利用IDEA算法之MA—结构的对合置换

赵全习，　陈西宏，　冯有前
(空军工程大学 导弹学院，陕西 三原　713800)

摘　要:利用国际流行的目前最安全的数据加密算法IDEA的核心构件MA—结构构造出了一种128比特长的对合置换,并对其进行了简要的分析,最后利用其构造了一种秘密密钥分组密码。

关键词:分组密码;IDEA算法;MA—结构;对合置换
中图分类号:TN918.4　　**文献标识码**:A　　**文章编号**:1009-3516(2001)03-66-68

Xuejia Lai与James Massey1990年公布了IDEA密码算法第一版(PES)[1]以后,为了抗击差分密码分析,又对其进行了改进,增加了密码算法强度,1992年改名为IDEA(国际数据加密算法)[2]。IDEA基于某些可靠的理论,是目前已公开的最好和最安全的分组密码算法之一,也是当前国际上普遍使用的加密算法,尤其是在DES被成功破译之后,其使用更为广泛。本文利用MA—结构设计了一种对合置换并进行了简要分析。

1　MA—结构的性质

IDEA体制轮函数的基本部件是群加密和MA—结构,其核心构件是MA—结构,如图1所示,这里田:16比特整数的模2^{16}加;⊙:16比特整数的模$2^{16}+1$乘(其中全零子块对应于2^{16}),p_1、p_2、q_1、q_2、z_5、z_6均为16比特子块。

MA—结构具有一些良好的性质:

1)MA—结构的设计原则来自代数群的混合运算。在每一个输出依赖于每个输入子块的意义下,此结构有一个完全的"扩散"和"混乱"效果。

2)MA(.,.,z_5、z_6)对任意选择的密钥子块z_5和z_6是一个可逆变换;MA(p_1,p_2,.,.,)对任意选择的p_1和p_2是一个可逆变换。

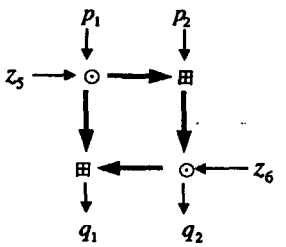

图1　MA—结构

下面来证明其可逆性:

定义:$q_i \odot q_i^{-1} = 1 \mod(2^{16}+1)$　　$-q_i$ 田 $q_i = 0 \mod 2^{16}$　　$i = 1,2$

$z_i \odot z_i^{-1} = 1 \mod(2^{16}+1)$　　$-z_i$ 田 $z_i = 0 \mod 2^{16}$　　$i = 1,2$

$q_1 = (((z_5 \odot p_1)$ 田 $p_2) \odot z_6)$ 田 $(z_5 \odot p_1)$

$q_2 = ((z_5 \odot p_1)$ 田 $p_2) \odot z_6$

$\therefore q_1 = q_2$ 田 $(z_5 \odot p_1)$　　$z_5 \odot p_1 = -q_2$ 田 q_1

$\therefore p_1 = (-q_2$ 田 $q_1) \odot z_5^{-1}$

$(z_5 \odot p_1)$ 田 $p_2 = q_2 \odot z_6^{-1}$　　$(-q_2$ 田 $q_1)$ 田 $p_2 = q_2 \odot z_6^{-1}$

$\therefore p_2 = (q_2 \odot z_6^{-1})$ 田 $(-q_1$ 田 $q_2)$

故对任意选择的密钥子块z_5和z_6,MA(.,.,z_5,z_6)是一个可逆变换。

类似地,可证明对任意选择的p_1和p_2,MA(p_1,p_2,.,.,)是一个可逆变换。

$z_5 = (-q_2$ 田 $q_1) \odot p_5^{-1}$　　$z_6 = q_2 \odot (-q_2$ 田 q_1 田 $p_2)^{-1}$

3)使用MA—结构,达到了完全混乱和扩散所要求的最小次数。

收稿日期:2000-05-14
作者简介:赵全习(1965-),男,陕西凤翔人,讲师,硕士,主要从事信息加密与分组密码研究.

2　利用MA—结构构造的对合置换D

在迭代分组密码体制的设计和分析中,对合置换的分析和构造具有十分重要的意义。所谓对合置换是指若映射 $p_1: F_2^n \to F_2^n$ 对任意的 $x \in F_2^n$,均有 $p_1(p_1(x)) = x$ 成立,则称该映射是一个对合置换。最简单的例子是在二进制下,和一个常数相加的运算。

MA—结构有以上分析的良好特性,本文用MA—结构来构造一种对合置换D,其计算框图见图2。图2中 x_i:16比特子块;y_i:16比特子块;⊕:16比特子块逐比特异或;田:16比特整数的模 2^{16} 加;⊙:16比特整数的模 $2^{16}+1$ 乘(其中全零子块对应于 2^{16})。

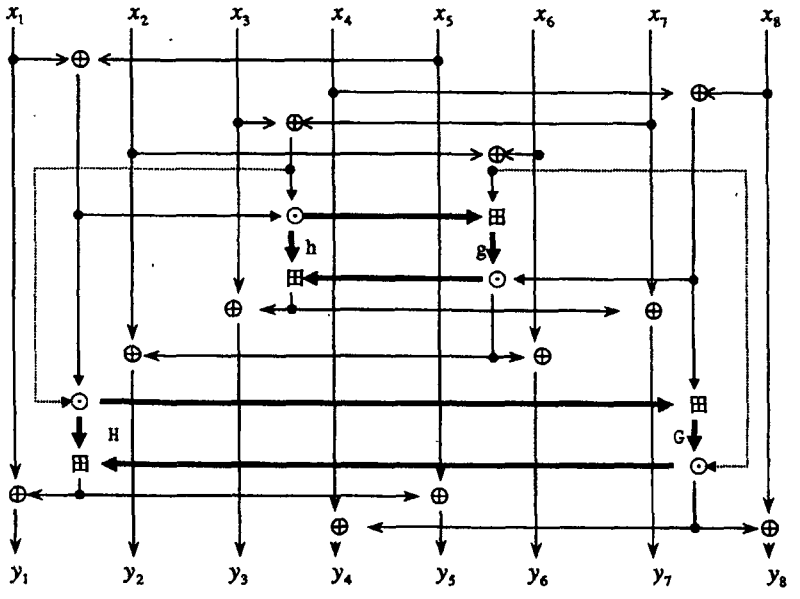

图2　对合置换D的计算框图

对合置换D的计算框图中含有两个MA—结构,一个是hg,另一个是HG。它没有密钥输入,而IDEA算法的MA—结构有密钥输入。

3　对合置换的简要分析

1)混乱:用于掩盖明文和密文间的关系。在对合置换D中,通过三种不同的群运算,使其取得混乱的效果。MA—结构中三种群运算⊕、⊙、田是不兼容的,即:

①三个运算中任意两个运算不满足分配律,如　a 田$(b \odot c) \neq (a$ 田$b) \odot (a$ 田$c)$。

②三个运算中任意两个运算间不满足结合律,如　a 田$(b \oplus c) \neq (a$ 田$b) \oplus c$。

在对合置换D的设计中,三种不同群运算的组合使得一种类型运算的输出绝不会被用作同一种类型运算的输入。这些运算使输入间实现了较复杂的组合运算,因而对合置换D的输出块对输入子块的依赖关系显得十分复杂,达到了混乱的目的。

2)扩散:通过将明文冗余度分散到密文中,使之分散开来。对合置换D中的扩散是由两个MA—结构提供的,其中MA—结构hg使得对合置换的输出子块 y_2、y_3、y_6、y_7 依赖于每个输入子块 x_1、x_2、x_3、x_4、x_5、x_6、x_7、x_8;MA—结构HG使得对合置换的输出子块 y_1、y_4、y_5、y_8 依赖于每个输入子块 x_1、x_2、x_3、x_4、x_5、x_6、x_7、x_8;这样对合置换的每个输出子块依赖于其每个输入子块,具有一个"完全"扩散的效果。

3)分组长度:分组长度是分组密码设计和分析中的重要参数之一,分组长度要足够大,才能防止明文穷举攻击法奏效。对一个固定密钥来说,2^n 个不同的明密文对实际上可完全刻划加密函数,所以分组密码的长度 n 应保证使得攻击者实际获得的明密文对的个数远小于 2^n。

在可预见的未来选择构造128比特的对合置换,并利用其设计分组长度为128比特且更为安全的分组密码体制。

4　对合置换的应用

对合置换在双结构迭代密码[3]的设计中有着重要的意义,双结构迭代密码 $s^n = (s_1 \times s_2 \times \sigma)^n$,这里 S 由

两个具互不相容代数结构或运算的密码 s_1, s_2 及 $\sigma \in G_p$ 构成。从安全性和实现上考虑,s_1, s_2 应选对合密码或部分地选对合密码,且 σ 为对合置换。利用以上的对合置换可以设计出一些分组长度为 128 比特的秘密密钥分组密码体制。以下用一个简单的例子来说明它的应用。在此种秘密密钥分组密码体制中,明文 P、密文 T 长度均为 128 比特,密钥 K 为 128 比特长,加密过程框图如图 3 所示。

图 3 中,将对合置换 D 的输出 y_3 与 y_4 交换,y_5 与 y_6 交换,这是一个简单的对合置换。此分组密码的解密过程同加密过程完全相同。

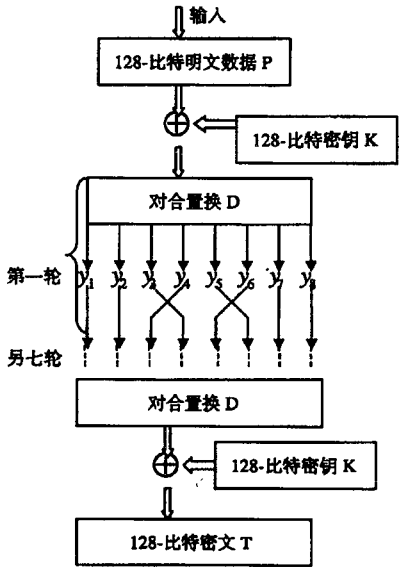

图 3 用对合置换 D 构造的加密算法

5 结论

本文在分析了 IDEA 之 MA—结构的一些性质的基础上,构造出了一种 128 比特长的对合置换,并对其特性进行了必要的分析,利用对合置换 D 构造出了一种秘密密钥分组密码体制,对合置换 D 的构造对 IDEA 类分组密码体制的研究和应用都具有积极意义。

参考文献:

[1] Lai xuejia, Massey J. A Proposal for a New Block Encryption Standard[A]. Advances in Cryptology - EUROCRYPT'90 Proceedings[C]. Berlin: Springer - Verlag, 1991. 389 - 404.

[2] Lai xuejia. On the Design and Security of Block Ciphers[A]. ETH Series in Information Processing, Vol. 1[C]. Konstanz: Hartung - gorre Verlag, 1992.

[3] 谷大武. 分组密码理论与某些关键技术研究[D] 西安:西安电子科技大学,1998.

An Involution Permutation Based on MA - Structure In IDEA

ZHAO Quan - xi CHEN Xi - hong FENG You - qian

(The Missile Institute of the Air Force Engineering University, Sanyuan 713800, China)

Abstract: The paper constructs an involution permutation with 128 bits long by using the MA - structure in IDEA and simply analyses its properties. Finally, a sort of secret - key block cipher is constructed with the help of this involution permutation.

Key words: block cipher; IDEA; MA - structure; involution permutation