第 34 卷 第 8 期 计 算 机 工 程 2008 年 4 月
Vol.34 No.8 Computer Engineering April 2008
·安全技术· 文章编号：1000—3428(2008)08—0132—03 文献标识码：A 中图分类号：TP309

基于双密钥的对称加密方案

徐江峰，赵 峰
(郑州大学信息工程学院，郑州 450001)

摘 要：在对混沌加密和传统加密特性进行分析的基础上，该文提出一个基于双密钥的对称加密方案，该方案通过一个对密钥极其敏感的函数及一个公开的动态密钥，可以实现类似于“一次一密”的加密目标。给出一个基于 Lorenz 混沌系统的实现方案，理论分析和实验结果表明，该方案可以提高传统加密方案的安全性能，并且实现简单。

关键词：双密钥；混沌；对称加密；敏感函数

Symmetric Encryption Scheme Based on Two Symmetric-keys

XU Jiang-feng, ZHAO Feng
(School of Information and Engineering, Zhengzhou University, Zhengzhou 450001)

【Abstract】 Symmetric encryption scheme is proposed based on two symmetric-keys. By mean of a very sensitive function with a private key and a changeable “public key”, the proposed scheme has a function similar to one-time pad scheme. Using a Lorenz system with mode function illustrates how to realize such encryption scheme. Theoretical analysis and experimental results demonstrate that the new scheme can increase the security of traditional encryption scheme and be easy to be realized.

【Key words】 two symmetric-keys; chaos; symmetric encryption; sensitive function

1 概述

加密技术作为安全通信的重要手段，应用越来越广泛。传统的数据加密分为对称加密和非对称加密两大类。对称加密的通信双方使用相同的密钥，而非对称加密则使用不同的密钥。由于非对称加密的安全性主要依赖难解的数学问题，密钥的长度比对称加密大得多，因此加密效率较低，主要使用在身份认证、数字签名等领域。而对称加密由于加密速度快、硬件容易实现、安全强度高，因此仍被广泛用来加密各种信息。但对称加密也存在着固有的缺点：密钥更换困难，经常使用同一密钥进行数据加密，给攻击者提供了攻击密钥的信息和时间。

基于混沌的加密技术自 1989 年由Matthews[1]提出后，得到了不断发展[2-7]。与传统的加密技术相比，混沌系统有许多优越的特性，如传统的加密方案要求密文对密钥是敏感的，而混沌系统则具有对初始条件和参数的极度敏感、类随机、不可预测等特性；传统加密方案通过迭代实现数据的混淆与扩散，而离散混沌系统通过迭代可以把初始区域扩散到整个相空间[8]。此外，混沌系统的参数和初始条件均可以作为密钥，具有很大的密钥空间。

本文提出了一个基于双密钥的对称加密方案，通信双方使用 2 个密钥进行加密和解密，一个是只有通信双方才有的私钥，另一个是可以公开的“公钥”。两个密钥通过一个敏感函数产生新的加密密钥或密钥序列，从而实现类似于“一次一密”的加密目标。实验结果和分析表明，通过混沌系统可以得到性能良好的敏感函数，提高传统加密方案的安全性。

2 基于双密钥的加密方案

与传统的对称加密方案相比，新的加密方案多了一个动态密钥。通信双方除了使用只有双方才知道的私钥外，还使用一个可以公开的动态密钥。动态密钥的主要作用是用来改变传统对称加密方案中密钥的不变性，并通过敏感函数产生“随机”的密钥或密钥流，使密文与明文之间的相关性不断发生变化，增强系统的安全性能。方案的结构如图 1 所示。

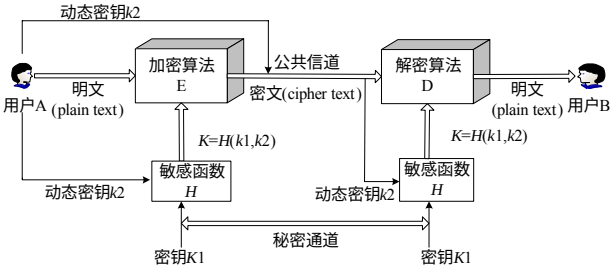

图 1 双密钥加密方案结构

在上述方案中，私钥 $k1$ 仍然需要通过专用通道或人工方式进行交换或协商，而 $k2$ 则由用户 A 在加密时随机选定，并同密文一起通过公共信道传送给用户 B。

在用户 A 和用户 B 确定了加密算法 E、解密算法 D 及私钥 $k1$ 之后，该方案的执行步骤如下：

(1)用户 A 输入明文 M；

(2)用户 A 选择一个动态密钥 $k2$，并计算 $K=H(k1,k2)$；

(3)用户 A 利用加密算法 E、密钥或密钥流 K 加密明文 M，得到密文 $C=E(K,M)$；

(4)用户 A 把密文 C 及动态密钥 $k2$ 发送给用户 B；

(5)用户 B 接收密文 C 及动态密钥 $k2$；

(6)用户 B 根据得到的动态密钥 $k2$ 及私钥 $k1$，计算 $K=H(k1,k2)$；

基金项目：河南省教委自然科学基金资助项目(2006520014)
作者简介：徐江峰(1965－)，男，副教授、博士，主研方向：信息安全，混沌加密通信；赵 峰，讲师
收稿日期：2007-04-30 **E-mail：**jfxu@zzu.edu.cn

(7)用户 B 利用解密算法 D 和计算出的密钥(密钥流)K 对密文 C 进行解密，得到明文 $M=D(C,K)$。

在上述方案中，密钥 $k1,k2$ 应满足下述条件：

(1)$k1$ 与 $k2$ 无关，即 $k2$ 的选择对 $k1$ 没有任何影响，不管给出多少个 $k2$ 的值都不可能由 $k2$ 得出 $k1$，反之也成立；

(2)函数 H 对 $k1, k2$ 是敏感的，即 $k1$ 或 $k2$ 的微小变化，将造成 K 值的巨大改变。

3 方案的安全性分析

基于“一次一密密码本”(one-time pad)的加密方案是绝对安全的，因为密码本中的密钥流是真随机产生的，并且每个密钥流只能使用一次，一个密文对所有可能的明文都是等概率的，所以攻击者得到密文后对明文的猜测与没有密文时相比，并没有增加任何知识[9]。

新的方案虽然不属于传统的“一次一密密码本”，但是通过动态改变密钥$k2$ 的值，可以实现类似于“一次一密”的加密目标。实际上，如果函数H满足对$k1$ 和$k2$ 单射性质，即当 $k1\neq k1'$ 或 $k2\neq k2'$ 时，$H(k1,k2)\neq H(k1',k2')$，则可以实现真正的“一次一密”，系统的安全性最高。

如果 H 对 $k1, k2$ 是敏感的，即 $k1, k2$ 的微小改变，$K=H(k1,k2)$都产生巨大的变化，则系统可以提高原加密方案的安全性能。因为密钥的不断变化，将使密文与明文的关联度极大降低，从而使基于统计分析的攻击变得困难或不可行。

在特殊情况下，如果 $K=H(k1,k2)= k1$，即 H 与 $k2$ 无关，此时该方案退化成了传统的对称加密方案，则系统的安全性将是原加密方案的安全性。

综上所述，采用新方案将会提高所选用的加密和解密算法的安全性，并且函数 H 对 $k1$ 及 $k2$ 越敏感，方案的安全性越高。

4 基于混沌的双密钥加密方案

为进一步说明上述方案的有效性和安全性，下面给出一个基于 Lorenz 混沌系统的双密钥加密方案，并对模拟实验结果进行研究和分析。

4.1 基于 Lorenz 混沌系统的双密钥加密算法

Lorenz混沌系统是美国著名气象学家Lorenz在 1963 年提出的[10]，是第 1 个混沌的物理和数学模型。从文献[11]中可以知道，该系统对初始条件非常敏感，当初始条件变化只有10^{-15}时，系统运行轨迹的偏差可以达到-30~30，是初始条件误差的 10^{16}倍。因此该系统非常适合用来生成敏感函数H。

在下面的实验及分析中，敏感函数 H 定义为

$$H(k1,k2)=\mathrm{mod}(\mathrm{abs}(\mathrm{round}(F_{k1,T}(t)\times k2)),256) \tag{1}$$

其中，$k1$ 为混沌系统初始条件；$k2$ 为动态密钥；T为采样规则；$F_{k1,T}(t)$为采样后的混沌信号；mod是求余运算；abs是求绝对值运算；round是四舍五入运算。

依据上述定义，函数 H 的输出结果是一个取值在[0,255]的整数序列，适合于流加密。为了便于分析新方案的特性，加密算法 E 选取简单的流加密算法，密文 C 由密钥流 $K=H(k1,k2)$与明文 M 异或得到，即 $C=E(K,M)=K\oplus M$。

基于混沌的双密钥加密方案可以描述如下：

(1)用户 A 输入明文 M。

(2)用户A用初始条件$k1$ 和Lorenz混沌系统产生混沌信号$F_{k1}(t)$，并保证它的长度足够加密明文。

(3)用户A选择动态密钥$k2$，并与采样规则T一起对$F_{k1}(t)$进行采样处理，得到加密用的混沌信号$F_{k1,T}(t)$。

(4)用户A利用$F_{k1,T}(t)$和$k2$，由函数H生成密钥序列K。

(5)用户 A 把 K 与 M 进行运算，得到密文 $C=K\oplus M$。

(6)用户 A 把密文 C 和动态密钥 $k2$ 发送给用户 B。

解密方案是加密方案的逆运算，只要用户 B 正确产生密钥流 K，并与 C 异或即可得到明文 M。

4.2 实验结果及分析

在上述方案中，由于加密和解密算法简单，系统的安全性完全由私钥 $k1$、动态密钥 $k2$、混沌采样规则 T 和敏感函数 H 确定。如果系统要具有高的安全性能，以上参数应该满足下面的几个要求：

(1)函数 H 对密钥 $k1$ 和 $k2$ 敏感，使得统计分析不可行。

(2)私钥 $k1$、采样规则 T 和函数 H 组成的密钥空间足够大，使穷举攻击不可行。

(3)动态密钥 $k2$ 有充分的选择空间，使得用户 A 在每次加密时可以选择不同的 $k2$，实现“一次一密”的加密。

(4)密钥序列中各元素分布是均匀的，以使密文中各元素能均匀分布。

针对上述要求，本文进行了多次试验，并对实验数据进行了分析。

4.2.1 函数 H 对密钥 $k1$ 的敏感性

根据 4.1 节中的加密算法，函数H产生的是一个密钥序列。设密钥序列的长度为n，$H_i(k1,k2)$表示$H(k1,k2)$的第i个元素，$\Delta k1$为$k1$ 的误差，序列$s=\{s(1), s(2),\cdots,s(n)\}$为

$$s(i)=\begin{cases}0 & \text{若 } H_i(k1,k2)=H_i(k1+\Delta k1,k2)\\ 1 & \text{否 则}\end{cases} \tag{2}$$

显然，序列 s 描述了 $H(k1+\Delta k1, k2)$ 与 $H(k1,k2)$对应位置元素的变化情况。

因此，参数

$$p=\frac{\sum_{i=1}^{n}s(i)}{n}\times 100\% \tag{3}$$

反映了在 $k1$ 发生误差 $\Delta k1$ 时，由 H 产生的混沌序列中发生变化的元素占序列元素总数的百分比。该参数可以很好地说明 H 对 $k1$ 的敏感程度。

由于$k1$ 是混沌系统的初始条件，因此对 $\Delta k1$ 分别取值 $10^{-1}, 10^{-3},\cdots,10^{-15}$，并进行了实验，实验结果见表 1。

表 1 函数 H 对密钥 $k1$ 的敏感性

$\Delta k1$	p/(%)
10^{-1}	99.57
10^{-3}	99.60
10^{-5}	99.63
10^{-7}	99.56
10^{-9}	99.58
10^{-10}	99.54
10^{-11}	99.56
10^{-12}	99.68
10^{-13}	99.63
10^{-14}	99.66
10^{-15}	99.52

4.2.2 函数 H 对密钥 $k2$ 敏感性

在 4.2.1 的分析中，H 的取值是[0, 255]中的整数，$k1$ 的微小改变造成了 H 值 99.5%以上发生了变化。而传统的加密分析都是对二进制数据进行，为便于对比，本节对 H 的二进制表示进行分析。该结果同样适用与 H 对 $k1$ 的敏感性分析。

H 对 $k2$ 的敏感性，同样以参数 p 作为评价指标，但序列 s 定义为

$$s(i)=\begin{cases}0 & \text{若}H_i(k1,k2)=H_i(k1,k2+\Delta k2)\\ 1 & \text{否则}\end{cases} \tag{4}$$

其中，$H_i(k1,k2)$, $H_i(k1,k2+\Delta k2)$ 分别表示 $H(k1,k2)$ 和 $H(k1,k2+\Delta k2)$ 转换为二进制后的第 i 个元素。实验结果见

表 2。

表 2　函数 H 对密钥 *k*2 的敏感性

Δ*k*1	*p*/(%)
10	46.81
20	49.13
30	49.27
40	51.82
50	50.49
60	49.72
70	51.07
80	50.81
90	51.28
100	51.90

从测试结果可以看出，无论是十进制还是二进制表示，函数 *H* 对 *k*1 和 *k*2 都是极其敏感的。当 *k*1, *k*2 有微小改变时，*H* 的十进制表示有 99.5% 以上的元素发生改变，二进制表示平均有 49.8%的值发生了变化，充分实现了 Shannon 信息论中提出的混淆特性。另一方面，从表 1 还可以看出，混沌初始条件中的每一位对加密都是有效的，并且它们的变化与密钥流的改变并不存在明显的关系，攻击者要想根据参数 *p* 的值来判断密钥的误差是很困难的。因此，*k*1 和 *k*2 可以很好地用来产生密钥序列。

5　结束语

本文提出了一个基于双密钥和敏感函数的对称加密新方案，给出了一个基于 Lorenz 混沌系统的实现方案。理论分析和实验结果表明，当私钥 *k*1(Lorenz 混沌系统的初始条件)或动态密钥 *k*2 发生极小的改变，由敏感函数产生的密钥序列将发生巨大的变化。所以，加密者通过改变动态密钥使得每次加密都用不同的密钥流，从而实现类似于“一次一密”的加密目标。

参考文献

[1] Matthews R. On the Derivation of a Chaotic Encryption Algorithm[J]. Cryptologia, 1989, 8(1): 29-42.

[2] Dachselt F, Schwarz W. Chaos and Cryptography[J]. IEEE Trans. on Circuits and Systems I, 2001, 48(12): 1498-1509.

[3] Jakimoski G, Kocarev L. Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps[J]. IEEE Trans. on Circuits and Systems I, 2001, 48(2): 163-169.

[4] 付生猛, 陈朝阳, 周亚安. 基于混沌映射的随机数产生器[J]. 计算机研究与发展, 2004, 41(4): 749-754.

[5] Min Lequn, Zhang Xianhua, Yang Miao. Secure Communication by Generalized Chaotic Synchronization[J]. J. Univ. Sci. Technol. Beijing, 2003, 10(2): 74-78.

[6] Xu Jiangfeng, Min Lequn. A Chaotic Communication Scheme Based on Generalized Synchronization and Hash Functions[J]. Chinese Physics Letters, 2004, 21(8): 1445-1448.

[7] 徐江峰, 杨　有, 黄小粟. 基于广义同步混沌的图像加密方案[J]. 计算机工程, 2006, 32(6): 154-156.

[8] Chen Guanrong, Mao Yaobin. A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps[J]. Chaos, Solitons and Fractals, 2004, 21(3): 749-761.

[9] Shannon C E. Communication Theory of Secrecy System[J]. Bell System Technical Journal, 1949, 28(4): 656-715.

[10] Lorenz E N. 混沌的本质[M]. 北京: 气象出版社, 1997.

[11] 徐江峰, 尚　晋, 胡　静. 基于连续混沌系统和 Hash 函数的图像加密算法[J]. 计算机应用, 2004, 24(12): 61-63.

(上接第 129 页)

哈希表、事务队列。按照实际需要，事务工作区记录了事务的主要参数，如状态、事务 ID、定时器，还维护了哈希表冲突指针(p_hash)和保存的事务结构指针(p_trans)。当哈希表发生冲突时，保存的事务结构指针与哈希冲突指针就指向同一个位置；事务哈希表两张，分别记录发送事务和接收事务；事务队列两个，分别记录与应用层交互的两个方向的事务，如图 4 所示。

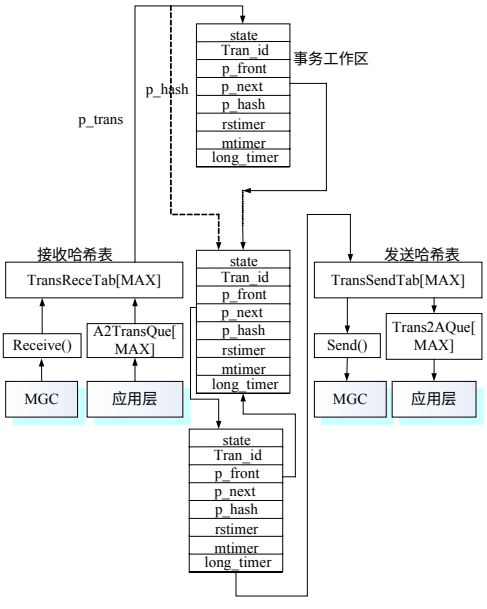

图 4　数据结构实现

5　测试结果分析

在媒体网关软件系统正式运行前，笔者进行了一些模拟测试。用一台主机作为 MG，另一台主机作为 MGC 进行 H.248 基本通信。

结果表明，定时器工作正常，事务传输准确无误，每秒钟平均处理 95 条信令消息(这与ASN.1 编解码模块处理速度有关)，达到了预期的目标[4]。目前，媒体网关在实验室运行良好。

6　结束语

随着 PSTN 和 IP 网的不断融合，作为软交换与媒体网关通信的 H.248 协议也显得越来越重要。如何在基于 IP 的分组交换网上实现可靠传输已经成为该协议在 NGN 中部署的关键技术。本文分析了基于 IP 的分组网络的特点及 H.248 协议在可靠传输需求，在此基础上提出了一种可靠传输解决方案，并进行了初步实现，结果表明该设计方案是可行的并保证了传输效率，它对其他网络设备的可靠传输处理有一定的借鉴意义。

参考文献

[1] 糜正琨. 软交换组网与业务[M]. 北京: 人民邮电出版社, 2005.

[2] Groves C, Pantaleo M, Anderson T, et al. Gateway Control Protocol Version 1[S]. RFC3015, 2003.

[3] 中国电信集团. H.248 标准[S]. 2003.

[4] 信息产业部传输所. 中华人民共和国通信行业标准——软交换设备总体技术要求(草案)[Z]. 2001.