带延迟的分组密码算法密钥结合模式设计

罗 岚，瞿泽辉，周世杰，张凤荔，秦志光，魏正耀

(电子科技大学计算机科学与技术学院 成都 610054)

【摘要】提出了一种分组密码算法的延迟结合模式，进行了基于信息论原则的安全性证明，并对加入延迟后的密钥执行效率进行了评估。对于算法公开的分组密码，使用密钥延迟技术加强密码体制本身的强度，弱化种子密钥通过互联网公开分发造成的信息泄漏，特别可以有效阻止中间人唯密文进行的算法还原攻击。

关 键 词 分组密码算法; 比特延迟; 密钥; 结合模式
中图分类号 TN918.1 文献标识码 A

A Key Delay Design on Block Cipher Algorithm

LUO Lan，QU Ze-hui，ZHOU Shi-jie，ZHANG Feng-li，QIN Zhi-guang，WEI Zheng-yao

(School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract A key delay design on block cipher is proposed and is demonstrated based on provable security with information theory. Furthermore, we evaluate the result of key delay module. For the published block cipher, the key delay technology can enforce the cryptography system and decrease the information leak from key distribution through internet. Especially, this model can prevent the only cipher-text attack by middle attack.

Key words block cipher; bit-delay; key; operation model

分组密码是网络上广泛使用的一类密码，也是国际上公开密码算法中最活跃的一个分枝。其设计理念是保密依赖于密钥，而算法大多公开；设计结构分为Feistel、代替/置换(Substitution-Permutation，SP)两大类。Feistel网络结构是由Horst Feistel 在设计Lucifer分组密码时发明的，并在数据加密标准(Data Encryption Standard，DES)中得以使用。还有许多密码体制如：GOST、FEAL、RC5、CAMELLIA等都采用了Feistel网络结构。SP网络结构的轮变换分为两层：(1) S混乱层，是由密钥控制的非线性置换，通常由并行查表(S盒)[1]实现；(2) P扩散层，通常由与密钥无关的可逆线性变换实现。SP结构分组密码的抗线性攻击和抗差分攻击的能力容易衡量，而且扩散速度快，因此许多著名的密码算法都采用了SP结构：如高级加密标准(Advanced Encryption Standard，AES)。

随着美国、欧洲、日本等地区对分组密码算法的公开征集，推动了全球对分组密码算法设计与分析的研究。以AES[2]为代表的新一代分组密码算法在设计上明显加强了密钥在整个密码体制中的作用程度。但是对密钥的结合方式上没有给予过多的关注。密钥设计上的漏洞会导致整个算法的抗攻击性质减弱。并且在全球公开标准中的分组密码算法，对密钥的使用没有采取过延迟的方式。事实上，对于掩盖明文的固有特征，密钥的延迟可以产生直接快速的效果。虽然分组密码算法的运算模式已得到国际密码学界广泛的关注，但是密钥延迟的技术还未见公开报道。本文提出对分组密码算法进行唯密文攻击，增强了密钥初始向量的抗分析能力。

1 带比特延迟密钥模块设计

分组密码算法在设计思想上仍然基于香侬关于信息的混乱与扩散原理[3]，通过简单函数进行若干圈迭代使得明文规律被充分掩盖。其优点是：密钥可以在一定时间内固定，不必每次变换，因此给密钥配发带来了方便。但是，由于分组密码存在着密文传输错误在明文中扩散的问题，因此在信道质量较差的情况下无法使用。

分组密码算法通常由密钥扩展算法和加密(解密)算法两部分组成。密钥扩展算法将b字节用户主密钥扩展成r个子密钥。加密算法由一个密码学上的弱函数f与r个子密钥迭代r次组成。混乱和密钥扩散

收稿日期：2006 – 04 – 04
基金项目：国家自然科学基金资助项目(60673075)；国家863计划项目(2006AA01Z428)
作者简介：罗 岚(1969 –)，女，博士，副研究员，主要从事信息安全、计划和科学技术方面的研究.

是分组密码算法设计的基本原则。抵御已知明文的差分和线性攻击，可变长密钥和分组是分组密码体制的设计要点。由于其使用环境的宽泛性，较其他密码而言，在强调密码学性质的同时，还要求工程实现上的高速。为了硬件设计在时效上的经济性，其密钥在安全上通常依赖密码算法本身的一些函数；在密钥结合及密码工作模式上的一些设计可以弥补分组密码算法自身的某些缺陷，而且能够提高速度和加强安全。设计者会针对最坏情况原则进行设计。但是对于攻击者，进行密码算法分析时通常面临的是唯密文的情况。因此，通过算法设计的各个模块加强安全程度是必要的。

2 分组密码算法密钥设计简介

目前使用的分组密码算法无论是FEISTEL网络结构模型或是SP网络结构模型，密钥算法的设计相对密码算法设计是独立的一部分，并且密钥算法都是基于加密算法已经使用的一些运算函数。例如分组密码算法AES的密钥设计即是使用了密码算法中的非线性部分S盒与线性仿射变换，再利用递推关系实现密钥的生成，如图1、2所示。

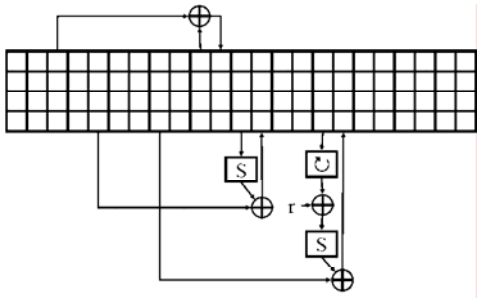

图1 128、192比特密钥生成图

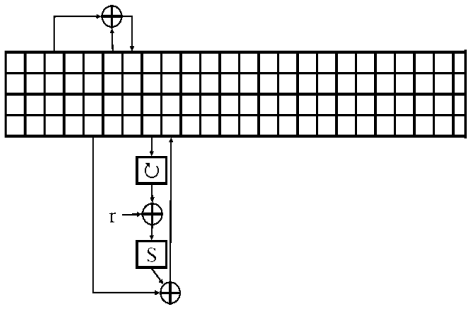

图2 256比特密钥生成图

2.1 分组密码算法密钥带延迟设计

由于分组密码算法保密依赖于密钥[4]，对密钥算法本身的设计需要重点研究以外，在密钥与密码算法本身结合部分如果进行设计上的改进，会使分组密码算法使用时更加安全。为了在使用基于网络使用的分组密码算法时不需要更多的专业密码方面的知识，密钥的相关协议是密码算法安全的保障[5]。本文提出一种带比特延迟的密钥结合模式，掩盖密钥算法与初始向量的关系，设计如图3所示。

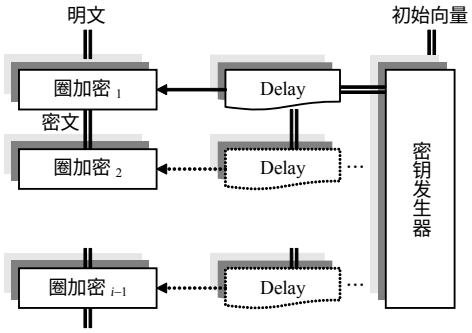

图3 分组密码算法密钥延迟结合模块

密钥算法是初始向量的代数表达式，设对于r比特分组的r维初始向量 $\boldsymbol{IV}=(IV_0,IV_1,\cdots,IV_{r-1})$，第$i$组密钥与每一比特初始向量信息泄露量$H$的关系为：

$$H=-\sum_{\forall i}E^n(\boldsymbol{P}_i)\log_2(E^n(\boldsymbol{P}_i)) \tag{1}$$

式中 E 代表密钥生成算法；$\boldsymbol{P}_i$为每一比特初始向量在实际使用时出现的概率，$0\le i\le N$，$\boldsymbol{N}$是初始向量比特数；$\boldsymbol{E}^i$表示对初始向量进行i次加密后的结果。图3中的虚线部分可以针对安全级别要求进行选择性使用，但是第一圈的延迟对初始向量的掩盖是必要的。这样，r次迭代需要$r+n$个圈密钥。

2.2 密钥延迟结合算法设计的安全性证明

由式(1)可知，密钥对初始向量的信息泄露随着密钥的产生而逐渐降低。根据分组密码算法的应用环境，如果对密钥算法在初始向量运算时进行n字节的延迟的信息泄露与带延迟密钥信息泄露量的对比度为：

$$D=(\sum_{\forall i}E(\boldsymbol{P}_i)\log_2(E(\boldsymbol{P}_i)))\div(\sum_{\forall i}(\boldsymbol{P}_i)\log_2(E^n(\boldsymbol{P}_i)))=O(2^{-nN}) \tag{2}$$

同时，比特延迟会造成算法执行效率的降低。从密码算法的抗线性分析和抗非线性分析的角度也同样可以证明比特延迟的作用[6]。在硬件条件下，使用软件对密钥算法的字节延迟时间可以通过具体算法在不同的平台上对速度做对比研究。如在Pentuime(R)4 CPU 2.66 GHz、504 M内存的单机上进行延迟密钥的实验。仅对第一圈使用的密钥进行延迟处理后其执行速度如表1所示。由式(2)及速度测试的结果可以得出：密钥算法模块针对运行网络和运行计算机的操作系统的实际情况选择不同程度的密

钥延迟，可以在安全级别与运算速度之间进行取舍。

表1　密钥延迟模块与运算速度的仿真结果

	128比特密钥	192比特密钥	256比特密钥
延迟8比特/MB·s^{-1}	198.8	198.6	197
延迟16比特/MB·s^{-1}	197.7	197.5	195
延迟32比特/MB·s^{-1}	196.6	196.2	194

3　结　论

由于分组密码算法在网络环境下使用的密钥分发方式由过去的离线分发转向在线式分发，使得初始向量被窃听的机率增加，对密钥安全的要求也随之增加，这样使得算法的安全性面临较多的问题。特别是互联网上的用户密码使用水平的差距，容易遭受中间人的唯密文攻击。按照国际惯例，分组密码算法需要公开，密码的安全强度依赖于密钥的保密。在对安全级别有特别要求的环境下，有必要用时效性去换取可靠性。本文通过对改善分组密码算法的密钥模块得到结论：添加延迟的方式对强调密钥的安全性是经济的方法；密钥延迟的方式还能对弱密钥有一定的防范功效；并且由于密钥的安全性加强，使得整个算法的抗线性攻击、差分攻击的能力加强，因此可以减少算法的圈数。对于具体的抗攻击度量及圈数设计本文不作进一步讨论。这样，虽然密钥的执行时间加长，但是整个密码系统随圈数的减少无论对硬件面积还是在执行效率上都有一定的弥补。

参　考　文　献

[1] NYBERG K. Differentially uniform mappings for cryptography[C]//Prodeeding of eurocrypt′93, Lecture Notes in Computer Science. Berlin: Springer-verlag, 1993.

[2] DAEMEN J, RIJMEN V. AES proposal[EB/OL]. Rijndeal http://www.nist.gov/aes, 2004-9-10.

[3] SHANNON C D. A mathematical theory of communication[J]. Bell System Technical Journal, 1948, 27: 379-423; 623-656.

[4] SCHNEIER B, KELSEY J. Unbalanced feistel netwoeks and block cipher design[C]//Fast Software Encryption, LNCS 1039. Berlin: Springer-Verlag, 1996: 121-144.

[5] CLIFFORD B. Neuman and theodore Ts'o. kerberos: an authentication service for computer networks[J]. IEEE Communications, 1994, 32(9): 33-38.

[6] MATSUI M. On correlation between the order of s-boxes and the strength of DES[C]//Advances in Cryptology: EUROCRYPT'94, LNCS 950. Berlin: Springer Verlag, 1995: 366-375.

编　辑　孙晓丹