针对 PRESENT 分组密码算法的代数分析 *

葛十景，谷大武，刘志强，刘 亚
（上海交通大学 计算机科学与工程系，上海 200240）

摘 要：研究针对 PRESENT 分组密码的代数分析。通过使用 S 盒的表达式形式，构建出多轮 PRESENT 加密中的代数方程组。这种构建方程的方法被推广到具有小型 S 盒的典型 SPN 型分组密码算法的方程构建问题中。对简化的 PRESENT 算法进行了攻击实验，采用 MiniSAT 作为攻击过程中的求解工具，对四轮、六轮 PRESENT 加密进行实际攻击。可以在 1 min 内恢复四轮加密的所有密钥，数小时内恢复六轮加密的密钥。通过引入了差分思想，将有效攻击轮数提高到八轮。

关键词：代数分析；PRESENT 算法；S 盒；可满足问题；可满足问题求解软件；分组密码
中图分类号：TP309.7 **文献标志码**：A **文章编号**：1001-3695(2011)05-1889-05
doi:10.3969/j.issn.1001-3695.2011.05.084

Algebraic attack on PRESENT cipher

GE Shi-jing, GU Da-wu, LIU Zhi-qiang, LIU Ya
(*Dept. of Computer Science & Engineering, Shanghai Jiaotong University, Shanghai* 200240, *China*)

Abstract: This paper studied algebraic attack of PRESENT cipher. Given a new method to generate equations for PRESENT. Then generalized this method for typical SPN cipher with small S-box. In the experiment, reduced round PRESENT was attacked by MiniSAT. It could recover keys of 4-round PRESENT in a minute. And it cost hours to recover keys of 6-round PRESEN. By introducing difference, the attack would be more effective. It could recover keys of 8-rounds PRESEN in reasonable time.

Key words: algebraic attack; PRESENT; S-box; SAT; SAT solver software; block cipher

代数分析是一种针对密码算法的新型攻击方法，与传统的基于统计学思想的差分分析、线性分析等分析方法相比有许多优点：需要的明/密文对数量少，更加符合实际需求；能够针对密码算法中代数结构的弱点进行攻击，有很强的针对性；可以作为一种基本思想，与各种传统分析方法相结合寻求更好的攻击效果。在 CHES2007 上，Bogdanov 等人[1]提出了 PRESENT 对称加密算法。该算法是一种超轻量级的 SPN 型分组密码，主要应用于 RFID 系统、嵌入式系统等计算资源受限的环境中。由于采用了更有利于硬件实现的小型 S 盒，PRESENT 算法有良好的硬件实现性能。

本文采用代数分析对超轻量级分组密码 PRESENT 进行了研究，取得了以下成果：a）提出了采用中间相遇思想构造多轮 PRESENT 加密中代数方程组的方法，并且将该方法推广到具有小型 S 盒的典型 SPN 型分组密码中；b）针对简化的 PRESENT 加密算法中的代数方程组采用 MiniSAT 进行求解，进行了攻击实验；c）使用差分思想，提高攻击效率将有效攻击轮数提高到八轮。

1 代数分析简介

1.1 代数分析的起源

代数分析方法源于 Shannon[2]提出的一个基本命题：对于一个完善的密码算法而言，攻破该算法所需的计算量不应亚于解决一个复杂的、规模未知的联立方程组的计算量。换句话说，如果将一个密码算法的计算过程表示成一组代数方程，通过求解这组方程中的未知元可获取该密码算法中的密钥信息，就攻破了该算法，而其中使用的分析方法则称为代数分析法。

针对加密算法的代数分析大致分为构建加密过程中的方程组和求解该方程组两步。代数分析中，求解方程组需要的时间代价最高。二元域（GF(2)）上的多元二次方程组的求解问题已被证明是一个 NP 困难问题[3]。如何构建有效的、适合求解的方程组是难点之一。

1.2 代数方程的构建

构建加密过程中的代数方程，是利用加密算法中 S 盒或其他非线性组件的代数特性，寻找一组以密钥和加密过程中的中间变元为未知量的方程。加密算法中广泛地应用了比特变换，所以这些方程大多是构建在 GF(2)上的。通常，构建多轮加密中的代数方程是通过将 S 盒或非线性组件中的方程扩展到整个加密过程来实现的。

对于一些 S 盒有特殊代数结构的密码算法（如 AES），描述 S 盒代数特征的等式即可以用于构建方程组。文献[4]中就基于 AES 中 S 盒的代数特性寻找到一些方程。

对于没有特殊代数结构或没有明显代数特性的 S 盒（如 DES 中的 S 盒），文献[5]提出了一种寻找稀疏—低次—超定

收稿日期：2010-10-26；**修回日期**：2010-11-26 **基金项目**：国家教育部高校博士点基金资助项目（200802480019）

作者简介：葛十景（1986-），男，江苏如东人，硕士，主要研究方向为代数分析（tonyge@sjtu.edu.cn）；谷大武（1970-），男，教授，博士，主要研究方向为计算机安全与密码学；刘志强（1977-），男，博士研究生，主要研究方向为分组密码的分析与设计；刘亚（1983-），女，博士研究生，主要研究方向为分组密码的分析与设计.

方程组来描述 S 盒的方法。这种方法广泛地适用于各种 S 盒。该方法也成为之后代数分析中寻找方程的通用方法。

此外,S 盒的表达形式也可以看做代数方程。对于任意一个 m 比特输入、n 比特输出的 S 盒,定义输入向量为 X、输出向量为 Y。输出向量中的任意比特可以表示成输入比特的表达式,表达式中仅包含乘积及加法运算(在 GF(2)中,加法运算等同于异或运算,乘法运算等同于与运算)。

S 盒输出中每个比特的表达式都可以转换成形如式(1)的形式。S 盒运算等价于式(2)中的 S 函数。

$$Y_i = f'_i(X) = f_i(X_0, X_1, X_2, \cdots, X_{m-1}) = \sum_{k=0}^{2^m-1} (\alpha_{i,k} \prod_{j=0}^{m-1} X_j^{s_{k,j}}) \quad (1)$$

其中:X_j 为向量 X 的第 j 比特,Y_i 为向量 Y 的第 i 比特,且满足 $k = \sum_{j=0}^{m-1} s_{k,j} \times 2^j$。

$$Y = (Y_0, Y_1, Y_2, \cdots, Y_{m-1}) = (f'_0(X), f'_1(X), f'_2(X), \cdots, f'_{m-1}(X)) = S(X) \quad (2)$$

其中:$f'_i(X)$ 函数为式(1)中对应的函数。

输出的任意比特表示为输入比特表达式的最高次数不超过输入维度 m。当 S 盒可逆时,输出维度也为 m,由输出比特表示输入比特的逻辑表达式最高次数也不超过 m。由此方法,可以创建两组,共 2 m 个次数不高于 m 的方程。这两组方程都是 S 盒的表达式,每一组方程都可以唯一确定 S 盒的映射关系。与文献[5]中给出的方法相比,这种方法中的冗余方程数量少。当 S 盒的输入/输出维度较小时,构造出的方程次数不高,可以直接用于构造代数方程组。文献[6]中给出了一种寻找这些表达式的算法。对于一些使用小 S 盒的分组密码,如 PRESENT、Serpent 可以使用这种方程来构造方程组。

保持密钥不变,每一组明/密文对可以产生一组代数方程。由随机的两组明文出发产生的两组方程,这两组方程中相互对应的中间变量相互独立。每当引入新的明/密文对时,方程数和变量数都会增加。新方程的引入在一定程度上能够增加限制条件,缩小满足方程系统的解的范围;新引入的变元也使得代数系统规模不断变大,方程组的求解复杂度增加。若选取两组明/密文对,两组中间变量对应比特间的异或值与差分链中差分特征对应位置比特相等。

1.3 代数方程的求解

已有学者在求解多元高次方程组方面作了大量的研究。Buchberger 最早提出了利用 Gröbner 基[7]求解多元高次方程组的方法(Buchberger 算法)。这是一种指数复杂度的算法,其本质是从多项式环中任意理想的生成元出发,计算出一组具有特殊性质的基——Gröbner 基,进而研究理想的结构并进行运算求解方程组的所有解。其中在计算 Gröbner 基部分的复杂度为指数级别,所以整个算法也是指数级的。尽管多位学者对计算 Gröbner 基的算法进行了优化[8,9],但是其复杂度仍然是指数级的。

在求解二次方程方面,Kipnis 等人[10]提出了再线性化方法,该思想是将方程中的二次项用一个新的项代替,从而将方程转换为线性方程组。Courtois 等人[11,12]给出了针对稀疏、超定方程组求解的有效算法——XL 算法,并在分析 Rijndeal 和 Serpent 算法时扩展了该算法[13]。但是线性化方法以及其扩展出来的各种算法的时间复杂度很难估计,而且其有效性目前还一直没有定论。

此外,还有一些方法尝试将求解方程组问题转换成其他问题进行求解,如文献[14]将方程组的求解问题转换成可满足性问题(SAT)的求解。目前对于可满足问题已经有了不少的研究,一些求解工具如 MiniSAT 可以求解一定规模的 SAT 问题。转换成可满足问题求解是一种相对简单的方法,便于进行实验。采用该方法,研究者可以更加容易地发现一些隐蔽的代数结构弱点。此外使用这种方法,攻击者可以有更多的精力去关注密码算法结构中的一些弱点,而不是求解本身。这也是本文选用 MiniSAT 作为求解工具的重要原因。Courtois 的网站(http://www.cryptosystem.net/)中给出了一些工具,可以将方程直接转换为 SAT 问题,并调用常见的 SAT Solver 进行求解。

2 PRESENT 分组密码算法简介

2.1 PRESNET 密码的提出

在 CHES2007 上,Bogdanov 等人提出了 PRESENT 算法,该算法属于超轻量级加密算法。所谓密码算法的量级,主要是通过其硬件实现时的复杂程度衡量的,PRESENT 密码算法与现有的轻量级分组密码 TEA[15]、MCRYPTON[16]、HIGHT[17]、SEA[18] 和 CGEN[19] 等相比,有着最简单的硬件实现,因此被称为超轻量级密码算法。80 bit 密钥的 PRESENT 密码算法进行硬件实现仅需要约 1 570 个与非门,是典型的轻量级加密算法。该算法在功耗方面也有很优秀的表现。

2.2 针对 PRESENT 密码的分析

尽管 PRESENT 算法的提出者声称该算法能够抵御简单的差分分析和线性分析,并且通过构造 21 个八元二次方程组描述一个 S 盒的方法构造出两轮的 PRESENT 加密过程的代数系统,通过 Magma 软件中实现的 F4 算法进行求解,未能在合理时间内给出结果。但是由于 PRESENT 算法在性能方面的出众表现,众学者对其安全性进行了深入分析。文献[20,21]分别对 PRESENT 作了差分和线性分析,采用大量明—密文对攻击了多轮的 PRESENT 密码算法。文献[22]通过猜测部分密钥再进行代数攻击的方法攻击了五轮的 PRESENT 算法。文献[23]指出使用 MiniSAT 可以攻击六轮的 PRESENT 加密算法。“对于六轮 PRESENT,利用四个(任意两个仅有 1 bit 不同)已知明密对,求出全部密钥比特的平均计算时间约为 202 h 23 min。”[23] 虽然该表述中,关于要求构造四个(任意两个仅有 1 bit 不同的明文)已知明密对有一些歧义,但是其给出的实验数据还是有一定的参考价值。

3 针对 PRESENT 分组密码算法的代数攻击

3.1 构建 PRESENT 算法中的代数方程

3.1.1 构建 PRESENT 加密过程中的代数方程

PRESENT 密码算法的 S 盒如表 1 所示。

表 1 PRESENT 加密算法中 S 盒运算

X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Y	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

S 盒的表达式形式可以表述为以下两组等式:

a)S 盒输出 Y 的表达式为

$$Y[0] = X[0] + X[2] + X[3] + X[1] * X[2]$$

$$Y[1] = X[1] + X[3] + X[1] * X[3] + X[2] * X[3] + X[0] * X[1] * X[2] + X[0] * X[1] * X[3] + X[0] * X[2] * X[3]$$

$$Y[2] = 1 + X[2] + X[3] + X[0] * X[1] + X[0] * X[3] + X[1] * X[3] + X[0] * X[1] * X[3] + X[0] * X[2] * X[3]$$

$$Y[3]=1+X[0]+X[1]+X[3]+X[1]*X[2]+X[0]*X[1]*X[2]+X[0]*X[1]*X[3]+X[0]*X[2]*X[3]$$

b)逆向表达式(S 盒输出 X 的表达式)为

$$X[0]=1+Y[0]+Y[2]+Y[1]*Y[3]$$

$$X[1]=Y[0]+Y[1]+Y[3]+Y[0]*Y[2]+Y[1]*Y[3]+Y[2]*Y[3]+Y[0]*Y[1]*Y[2]+Y[0]*Y[1]*Y[3]+Y[0]*Y[2]*Y[3]$$

$$X[2]=1+Y[3]+Y[0]*Y[1]+Y[0]*Y[2]+Y[0]*Y[3]+Y[1]*Y[2]+Y[1]*Y[3]+Y[0]*Y[1]*Y[2]+Y[0]*Y[1]*Y[3]+Y[0]*Y[2]*Y[3]$$

$$X[3]=Y[0]+Y[1]+Y[2]+Y[3]+Y[0]*Y[1]+Y[0]*Y[1]*Y[2]+Y[0]*Y[2]*Y[3]$$

其中:$X[i]/Y[i]$表示输入/输出的第 i 比特。PRESENT 算法 S 盒中的方程次数均不高于 3 次。使用中间相遇思想消去中间变量,可以构造出 PRESENT 运算两轮加密的表达式:

$$L(S(M+K_0))+C=K_1 \tag{3}$$

其中:S 运算为 S 盒运算;L 运算为线性层运算;M 为明文;C 为密文。

$$L(S(M+K_0))+S^{-1}(Y_1)=K_1 \tag{4}$$

其中:S^{-1}运算为 S 盒运算的逆运算。

$$L(S(X_2))+C=K_3 \tag{5}$$

$$L(Y_1)+X_2=K_2 \tag{6}$$

其中:K_i 为第 i 轮密钥,X_i 为第 i 轮 S 盒输入,Y_i 为第 i 轮 S 盒输出。

采用类似的方法可以构造出六轮以及更多轮数的方程组。

3.1.2　构建 PRESENT 轮密钥生成中的代数方程

在 3.1.1 节构建的方程中,变量包括加密过程中的中间变量和轮密钥。轮密钥由主密钥通过轮密钥生成算法得到,在轮密钥生成中,可以构建轮密钥与主密钥之间的方程。

在 PRESENT 密码算法中,轮密钥生成算法采用与加密过程同样的 S 盒及相对简单的线性层。PRESENT 轮密钥生成算法中,每一轮迭代包含一个 S 盒运算、异或常数和线性变换。若将轮密钥生成算法中的中间量表示成主密钥的表达式,则只有 S 盒运算会影响表达式的次数。由于每轮迭代仅有一个 S 盒运算,对于 16 轮及其之前的所有轮密钥比特的表达式次数均不高于 3 次。这种表达式可以表示成为式(7)的形式。

$$K_i=F_i(K) \tag{7}$$

其中:K 为 80 bit 主密钥,K_i 为第 i 轮轮密钥。

此外 16 轮以上的轮密钥表示成主密钥的表达式次数不高于 9 次。当需要攻击 16 轮以上的加密时,可以通过引入中间变量的方法实现降次[14]。

3.1.3　代数系统规模分析

对于低轮(不大于 16 轮)PRESENT 加密,当加密轮数为偶数($2N$)时,采用相遇式方法可以构造代数系统。每两轮引入 $64\times2=128$ 个中间变量。明文和密文代入方程中可以消去 128 个变量,所以一共需要引入 $128\times(N-1)$ 个中间变量。每两轮可以构造出 64 个三次方程,衔接处的线性变换产生$64\times(N-1)$个一次方程。方程数一共为 $128\times N-64$。这些方程中除了引入的中间变量以外,主密钥比特也作为变量存在。所以对于一组明—密文对,构造的方程系统,有 $128\times N-128+80$ 个未知量,及 $128\times N-64$ 个方程。

采用文献[5]中的构造代数系统系统的方法,构造两次方程,每个 S 盒产生 21 个方程。这 21 个方程代表的 S 盒与实际 S 盒之间无法从理论上给出等价关系。这些方程中的未知元涉及 S 盒的所有输入/输出比特。考虑加密过程需要引入的中间变量,每轮引入 128 个中间变量,是以上方法的两倍。

3.1.4　在典型 SPN 型分组密码算法中的推广

典型的 SPN 型分组密码算法采用可逆 S 盒,加密结构如图 1 所示。PRESENT 作为一种典型的 SPN 型分组密码,应用在它身上的构建方程方法可以推广到一般的 SPN 型分组密码中。利用中间相遇的思想,可以使用 S 盒的表达式形式构造出两轮加密过程中的代数系统。

图 1　SPN 型分组密码两轮加密结构

将首轮的 S 盒输出表示成首轮输入的表达式,将次轮输入表示成次轮输出的表达式,首轮 S 盒输出经过线性变换与次轮输入的差为轮密钥。使用 L 运算表示加密的线性置换层,S 运算代表 S 盒运算,其等式形式为

$$L(S(X_i))+S^{-1}(Y_{i+1})=K_{i+1} \tag{8}$$

以两轮加密为单位,每两个单位之间的线性层可表示为

$$L(Y_{i-1})+K_i=X_i \tag{9}$$

对于加密过程中的第一轮,将明文代入式(1)可得 $L(S(M\oplus K_0))+S^{-1}(Y_{i+1})=K_{i+1}$;加密过程的最后一轮时(假设加密轮数为奇数),将密文代入式(2)可得 $L(S(X_i))\oplus C=K_{n-1}$。

使用以上两个等式,可以将多轮的加密过程代数系统化。在得到的方程系统中,引入了新的变元 K_i,K_i 为加密过程中使用的轮密钥。轮密钥由主密钥产生,针对不同的轮密钥生成算法可以采用类似的方法构造出代数系统。此外每两轮的衔接,需要引入两组中间变量 Y_{i-1} 及 X_i,这些中间变元与密钥 K 一起构成代数系统中的未知量。

3.1.5　使用两组明/密文对构建 PRESENT 中的方程组

当选取两组明/密文对时,构造的代数系统已经是超定[13]的,其解空间已经在可控范围内。若已知加密过程中的差分特征,由输入/输出的差分与中间变量对应位置的异或产生的等式关系如下:

$$X_i\oplus X_i'=\triangle X_i \tag{10}$$

$$Y_i\oplus Y_i'=\triangle Y_i \tag{11}$$

以上等式描述了两组明/密文对中的所有中间变元的相互关系。形如上式的一次方程,每个方程可以消去一个中间变元。可以有效地提高整个方程系统的求解速度。若已知一条差分链的成立概率为 p,寻找一组正确的明/密文对满足该差分链需要约 $1/p$ 对明/密文对。本文中给出的构造方程系统方法并不涉及加密过程中所有的中间变量,所以不需要完整的差分链,其需要的明/密文对数量略少于 $1/p$,但无法从理论上预估实际值。

实验证明,即使无法得到完整的差分链,仅引入部分差分特征,即仅采用整个差分链中的部分比特,也可以有效地提高方程系统的求解速度。

3.2　基于 MiniSAT 的求解实验

3.2.1　实验环境

实验采用本文中给出的方法构造代数方程组,并使用文献[10]中方法将其转换成 SAT 问题,选取 Courtois 网站中提供的

MiniSAT 版本进行求解。硬件环境为:Intel Core(TM)2 Duo CPU T7500,4GB RAM,Windows 7(64 bit)。

3.2.2 攻击四轮简化的 PRESENT 算法

实验内容:随机选取一个密钥,随机生成明文的 60 bit,穷举明文的最后 4 bit,产生 16 个明文。采用随机选取的密钥分别对这 16 个明文进行四轮 PRESENT 加密。在这 16 组明/密文对中选取部分明/密文对,采用以上方法构成代数方程系统并进行求解。并且逐渐增加明/密文对数量进行对比实验。

实验结果:实验中不同明文对的实验数据有一定差距不适合取平均值,以下为其中一组实验数据(时间单位为秒)。

表 2　明/密文对数量与求解实验间关系

数量	2	4	6	8	12	16
时间/s	68.89	15.71	29.26	61.95	125.14	163.88

实验结果分析:由以上实验结果可知,适当引入多对明/密文对可以有效地提高求解速度。但是当选取的明/密文对超过一定数量时,求解时间反而变长。其主要原因是大量新的中间变量引入,使得方程系统中复杂度增大,需要更多时间求解新引入的中间变量。

在该实验中攻击实验与文献[13]中攻击四轮实验时间消耗相比有大幅度的降低。

3.2.3 攻击六轮简化 PRESENT 算法

实验内容:随机选取一个密钥,随机生成明文。对明文进行六轮 PRESENT 加密,产生一对明/密文。对明文最后一比特取反,再次对新明文进行六轮加密,产生一对明/密文。采用上文中方法构建两组明/密文对的方程组。对产生的方程组采用 MiniSAT 进行求解。随机选取密钥中 20 bit,作为已知量加入方程组中,对新方程组采用 MiniSAT 进行求解。重复以上实验。

实验结果:对于未加入密钥信息的方程组,进行了三次实验,其中一次在 35 h 后得到结果,其他两次实验均无法在 72 h 内给出结果;对于加入密钥信息的方程组,进行了 10 次实验。攻击时间消耗差距较大。其中有三次实验无法在 10 h 内给出完整解。剩余七次实验的求解时间在 0.5 ~8 h 不等。

实验结果分析:由以上实验结果可知,该攻击实验中存在一定的偶然性。

当密钥完全未知时,文献[15]中给出攻击六轮加密的时间为 202 h。该结果应该仅为一次实验的结果。

3.3 引入差分思想攻击八轮 PRESENT 加密

使用两组明—密文对时,由于在实际攻击中无法获取整个差分链的信息,无法构造出两组代数系统中对应中间变量的等式关系。但是通过选取一些特定的明/密文对,可以控制差分链中的一部分,从而构造出一些等式关系。若已知密钥的部分比特,通过选取明文,可以得到更多差分链的信息,从而构造更多中间变量之间的等式。

对于 PRESENT 而言,考虑差分链,每一个活动 S 盒在经过线性层时,会被扩展到下一轮的 4 个 S 盒。对于非活动 S 盒,其输入/输出比特对应的两组中间变量相等。对于活动 S 盒对应变量之间的关系未知。当已知密文的部分比特时,通过构造明文对的方式,可以控制多轮的差分,进而从中获取等式关系。图 2 为四轮 PRESENT 加密的结构图,其中一种构造方式是,通过控制明文的最后 16 bit(4 个 S 盒)构造出两组明文,使得 S 盒 5 的输入差分为满足一定性质。

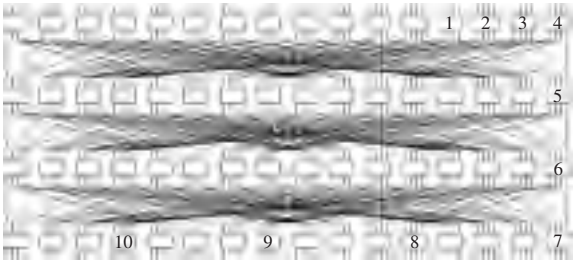

图 2　PRESENT 四轮加密结构

实验方法:通过控制明文的最后 16 bit 构造出两组明文,使得图 2 的 S 盒 6 的输入差分为 1(最低位为 1),且该轮的其他 S 盒均为非活动 S 盒(输入差分为 0)。为了获得以上的两组明/密文对,需要给定影响 S 盒 1、2、3、4、5 的 20 bit 密钥。随机选取一组明文进行加密,通过逆向计算,即可以获得另一组明文。

由于第三轮的输入差分为 1,由差分分析可知,输入为 1 的两轮差分链共有 160 种可能。通过穷举,可以遍历这 160 种可能进行求解。

实验结果:若当前考虑的差分符合实际的差分时,求解六轮加密过程构造的代数系统仅需数分钟。八轮加密过程构造成代数系统,求解需要数小时(实验结果为 1 ~5 h 不等)。若当前考虑的差分不符合实际差分时,求解时间比符合时所用时间略少。在该实验中,通过选定 20 bit 的密钥,可以在约160 × 5 = 800 h 内恢复出正确的密钥。若采用穷举方法进行破译需要穷举 60 bit 密钥,在目前的计算能力下需要的时间远大于 800 h。

4 结束语

PRESENT 密码算法作为一个知名超轻量级密码算法,已经得到了不少应用,且在未来可能会得到更大规模的应用。但是,PRESENT 密码算法的轮密钥生成算法相对简单,构造出的轮密钥与主密钥之间关系的表达式也相对简单。这种相对简单的等式关系使得由轮密钥恢复主密钥变得更加迅速有效。若在轮密钥生成的过程中引入多个 S 盒,可以有效地提高轮密钥表达式的次数,提高该密码算法在代数以及其他分析面前的安全性。本文使用 S 盒的代数表达式形式,给出针对 PRESENT 密码算法构造代数方程的一种方法,并将这种方法推广到典型的 SPN 型分组密码中。针对 PRESENT 算法的攻击实验证明该方法是有效的。与文献[20,21]中的方法相比,针对 PRESENT 的攻击在使用基本代数攻击时,攻击速度基本一致。由于该方法方程数更少,中间变量数量也较少,更加有利于与差分思想结合。改进后的攻击方法可以有效地减少了中间变量数,提高了攻击速度,取得了比较好的攻击效果。由于包括 MiniSAT 在内的一些求解工具都无法预估代数系统的求解代价。对于更多轮数的加密,本文也无法给出更加具体的攻击复杂度。但是,实验证明本文给出的方法是有效的,而且与传统方法相比有一定的改进。本文中仅分析了偶数轮 PRESENT 加密的情况,对于奇数轮($2 \times N + 1$)的加密,可以通过$2 \times N$加密中的方程组进行扩展。代数分析作为一种新型的分析方法还存在很多不足,其中一个重要的问题是对于给定的代数系统,无法从理论上给出求解的复杂度估计。过分地依赖实验,使得代数分析无法在理论上得到很好的突破。与其他分析方法结合是有效提高攻击效率的方法,也使得代数分析能够突破实验

限制,在理论上分析更多轮加密成为可能。

参考文献:

[1] BOGDANOV A, KNUDSEN L R, LEANDER G, *et al*. PRESENT: an ultra-lightweight block cipher[C]//Proc of Cryptographic Hardware and Embedded Systems. 2007: 450-466.

[2] SHANNON C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 704.

[3] GAREY M, JOHNSON D S. Computers and intractability, a guide to the theory of NP-completeness[M]. New York: Freeman W H & Co., 1990: 251.

[4] MURPHY S, ROBSHAW M J B. Essential algebraic structure within the AES[C]//Proc of the 22nd Annual International Corgptology Conference on Advances in Cryptology. London: Springer-Verlag, 2002: 1-16.

[5] COURTOIS N T, BARD G V. Algebraic cryptanalysis of the data encryption standard[C]//Proc of the 11th IMA International Conference on Cryptography and Coding. 2007.

[6] 易训. 关于 S 盒的布尔函数表达式[J]. 通信保密, 1995(2): 55-60.

[7] BECKER T, KREDEL H, WEISPFENNING V. Gröbner Bases: a computational approach to commutative algebra[M]. London: Springer-Verlag, 1993.

[8] FAUGERE J C. A new efficient algorithm for computing Gröbner bases (F4)[J]. Journal of Pure and Applied Algebra, 1999, 139(1-3): 61-88.

[9] FAUGERE J C. A new efficient algorithm for computing Gröbner bases without reduction to zero(F5)[C]//Proc of ISSAC. New York: ACM Press, 2002: 75-83.

[10] KIPNIS A, SHAMIR A. Cryptanalysis of the HFE public key cryptosystem by relinearization[C]//Proc of the 19th Aunual International Cryptology Conference on Advances in Cryptology. London: Springer-Verlag, 1999: 788.

[11] SHAMIR A, PATARIN J, COURTOIS N T, *et al*. Efficient algorithms for solving overdefined systems of multivariate polynomial equations[C]//Proc of the 19th International Conference on Theory and Application of Cryptographic Techniques. Berlin: Springer, 2000: 392-407.

[12] COURTOIS N, GOUBIN L, MEIER W, *et al*. Solving underdefined systems of multivariate quadratic equations[C]//LNCS, Vol. 2274. London: Springer, 2002: 211-225.

[13] COURTOIS N T, PIEPRZYK J. Cryptanalysis of block ciphers with overdefined systems of equations[C]//LNCS, Vol. 2501. London: Springer, 2002: 267-287.

[14] COURTOIS N, BARD G V, JEFFERSON C. Efficient methods for conversion and solution of sparse systems of low-degree multivariate polynomials over GF(2) via SAT-solvers[EB/OL]. (2007). http://eprint.iacr.org/2007/024/.

[15] WHEELER D J, NEEDHAM R M. TEA, a tiny encryption algorithm[C]//LNCS, Vol. 1008. 1995: 363-366.

[16] LIM C H, KORKISHKO T. mCrypton-a lightweight block cipher for security of low-cost RFID tags and sensors[C]//LNCS, Vol. 3786. 2006: 243-258.

[17] HONG D, SUNG J, HONG S, *et al*. HIGHT: a new block cipher suitable for low-resource device[C]//Proc of Cryptographic Hardware and Embedded Systems. 2006: 46-59.

[18] STANDAERT F X, PIRET G, GERSHENFELD N, *et al*. SEA: a scalable encryption algorithm for small embedded applications[C]//Proc of CARDIS. 2006: 222-236.

[19] ROBSHAW M J B. Searching for compact algorithms: CGEN[C]//Proc of Progress in Cryptology -VIETCRYPT. 2006: 37-49.

[20] WANG Mei-qin. Differential cryptanalysis of reduced-round PRESENT[C]//LNCS, Vol. 5023. 2008: 40-49.

[21] CHO J Y. Linear cryptanalysis of reduced-round PRESENT[C]//LNCS, Vol. 5985. 2010: 302-317.

[22] NAKAHARA J, SEPEHRDAD P, ZHANG Bing-sheng, *et al*. Linear (hull) and algebraic cryptanalysis of the block cipher PRESENT[C]//Proc of Cryptology and Network Security. 2009: 58-75.

[23] 卜凡, 金晨辉. 针对低轮 PRESENT 的代数攻击[J]. 计算机工程, 2010, 36(6): 128-130.

(上接第 1888 页)

3　结束语

无线传感器网络的应用环境和传感器节点的资源受限,使得在实际中大规模安全应用无线传感器网络成为一种挑战。许多学者在结合无线传感器网络自身特点的基础上,研究设计适用于无线传感器网络的安全协议,但都无法同时满足网络安全连通性和网络抗毁性。本文在文献[10]方案的基础上提出了一些改进措施,改进后的方案能够更充分发挥和利用散列链的特点,在网络安全连通性和网络抗毁性两方面都取得了优异的性能,为无线传感器网络中的密钥协议提供了一种解决方案。当然,面对越来越严重的网络攻击,本文提出的方案还需要进一步改进,以保证网络的安全有效使用。

参考文献:

[1] AKYILDIZ I F, SU W, SANKARASUBRAMANIAM Y, *et al*. Wireless sensor networks: a survey[J]. Computer Networks, 2002, 38(4): 393-422.

[2] GURA N, PATEL A, WANDER A, *et al*. Comparing elliptic curve cryptography and RSA on 8-bit CPUs[C]//Proc of the 6th International Workshop on Cryptographic Hardware and Embedded Systems. 2004: 925-943.

[3] MALAN D, WELSH M, SMITH M D. A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography[C]//Proc of the 1st IEEE International Conference on Communications and Networks (SECON). 2004: 71-80.

[4] DU Xiao-jiang, GUIZANI M, XIAO Yang, *et al*. A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks[J]. IEEE Trans on Wireless Communications, 2009, 8(3): 1223-1229.

[5] ESCHENAUER L, GLIGOR V D. A key management scheme for distributed sensor networks[C]//Proc of the 9th ACM Conference on Computer and Communication Security. 2002: 41-47.

[6] CHAN H, PERRIG A, SONG D. Random key pre-distribution schemes for sensor networks[C]//Proc of IEEE Symposium on Security and Privacy. 2003: 197-213.

[7] LIU Dong-gang, NING Peng, LI Rong-fang. Establishing pair-wise keys in distributed sensor networks[C]//Proc of the 10th ACM Conference on Computer and Communications Security. 2003: 52-61.

[8] ANJUM F. Location dependent key management using random key pre-distribution in sensor networks[C]//Proc of the 5th ACM Workshop on Wireless Security. 2006: 21-30.

[9] YOUNIS M F, GHUMMAN K, ELTOWEISSY M. Location-aware combinatorial key management scheme for clustered sensor networks[J]. IEEE Trans on Parallel and Distributed Systems, 2006, 17(8): 865-882.

[10] 苏忠, 林闯, 任丰原. 无线传感器网络中基于散列链的随机密钥分发方案[J]. 计算机学报, 2009, 32(1): 30-41.