“RFID密码算法”读书报告

姓名：金泽文 学号：PB15111604

摘要：

RFID技术因为其自动识别、数据交换、追踪定位等功能的优势，目前正在被广泛地应用在交通、军事、物流等等领域中。因而，RFID的安全性显得愈发重要。本报告针对RFID的两种密码算法：PRESENT和PICCOLO展开介绍与分析，同时对新的攻击模型——差分功耗攻击进行分析。

关键词：

RFID、PRESENT、PICCOLO、差分功耗攻击

1. 前言

RFID(radio frequency identification)技术的应用越来越广泛，安全性也越来越被人们所重视。但是由于RFID标签的硬件资源的有限，优秀的安全策略极为有限，一般只能采用轻量级加密算法。

目前，广泛采用的密码算法大致可分为两类：SP结构与Feistel结构。本报告针对两种结构选取其中的代表：PRESENT和PICCOLO进行介绍与分析。并在最后针对日前的新的攻击模型——差分功耗攻击进行调研与分析。

1. 两种典型RFID密码算法：PRESENT与PICCOLO

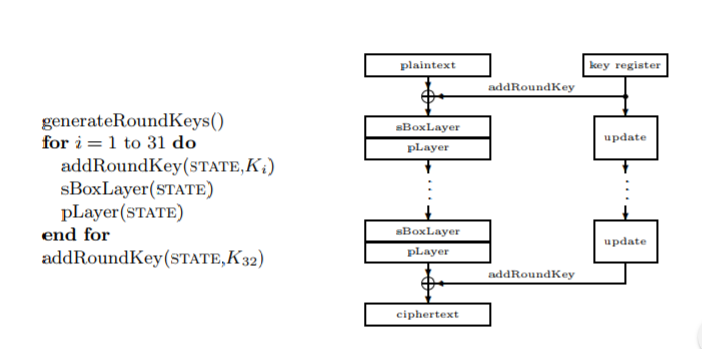
2.1 PRESENT密码算法

2.1.1 概述

PRESENT算法是一种超轻量级的分组加密算法，于2007年由Bogdanov等[1]提出。PRESENT算法是一个应用SP结构的例子，由31轮组成。它的分组数据长度是64位，密钥有80位和128位两种。针对硬件的超密集型结构的需求，一般以80位为主。PRESENT-80以仅需要1570GE闻名。

2.1.2算法

PRESENT算法主要分为密钥生成模块和轮函数运算模块两部分。密钥生成模块一个80位密钥寄存器，初始密钥为80 位，输入64位明文经过31轮的循环加密以及最后一轮的post-whiten变换，同时每一次轮变换进行密钥更新，得出轮密钥的值为密钥寄存器的高64位的值。轮函数运算模块由数据与轮密钥异或操作、S盒非线性置换操作、P位变换操作3部分组成。

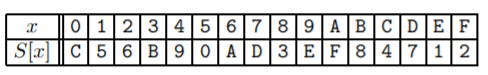
PRESENT算法的顶层模块架构如图一（左边为伪代码）。

对于31轮中的每一轮，依次进行addRoundKey，sBoxLayer，pLayer操作。最后进行post\_whiten操作。

图一

addRoundKey：对于目前的状态b与Ki两个输入，这一步生成每一位的异或操作的结果。

sBoxLayer：在PRESENT算法中使用的S盒使用的是4位到4位的，避免了8位的复杂性与冗余性。

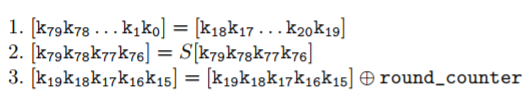
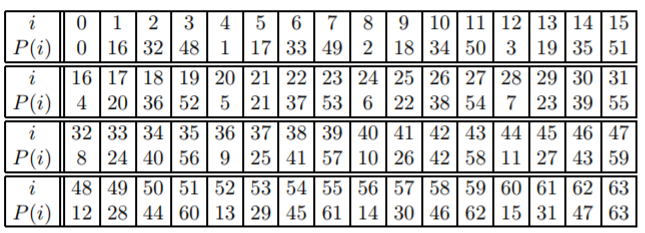
如表一：

表一

pLayer（permutation layer-置换层）：

PRESENT算法中采用了位置换，置换表如表二

表二

key schedule（密钥调度）：采用80位密钥。用户提供的密钥存在密钥寄存器K，输入64位明文经过31轮的循环加密，同时每一轮进行密钥更新，得出轮密钥的值为密钥寄存器的高64位的值。最后的密钥寄存器K中：

2.1.3安全性分析

a. 差分和线性密码分析：

差分和线性密码分析是两种最强大的密码分析技术。针对这两种技术，PRESENT算法采用了称作active S盒的策略。由于PRESENT中任意的五轮差分特性至少对应10个active S盒，得出一般差分分析的不可行性；另外得出线性密码分析的复杂性。针对一些高级的差分、线性攻击，PRESENT算法的特定结构也得到了很好的结果。

b. 结构攻击：

PRESENT算法由于是按位操作，并且虽然位置换有一定的规律性但是已经被彻底打乱，所以注入integral attacks和bottleneck attacks等典型结构攻击将不再具有威胁。

c. 代数攻击：

由于PRESENT中的4位S盒能被至少21个8位的二次方程所描述，所以整个密码能被e=n \* 21个含有v=n\*8个变量的二次方程所表示，（其中n表示算法中使用的S盒的数量）。PRESENT中n=(31\*16)+31，所以整个系统由11067个含有4216个变量的二次方程所表示。PRESENT的SP结构能够为这种代数攻击带来时间和内存上的绝对困难。

e.综上所述，以simpicity为宗旨的PRESENT算法有着强大的安全性与可靠性。

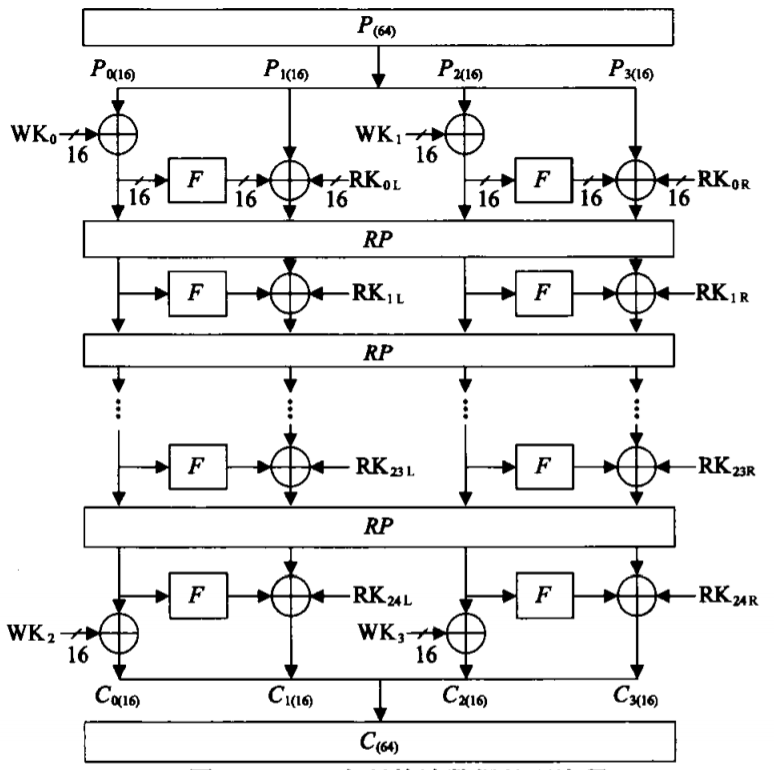
2.2 piccolo密码算法

2.2.1概述

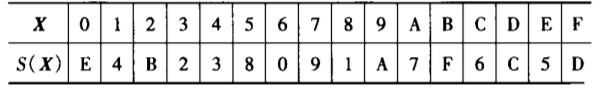
Piccolo算法采用广义Feistel结构，于索尼公司在2011的CHES2011上提出。Piccolo分组密码算法的分组长度为64位，支持80位和128位两种密钥长度，分别用Piccolo-80和Piccolo-128表示，对应的迭代轮数分别为25轮和31轮。本文以Piccolo-80为主。

2.2.2算法：

数据处理部分以64位明文、白化密钥和轮密钥为输入经由25轮迭代后产生64位密文输出，如图二所示。从图中可以看出，除最后一轮外，每轮包含两类变换，分别是函数F：GF(2^16)一GF(2^16)和轮置换RP：GF(2^64)一GF(2^64)，最后一轮不包含轮置换RP。

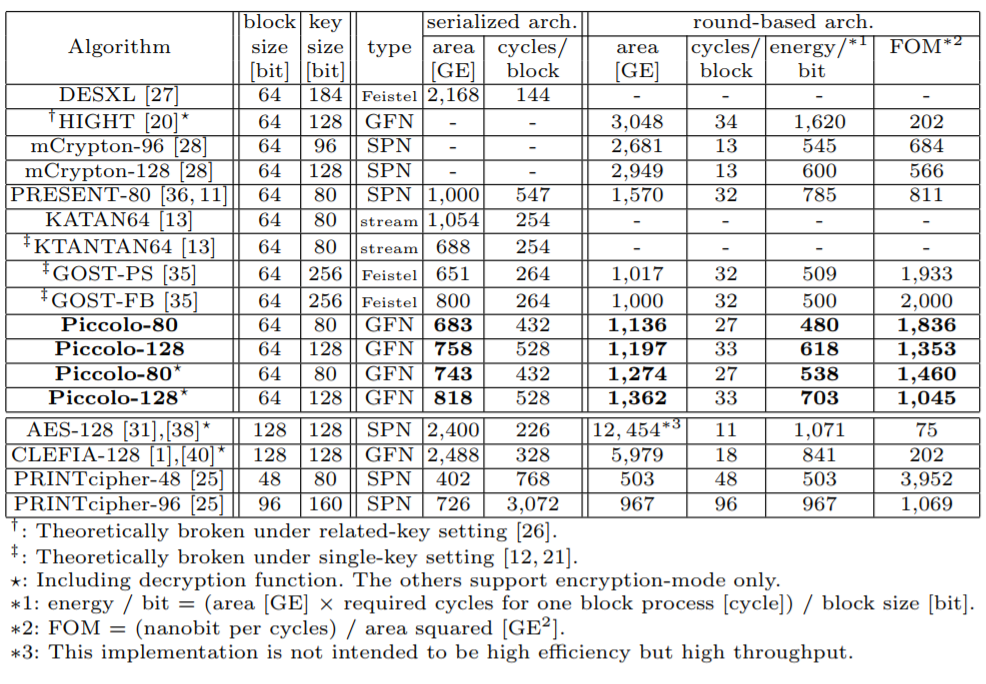
这里的函数F：GF(2^16)一GF(2^16)被称为超级S盒，采用两层S盒内夹混淆矩阵M层的三明治结构，具有更强的混淆能力，其中，S盒S：GF(24)一GF(24)是Piccolo中唯一的非线性操作，其映射关系如表三所示．

图二



表三

2.2.3分析：

首先是硬件实现上的比较分析，如表四。

表四

可以明显看出PICCOLO的强大的硬件优势。

然后是安全性的分析

a. 差分和线性密码分析：

根据文献[2]，PICCOLO至少有7/8轮提供至少7/8个active F函数，并且没有概率超过2^-64的差分/线性追踪轨迹。因此，PICCOLO对差分和线性密码分析具有足够强大的免疫力。

b. 其他攻击

根据文献[2]，PICCOLO对其他典型攻击，诸如回旋攻击、不可能差分攻击、相关密钥差分攻击等都有极好的免疫力。

1. 新的挑战与改进

3.1 新的攻击模型——功耗攻击

近年来，一种新的攻击模型横空出世——差分功耗攻击（Differential Power Analysis, DPA）。DPA利用的是智能卡中芯片的电力使用与所包含的密钥之间的关系。DPA通过测量芯片不同部分的功耗水平并应用统计分析来采取相应措施，比如采取用来掩饰single bit的补充噪音等。由于芯片的各种操作对应的特定区域的功耗水平的不同，DPA便可一次次得到可能的密钥，并通过大量的重复、统计，最终可以得到整个密钥。

DPA具有较小的时间复杂度，较低的成本，并且DPA攻击并非入侵式，所以很难留下痕迹，具有极大的攻击性。因此给密码算法带了个新的挑战。

3.2 对抗DPA的措施

目前有一些DPA防护措施的提出，但是由于RFID标签的有限资源，这些要求一定量芯片面积和功耗的措施并不适用于目前的条件。于是，对抗DPA的轻量级算法的研究显得愈发重要。针对这一问题，[3]中Poschmann等人提出了仅用2,300GE的PRESENT算法的可行性。他们将Threshold技术实现于串行化的PRESENT密码算法中，并且仅需2,300GE。

另一方面，[4]中王晨旭等人针对Poschmann的改进中的毛刺的潜在问题，提出了Threshold技术与PICCOLO算法结合的另一种改进方式，分别基于布尔式重组和改进型穷举搜索的方式实现了面积最优的S盒及其逆的threshold(3，3)分享，提出了基于锁存器方式解决S盒及其逆实现中潜在的毛刺威胁问题并且实现了只要求2155GE的方案。

1. 小结

RFID的应用确实越来越广泛，今后也将是热议的焦点。RFID标签的安全性也愈发受到重视。越来越多的轻量级密码算法的出现，与越来越多的攻击模型的产生，这种更迭与对抗将继续持续下去。通过本次的调研与学习，愈加体会到了社会的脆弱与韧性，RFID发展的纠结与活力，以及信息安全这个领域的挑战与振奋。这次报告调研了很多，学习了很多，感受到了自己很多的不足，也感受到了物联网发展的无尽未来。

参考文献

[1] A. Bogdanov, L.R. Knudsen, G. Leander et al. Present: An Ultra-lightweight Block cipher[A]. Proc of Cryptugraphic Hardware and Embedded Systems[C]. 2007. 450-466.

[2] Kyoji Shibutani, Takanori Isobe，et al. Piccolo：An Ultra-lightweight Blockcipher[A]．2011 13th International Workshop on Cryptographic Hardware and Embedded Systems Proceedings[C]. 2011. 342-357.

[3] Axel Poschmann, Amir Moradi, Khoongming Khoo, et al. Side-channel resistant crypto for less than 2,300 GE[J]. Jounal of Cryptology. 2011, 24(2). 322-345.

[4]王晨旭, 韩良, 喻明艳, 王进祥. 一种适用于RFID标签的安全化密码算法实现[J]. 电子学报, 2014, 42(8). 1465-1473.

WANG Chen-xu, HAN Liang, YU Ming-yan, WANG Jin-xiang. A Secure Cipher Implementation Suitable for RFID-Tags. Chinese Journal of Electronics, 2014, 42(8): 1465-1473.