·安全技术· 文章编号：1000-3428(2015)03-0110-06 文献标识码：A 中图分类号：TP309

基于 PRESENT 算法的安全标签基带设计

秦 琴[1]，李 聪[2]，蔡 磊[1]，黄 冲[2]，郭俊平[1]，李建成[2]

（1. 湘潭大学材料与光电物理学院，湖南 湘潭 411005；2. 国防科学技术大学电子科学与工程学院，长沙 410073）

摘 要： 针对无线射频识别（RFID）标签芯片中存在的安全问题，设计一款具有安全功能的 UHF RFID 标签基带，该基带遵循我国自主射频识别空中接口协议 GJB 7377.1－2011。通过研究 RFID 标签的设计需求和安全策略，给出基于 PRESENT 加密算法和安全协议的标签安全性设计方案。基带设计采用寄存器分时复用、功耗管理、多时钟域设计、门控时钟等低功耗策略。实验结果表明，该数字基带符合自主标准，具有安全功能，基带总面积为 339.84 μm×332.56 μm，其中安全模块占总面积的 36.5%，基带总功耗低至 5.26 μW。

关键词： 无线射频识别；PRESENT 算法；自主标准；安全标签；数字基带；低功耗

中文引用格式： 秦 琴，李 聪，蔡 磊，等. 基于 PRESENT 算法的安全标签基带设计[J]. 计算机工程，2015，41(3)：110-115.

英文引用格式： Qin Qin，Li Cong，Cai Lei，et al. Design of Security Tag Baseband Based on PRESENT Algorithm[J]. Computer Engineering，2015，41(3)：110-115.

Design of Security Tag Baseband Based on PRESENT Algorithm

QIN Qin[1]，LI Cong[2]，CAI Lei[1]，HUANG Chong[2]，GUO Junping[1]，LI Jiancheng[2]

（1. School of Materials and Optoelectronics Physics，Xiangtan University，Xiangtan 410005，China；
2. College of Electronic Science and Engineering，National University of Defense Technology，Changsha 410073，China）

【Abstract】 To improve the security and privacy problems in Radio Frequency Identification（RFID）tags，a low power UHF RFID security tag baseband in accordance with the independent national protocol（GJB 7377.1－2011）is designed. Through studying RFID tags' security strategy and comparing plenty of cryptographic algorithms，PRESENT cryptographic algorithm and security protocol are used to ensure tag's security. Reuse of several blocks，time-sharing reuses of registers，power management and multiple time regions design are employed to minimize the power consumption of baseband. Experimental results show that the baseband is in accordance with the independent national UHF RFID standard and has security function. The area of the digital baseband is 369.84 μm×362.56 μm，of which the security module takes 36.5%，and the power consumption of the baseband is 5.26 μW.

【Key words】 Radio Frequency Identification（RFID）；PRESENT algorithm；independent standard；security tag；digital baseband；low power consumption

DOI： 10.3969/j.issn.1000-3428.2015.03.021

1 概述

无线射频识别（Radio Frequency Identification，RFID）技术是通过空间耦合实现信息无接触传递，并通过传递的信息来识别特定目标的技术。RFID 技术广泛应用公共交通、供应链管理、公共管理、安全防伪、运动赛事、工业自动化、医疗等诸多领域[1-2]。

RFID 系统的通信主要通过电磁波传输，这种非接触的无线通信很容易受到窃听和干扰，RFID 系统面临着信息被非法监听、窃取甚至篡改等安全威胁[3]。安全与隐私问题已经成为决定 RFID 系统能否更为广泛应用的重要因素。

我国的 RFID 技术起步较晚，目前超高频芯片的设计大都使用国外的标准，如 ISO/IEC 18000-6C（以下简称 6C）、EPC class1 gen2、Ubiquitous ID 等，其中 6C 是 SIO/IEC 通过适当修改 EPC class1 gen2 而制定，最为常用。在 6C 协议中存在着若干安全问题，6C 中采用的数据保护是在执行写入操作时，用一个 16 位

作者简介： 秦 琴（1990－），女，硕士研究生，主研方向：加密算法，数字集成电路设计；李 聪，博士研究生；蔡 磊、黄 冲、郭俊平，硕士研究生；李建成，教授。

收稿日期： 2014-03-17 **修回日期：** 2014-05-11 **E-mail：** qinqin7799@163.com

的随机数与待写入的数据异或后传送,虽然避免了明文传输,但是攻击者可以很容易地截获用于异或操作的 16 位的随机数,从而分析出要写入标签的信息,甚至冒充合法读写器对标签的数据任意篡改。

具有我国自主知识产权的 RFID 标准:《军用射频识别空中接口第一部分:800/900 MHz》(以下简称自主标准)于 2011 年 10 月 1 日正式颁布[4],该标准规定了 840 MHz ~845 MHz 及 920 MHz ~925 MHz超高频频段的通信协议和空中接口规范。相比于 6C,自主标准根据数据密级需要,选择是否工作在安全模式。在安全模式下,读写器和标签通信前需要进行安全鉴别。安全鉴别通过后,重要信息以密文的方式传输,读写器每次发起请求时都会首先发送一个随机数,能有效抵抗重放攻击、假冒攻击、跟踪攻击和篡改攻击等安全威胁。

本文通过研究 RFID 标签数字基带的安全技术,设计了一款基于自主标准、具有安全功能、低功耗的无源 UHF RFID 标签数字基带。

2　标签芯片的安全性

2.1　安全标签芯片的设计要求

标签的安全性主要解决标签与读写器的合法性认证及数据保密的问题,以防止跟踪、窃取、非法访问或篡改标签信息的行为。

受芯片成本的限制,标签芯片的硬件资源十分有限,用于实现安全功能的硬件资源更少。对存储容量为几百位的标签,用于实现安全功能的等效门电路数仅为 250 门 ~5 000 门[5]。

对于无源标签,标签工作的能量由整流读写器发送的电磁波获得,标签的工作距离与功耗成反比。降低标签的功耗能有效提高无源标签的工作距离。

RFID 安全性设计的目标是用最小的芯片面积,确保标签信息在存储、处理和传输过程中的有效性和安全性,并尽可能地降低芯片的功耗。

2.2　标签芯片安全性机制

目前,实现 RFID 安全防护所采用的方法主要有物理安全机制和密码安全机制[6]。

物理安全机制是采用物理方法保护标签的安全性。常用的物理安全机制有静电屏蔽、阻塞标签、Kill 命令机制、剪裁标签和主动干扰等[7]。使用物理安全机制需增加额外设备或破坏标签,存在较多的局限性。

密码安全机制通过认证协议和消息密文传输保证数据安全。

认证是指在信息交互前,读写器和标签对对方身份的合法性的判定。标签有 3 种认证方式:读写器对标签的单向认证;标签对读写器的单向认证;读写器与标签的双向认证。

消息密文传输是指将重要数据用加密算法和加密密钥加密后传输,接收方接到数据后通过解密算法和解密密钥将密文恢复成明文。在通常情况下,标签与读写器间的无线通信为明文传输,通信信息容易被攻击者获取和利用。当消息密文传输时,即使信息被截获,攻击者也不知道信息内容。同时,标签不响应非法读写器的相关操作,有效地防止了篡改攻击。

与物理安全机制相比,密码安全机制更加经济、灵活和便捷。本文设计的基带,通过安全协议和加密算法的使用来保证标签的安全性。

3　安全功能实现

3.1　安全协议

基带设计遵循自主标准中的双向鉴别协议和安全通信协议。

自主标准中的双向鉴别协议是基于 Hash 函数与密钥更新的双向安全认证协议,既解决了已有协议存在的安全问题,同时能够满足无源标签计算能力与存储容量的苛刻要求。

图 1 为读写器和标签的双向鉴别协议流程。首先读写器发送安全参数获取命令,收到命令后,标签将包含加密算法、密钥长度、安全模式、安全功能及响应参考时间的安全参数发送给读写器。接着读写器发送请求加密鉴别命令,收到命令后,标签生成随机数 RN_t 发送给读写器。之后读写器用根密钥 AK 加密接收到的 RN_t 及生成的随机数 RN_r 和会话密钥 SK,发送双向鉴别命令。收到命令后,标签用根密钥 AK 解密接收到的数据,并将接收到的随机数RN_t'与跟发送的 RN_t 进行比较,若两者相等,则判定读写器通过安全鉴别,且会话密钥为 SK,并将随机数RN_r'发送给读写器。读写器比较接收到的RN_r'和发送的 RN_r,若两者相等,则判定标签通过安全鉴别。

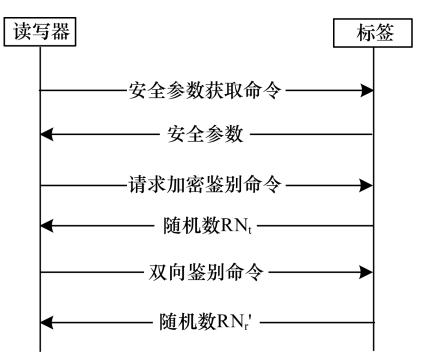

图 1　双向鉴别协议

读写器和标签通过鉴别后,便可按图 2 所示的安全通信协议流程进行通信[3]。读写器生成随机数 RN_t,用会话密钥 SK 加密随机数和通信命令。随后,标签用 SK 解密接收的数据,并根据通信命令类型做相应的处理,同时将响应数据和生成的随机数 RN_r 用 SK 加密后返回给读写器。通信协议中会话密钥和随机数的引用能有效防止跟踪、重放攻击等安全威胁。

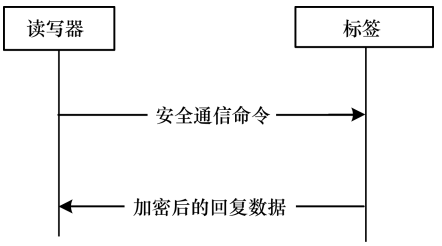

图 2 安全通信协议

3.2 加密算法选取及实现

在 RFID 系统中,标签有严格的成本限制,硬件资源非常有限[8],难以使用较复杂的加密算法来保障标签和读写器之间的通信安全,因此,加密算法的简洁高效至关重要。

3.2.1 加密算法的选取

随着 RFID 的广泛应用,国内外学者提出了很多用于 RFID 应用的轻量级加密算法,如 Hight,mCrypton,DESL,PRESENT 等[9-12]。表 1 为上述算法的比较。

表 1 轻量级算法的比较

算法	密钥/bit	明文/bit	周期数	吞吐率/(Kb·s^{-1})	等效门数
PRESENT-80[13]	80	64	32	200.0	1 570
mCryton[14]	64	64	13	492.3	2 420
AES-128[15]	128	128	1 032	12.4	3 100
Hight[16]	128	64	34	188.2	3 048
DES[17]	56	64	144	44.4	2 309
DESL[17]	56	64	144	44.4	1 848
DESXL[17]	184	64	144	44.4	2 168
Ktantan-64[18]	80	64	254	25.2	688
Katan-64[18]	80	64	254	25.2	1 054
MIBS-80[19]	80	64	32	200.0	1 530
Puffin[20]	128	64	132	194.0	2 577
Klein-80[21]	80	64	17	376.0	2 475
Humingbird-1[22]	256	16	16	100.0	2 167
Humingbird-2[23]	128	16	16	100.0	2 332
Trivium[10]	80	1	1	100.0	2 599
Grain-80[24]	80	1	1	100.0	1 294

从表中可以看到,PRESENT,DESL,Ktantan,Katan,Grain 5 种算法硬件实现所需的面积较小。考虑到自主标准规定读写器发送命令后,标签需在一定时间范围响应,因此,吞吐率较小的 DESL,Ktantan,Katan 算法不利于读写器与标签的信息交互。Grain 算法所需的门数较低,但算法消耗的功率较大[10],不适合要求低功耗的标签芯片。综合考虑,基带设计选用面积和吞吐率都较优的 PRESENT 算法。

3.2.2 PRESENT 算法的硬件实现

PRESENT 是由 Bogdanov 等人于在 2007 年的 CHES 会议上在提出的轻量级分组密码[13],加密流程如图 3 所示。算法采用 SPN 结构,分组长度为 64 位,支持 80 位和 128 位 2 种密钥长度,共迭代 31 轮。使用 128 位密钥时,密钥更新时使用 2 个 S 盒,同时需要 128 位的寄存器,增加了额外的门数和功耗,而使用 80 位密钥的足以提供满足 RFID 众多应用的安全等级[25],故本设计选用长度为 80 位的密钥。

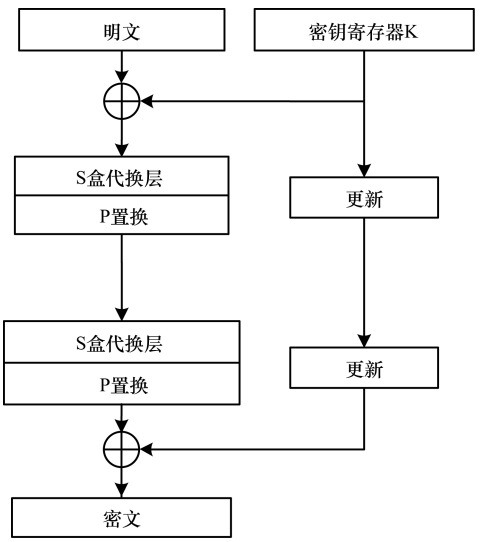

图 3 PRESENT 加密流程

根据 PRESENT 加密运算过程,其硬件实现结构可以有并行处理、串行处理及循环迭代 3 种。并行处理结构可以在 1 个时钟周期内完成加密过程,但硬件实现时需共用到 496 个 S 盒和 31 个 64 位的寄存器,占用硬件资源多,适合高速或实时数据处理等应用场合。串行处理一次处理 4 位数据,完成加密过程仅需用到一个 S 盒,硬件实现时所需的硬件资源少,消耗的功耗低。不足之处是完成一轮运算需要 16 个周期,完全所有加密需要 497 个时钟周期,仅适用与对时间没有限制的应用场合。循环迭代结构中,需要的硬件资源和时钟周期及消耗的功耗介于并行处理结构和串行处理结构之间,包含 16 个 S 盒,完成一次加密过程需 32 个时钟周期,适合对实

时性要求不高,硬件资源有限,低功耗的应用。本文的硬件设计采用循环迭代结构。

采用循环迭代结构,PRESETN 算法的硬件实现如图 4 所示。图 4 左部分是数据路径的块加密操作,首先一个 64 位的 2 选 1 选择器选择初始明文或上一轮加密后的数据作为输入,并存储在一个64 位的寄存器中。接着数据与轮密钥的右 64 位进行逐位异或。然后 6 位的轮计数器判断是否为第32 轮,若是,则直接输出数据,即密文,否则将数据依次通过 S 盒代换层和 P 置换层。S 盒将一个 4 位的数值用另一个 4 位的数值替代,保证了数据的随机性和非线性,S 盒层由 16 个并行的 S 盒构成。P 置换层是将原来的数值重新排列,保证了算法的非线性。P 置换层直接由连线实现。

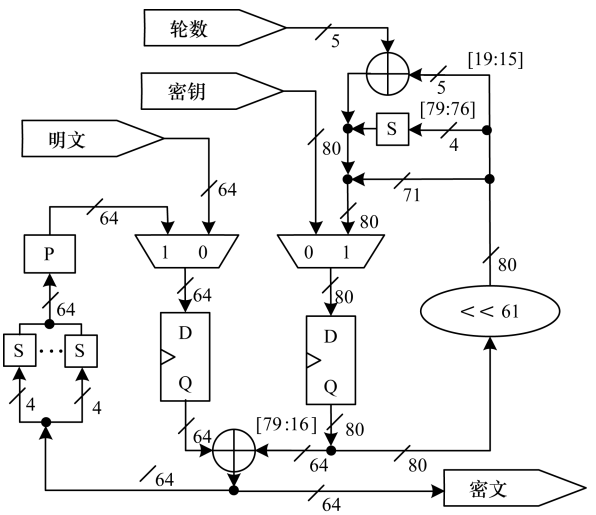

图 4　PRESENT 硬件实现

图 4 右部分为密钥更新操作。一个 80 位二选一选择器根据轮计数器数值选择密钥,除第一轮使用初始密钥外,其他轮的运算均使用上一轮的更新密钥。密钥跟新由移位操作(循环左移 61 位)、左 4 位的 S 盒代换和 19 位 ~15 位的数值与轮数的异或组成。硬件实现时需用到一个 80 位的移位寄存器、一个 S 盒和一个 5 位的异或器。注意到块加密和密钥跟新使用相同的 S 盒,且它们分别在一个时钟周期的高电平和低电平阶段完成,因此,硬件实现时对 S 盒进行复用,节约了部分硬件资源。此外,轮密钥在每轮加密之前计算,使用后进行更新,这样节省大量的存储单元。

4　基带总体设计及低功耗设计

4.1　基带总体设计

本文设计的数字基带总体结构如图 5 所示。首先标签上电后初始化模块完成初始化存储区、读取标签状态和鉴别密钥、产生随机化种子等操作。随后,解密模块对射频模拟前端解调后的 TPP 编码信号进行解码,并将命令头和命令中的参数分别传至命令解析模块和接收模块,需要进行解密操作的参数传送至安全模块。接着状态机模块作根据接收到的参数作相应的状态跳转,发送模块完成标签的响应操作,并将需要进行加密的数据传至安全模块。最后,标签的响应由编码模块编码输出。各个模块与存储的数据交互由存储器控制模块完成。功耗管理模块负责为其他各个模块产生使能信号;分频模块对系统主时钟进行分频,产生其他各模块工作所需的时钟信号。

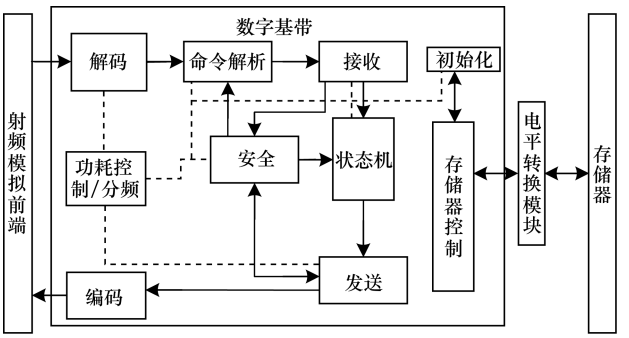

图 5　数字基带结构

4.2　低功耗设计

4.2.1　寄存器分时复用

多位寄存器占相当多的硬件资源,所使用的工艺中,一个带异步复位的触发器所占面积为 7.5 个等效门电路。数字基带中安全功能的使用需要用到大量寄存器,接收模块对安全鉴别命令的数据、安全通信命令的数据进行了分时复用,节约了一个 64 位的寄存器。

4.2.2　功耗管理

通过功耗管理模块中的使能信号控制模块中主要时钟的关断,让各个模块依次工作,未用到的模块处于关断状态,大大减小了动态功耗。

4.2.3　时钟域策略

自主标准对反向链路频率允差有苛刻规定,为了达到时钟频率精度要求,时钟频率需大于 1.60 MHz[26]。自主标准中反向链路时钟最高频率为 640 KHz[4],本文通过主时钟分频的方式产生链路时钟,故选取1.92 MHz 作为基带的主时钟频率。

动态功耗与频率成正比,本设计使用主时钟频率、链路时钟频率、主时钟频率的八分频 3 个时钟域,使不同模块根据需要工作在不同时钟频率下。解码模块在主时钟频率下工作,保证了反向链路频率允差。存储器控制模块在初始化时工作频率为主时钟频率的八分频,用最低频率完成了从存储器读取所需数据操作。其余模块在频率适中的链路时钟

频率下工作,保证了标签的反应速度。这种多时钟域的设计在保证基带功能和效率的同时大大降低了基带的总功耗。

4.2.4 门控时钟

通过使用门控时钟进一步降低功耗。表 2 给出对芯片数字基带进行逻辑综合后的功耗和面积报告。可以看出,使用门控时钟后,设计的动态功耗降低很多,并且,在降低功耗的同时,面积也有了一定的减小。

对基带进行物理设计,面积为 339.84 μm × 332.56 μm,约 12 872 门。其中,安全模块所占面积为 339.8 μm × 121.48 μm,占基带总面积的 36.5% 。进行功耗分析,工作电压为 1.0 V,系统时钟采用 1.92 MHz,总功耗 5.26 μW,各个模块的功耗分布如表 2所示。可以看出,由于需要多次对数据进行加解密,安全模块消耗的功耗较大。其功耗分布如图 6 所示。

表 2 使用门控时钟前后的功耗和面积报告

指标	未使用门控时钟	使用门控时钟
动态功耗/μW	30.55	5.26
泄露功耗/nW	146.34	138.26
面积/μm^2	118 145.73	102 228.34

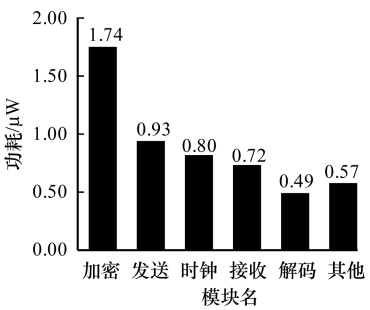

图 6 各模块的功耗分布

5 FPGA 验证及对比分析

5.1 FPGA 验证

建立 RFID 读写器的仿真模型,并用该模型向标签数字基带发送相关的操作命令,对数字基带进行功能验证。验证结果显示,当读写器未通过安全鉴别时,标签对读写器的访问命令不予响应,数字基带具有一定的安全性。图 7 为读写器模型与标签进行安全鉴别和安全通信的仿真结果。

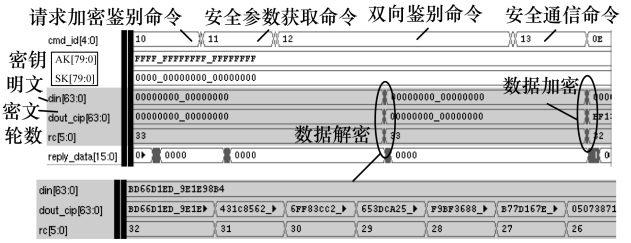

图 7 安全鉴别和安全通信仿真结果

基于 FPGA 开发标签模拟器,将标签数字基带下载到 FPGA,得到标签原型。用基于 NI-VISN-100 射频识别软件无线电平台搭建的模拟读写器发送命令,与标签之间进行通信,完成标签数字基带的原型验证。图 8 为测试平台实物图。图 9 给出了发送 Query 命令时,示波器测得的模拟读写器和标签响应的波形。

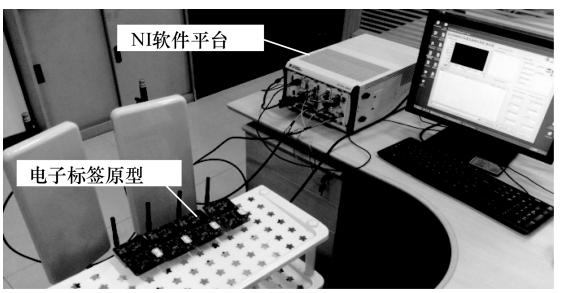

图 8 原型验证平台

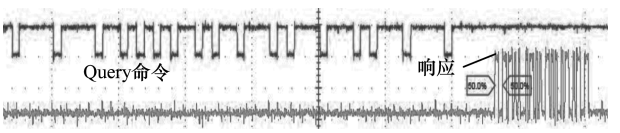

图 9 Query 命令和标签响应的测试波形

5.2 与其他基带方案的对比分析

目前,具有安全功能的标签芯片较少。表 3 将本文的设计与同类工作进行对比,与文献[27]相比,本文设计的基带面积更小,功耗更低,与文献[28]相比,面积更低,功耗略大,与文献[29]相比,安全模块所占的面积更小,而且本文设计采用了复杂的安全协议,更能保证标签的通信安全。在表 3 中,部分数据文献[28]没给出明确数值,*1 表示根据面积和工艺折算,*2 表示根据版图估算。

表 3 本文基带方案与其他基带方案对比

方案	协议	系统时钟/MHz	工作电压/V	加密算法	门数	安全模块所占面积比例/%	功耗/μW
文献[27]	EPC class1 gen2	1.28	1.2	Hummingbird	16 986	23.6	30.67
文献[28]	EPC class1 gen2	3.55	1.8	AES	50 981 *1	36.6 *2	4.695
文献[29]	ISO/IEC 18000-6C	2.00	0.6	AES	11 572	51.9	2.500
本文方案	自主标准	1.92	1.0	PRESENT	12 872	36.5	5.260

6　结束语

本文通过研究我国自主标准及标签设计的安全策略,比较分析多种加密算法和研究标签的安全协议,提出基于 PRESENT 算法,设计一款双向认证协议与安全通信协议的符合自主标准的 UHF RFID 安全标签数字基带。通过模块划分、模块复用、寄存器分时复用、引入功耗管理模块、多时钟域方案以及门控时钟等方法,使整个基带的功耗低至 5.26 μW。FPGA 验证结果表明,本文设计的标签符合自主标准,具有安全功能。采用 TSMC 0.18 μm mix RF 工艺,数字基带总门数为 12 872,其中安全模块占 36.5% 。

参考文献

[1] Klaus F. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-field Com-munication[M]. 3rd ed. [S. 1.]: Wiley, 2010.

[2] 林为民,张　涛,马媛媛,等. 射频识别(RFID)技术应用及其安全[M]. 北京:电子工业出版社,2013.

[3] Thornton F, Haines B, Das A M, et al. RFID Security[M]. [S. 1.]: Syngress Publishing, 2006.

[4] 解放军总装备部. GJB 7377.1-2011 军用射频识别空中接口第一部分:800/900MHz 参数[S]. 2011.

[5] 粟　伟,崔　喆. 基于 Hash 链的 RFID 隐私增强标签研究[J]. 计算机应用,2006,26(10):2328-2331.

[6] Juels A. RFID Security and Privacy: A Research Survey[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 381-394.

[7] Juels A, Rivest R L, Szydlo M. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy[C]//Proceedings of the 10th ACM Conference on Computer and Communications Security. [S. 1.]: ACM Press, 2003: 103-111.

[8] Robshaw M J B. An Overview of RFID Tags and New Cryptographic Developments[J]. Information Security Technical Report, 2006, 11(2): 82-88.

[9] Maimut D, Ouafi K. Lightweight Cryptography for RFID Tags[J]. IEEE Security & Privacy, 2012, 10(2): 76-79.

[10] Good T, Benaissa M. Hardware Results for Selected Stream Cipher Candidates[J]. State of the Art of Stream Ciphers, 2007: 191-204.

[11] Kitsos P, Sklavos N. A Comparative Study of Hardware Architectures for Lightweight Block Ciphers[J]. Computers & Electrical Engineering, 2012, 38(1): 148-160.

[12] Engels D, Fan X. Hummingbird: Ultra-lightweight Cryptography for Resource-constrained Devices[C]//Proceedings of Financial Cryptography and Data Security Conference. Berlin, Germany: Springer, 2010: 3-18.

[13] Bogdanov A, Knudsen L R, Leander G, et al. PRESENT: An Ultra-lightweight Block Cipher[C]//Proceedings of CHES'07. Berlin, Germany: Springer, 2007: 450-466.

[14] Lim C H, Korkishko T. mCrypton——A Lightweight Block Cipher for Security of Low-cost RFID Tags and Sensors[C]//Proceedings of Information Security Applications Conference. Berlin, Germany: Springer, 2006: 243-258.

[15] Feldhofer M, Wolkerstorfer J, Rijmen V. AES Implementation on a Grain of Sand[J]. IEE Proceedings-information Security, 2005, 152(1): 13-20.

[16] Hong D, Sung J. HIGHT: A New Block Cipher Suitable for Low-resource Device[C]//Proceedings of CHES'06. Berlin, Germany: Springer, 2006: 46-59.

[17] Poschmann A, Leander G. New Light-weight Crypto Algorithms for RFID[C]//Proceedings of ISCAS'07. Berlin, Germany: Springer, 2007: 1843-1846.

[18] de Canniere C, Dunkelman O, Knežević M. KATAN and KTANTAN——A Family of Small and Efficient Hardware-oriented Block Ciphers[C]//Proceedings of CHES'06. Berlin, Germany: Springer, 2009: 272-288.

[19] Izadi M, Sadeghiyan B, Sadeghian S S, et al. MIBS: A New Lightweight Block Cipher[C]//Proceedings of Cryptology and Network Security Conference. Berlin, Germany: Springer, 2009: 334-348.

[20] Cheng H, Heys H M. Puffin: A Novel Compact Block Cipher Targeted to Embedded Digital Systems[C]//Proceedings of the 11th EUROMICRO Conference on Digital System Design Architectures, Methods and Tools. [S. 1.]: IEEE Press, 2008: 383-390.

[21] Gong Z, Nikova S. KLEIN: A New Family of Lightweight Block Ciphers[C]//Proceedings of Security and Privacy Conference. Berlin, Germany: Springer, 2012: 1-18.

[22] 肖梦琴,沈　翔,杨玉庆,等. Hummingbird 算法在射频识别标签中的应用[J]. 计算机工程,2011,37(17):78-80.

[23] Engels D, Saarinen M J O, Schweitzer P, et al. The Hummingbird-2 Lightweight Authenticated Encryption Algorithm[C]//Proceedings of Security and Privacy Conference. Berlin, Germany: Springer, 2012: 19-31.

[24] Hell M, Johansson T, Meier W. Grain: A Stream Cipher for Constrained Environments[J]. International Journal of Wireless and Mobile Computing, 2007, 2(1): 86-93.

[25] Rolfes C, Poschmann A, Leander G, et al. Ultra-lightweight Implementations for Smart Devices——Security for 1 000 Gate Equivalents[C]//Proceedings of Smart Card Research and Advanced Applications Conference. Berlin, Germany: Springer, 2008: 89-103.

[26] 李　聪,谷晓忱,李建成,等. 一种对时钟偏差不敏感的无源 RFID 标签编解码算法[J]. 国防科技大学学报,2013,35(3):126-131.

[27] Xiao M, Shen X, Wang J, et al. Design of a UHF RFID Tag Baseband with the Hummingbird Cryptographic Engine[C]//Proceedings of ASIC'11. [S. 1.]: IEEE Press, 2011: 800-803.

[28] Man A S W, Zhang E S, Lau V K N, et al. Low Power VLSI Design for a RFID Passive Tag Baseband System Enhanced with an AES Cryptography Engine[C]//Proceedings of Radio Frequency Identification Conference. [S. 1.]: IEEE Press, 2007: 1-6.

[29] Ricci A, Grisanti M, De Munari I, et al. Design of a 2 μW RFID Baseband Processor Featuring an AES Cryptography Primitive[C]//Proceedings of the 15th IEEE International Conference on Electronics, Circuits and Systems. [S. 1.]: IEEE Press, 2008: 376-379.

编辑　索书志