 Logistic 映射产生，不再由种子密钥直接填充。攻击者得到种子密钥更加困难，改进型 MAC 具有可靠的认证功能。

5　结　语

本文利用 Logistic 映射初值作为种子密钥生成混沌序列经量化后作为 MAC 算法中 Rijndael 的初始密钥，实现了一次一密的加密思想，减少密钥种子字节数，使得 MAC 算法软硬件具备更强的抵抗穷举攻击的能力，克服了 Rijndael 算法密钥扩展方案容易暴露种子密钥的缺点。进一步增加了 MAC 算法初始密钥混淆程度，提高了抵抗线性分析和差分分析的能力[5]。改进后的 MAC 算法使得算法求逆更加困难，确保报文认证的真实性和安全性。

参考文献：

[1] Joan Daemen, Vincent Rijmen. AES Proposal: Rijndael[EB/OL] .http://www.east.Kuleuven.ac.be/~rijndae/rijndael,1999-10-05.

[2] Black J,Rogaway P. CBCMACs for arbitrary-length messages: the three-key constructions, full version of paper from advances in cryptology-CRYPTO'00[J].Lecture Notes in Computer Science,2000, 101:100-214.

[3] GHOBAD HEIDARI-BATENI, CLARED. MCGlem. A Chaos Direct Sequence Spread-spectrum Communication System[J].IEEE Trans. Commun,1994,42(2)：1524-1527.

[4] TOHRU KOHDA,AKIO TSUNEDA. Pseudonoise Sequences by Chaotic Nonlinear Maps and Their Correlation Properties[J].EICE Trans.Commun,1993,E76-B-(8)：855-861.

[5] Gilbert H, Minier M. A Collision Attack on 7 Rounds of Rijndael[C]//The Third Advanced Encryption Standard Candidate Conference. Gaithersburg: NIST, 2000: 230-241.

[6] 杨皎平,高雷阜,赵宏霞.多极值函数的混沌优化法[J].辽宁工程技术大学学报,2004,23(5):711-714.