“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。

2. 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。

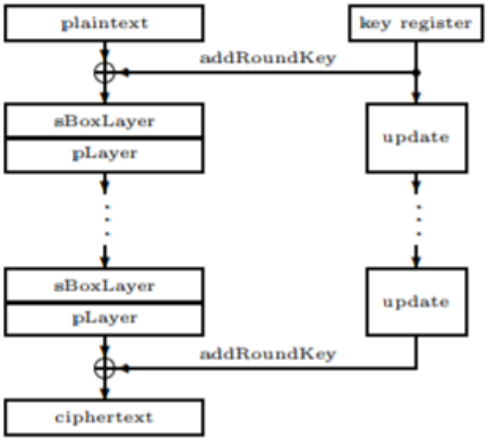
2.1.2 算法

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，

```
generateRoundKeys()
for i = 1 to 31 do
   addRoundKey(STATE,K_i)
   sBoxLayer(STATE)
   pLayer(STATE)
end for
addRoundKey(STATE,K_32)
```



图一

pLayer 操作。最后进行 post_whiten 操作。

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：

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

表一

pLayer（permutation layer-置换层）：

PRESENT 算法中采用了位置换，置换表如表二

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P(i)$	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P(i)$	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

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：

1. $[k_{79}k_{78}\ldots k_1k_0] = [k_{18}k_{17}\ldots k_{20}k_{19}]$
2. $[k_{79}k_{78}k_{77}k_{76}] = S[k_{79}k_{78}k_{77}k_{76}]$
3. $[k_{19}k_{18}k_{17}k_{16}k_{15}] = [k_{19}k_{18}k_{17}k_{16}k_{15}] \oplus \texttt{round\_counter}$

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

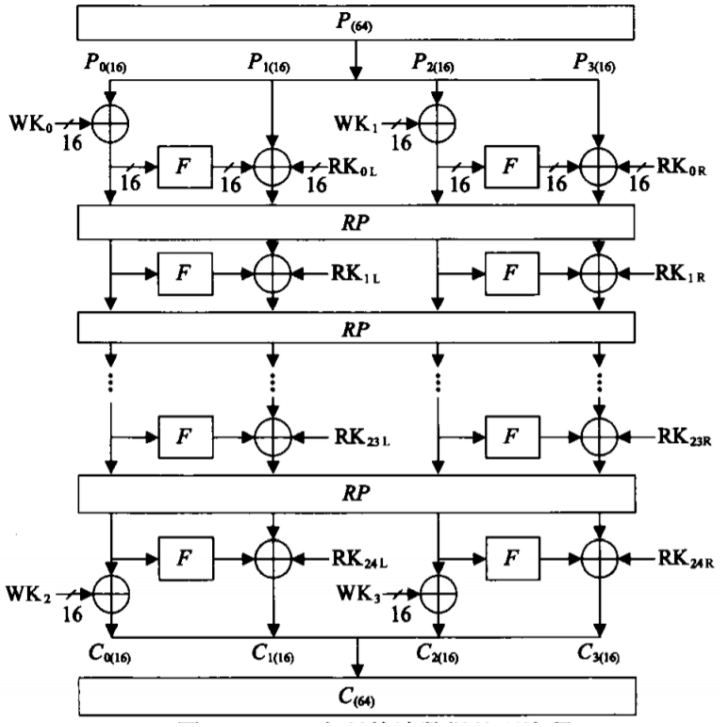
Piccolo 算法采用广义 Feistel 结构，于索尼公司在 2011 的 CHES2011 上提出。Piccolo 分组密码算法的分组长度为 64 位，支持 80 位和 128 位两种密钥长度，分别用 Piccolo-80 和 Piccolo-128 表

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)— GF(2^16)和轮置换 RP：GF(2^64)— GF(2^64)，最后一轮不包含轮置换 RP。

这里的函数 F：GF(2^16)— GF(2^16)被称为超级 S 盒，采用两层



图二

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)— GF(24)是 Piccolo 中唯一的非线性操作，其映射关系如表三所示．

X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(X)$	E	4	B	2	3	8	0	9	1	A	7	F	6	C	5	D

表三

2.2.3 分析：

首先是硬件实现上的比较分析，如表四。

Algorithm	block size [bit]	key size [bit]	type	serialized arch. area [GE]	serialized arch. cycles/ block	round-based arch. area [GE]	round-based arch. cycles/ block	round-based arch. energy/*1 bit	round-based arch. FOM*2
DESXL [27]	64	184	Feistel	2,168	144	-	-	-	-
†HIGHT [20]⋆	64	128	GFN	-	-	3,048	34	1,620	202
mCrypton-96 [28]	64	96	SPN	-	-	2,681	13	545	684
mCrypton-128 [28]	64	128	SPN	-	-	2,949	13	600	566
PRESENT-80 [36, 11]	64	80	SPN	1,000	547	1,570	32	785	811
KATAN64 [13]	64	80	stream	1,054	254	-	-	-	-
‡KTANTAN64 [13]	64	80	stream	688	254	-	-	-	-
‡GOST-PS [35]	64	256	Feistel	651	264	1,017	32	509	1,933
‡GOST-FB [35]	64	256	Feistel	800	264	1,000	32	500	2,000
Piccolo-80	64	80	GFN	**683**	432	**1,136**	27	**480**	**1,836**
Piccolo-128	64	128	GFN	**758**	528	**1,197**	33	**618**	**1,353**
Piccolo-80⋆	64	80	GFN	**743**	432	**1,274**	27	**538**	**1,460**
Piccolo-128⋆	64	128	GFN	**818**	528	**1,362**	33	**703**	**1,045**
AES-128 [31],[38]⋆	128	128	SPN	2,400	226	12,454*3	11	1,071	75
CLEFIA-128 [1],[40]⋆	128	128	GFN	2,488	328	5,979	18	841	202
PRINTcipher-48 [25]	48	80	SPN	402	768	503	48	503	3,952
PRINTcipher-96 [25]	96	160	SPN	726	3,072	967	96	967	1,069

†: Theoretically broken under related-key setting [26].
‡: Theoretically broken under single-key setting [12, 21].
⋆: Including decryption function. The others support encryption-mode only.
∗1: energy / bit = (area [GE] × required cycles for one block process [cycle]) / block size [bit].
∗2: FOM = (nanobit per cycles) / area squared [GE^2].
∗3: This implementation is not intended to be high efficiency but high throughput.

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。

3. 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。

4. 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.