一种低成本物理不可克隆函数结构的设计实现及其RFID应用

刘伟强,崔益军,王成华
(南京航空航天大学电子信息工程学院雷达成像与微波光子技术教育部重点实验室,江苏南京 210016)

摘 要: 物理不可克隆函数(PUF:Physical Unclonable Function)是一种新型的加密组件,具有防伪、不可克隆及不可预测等特性.本文提出了一种新型的低成本PUF,与传统PUF相比更适用于无线射频识别(Radio Frequency Identification,RFID)系统.该PUF结构主要由上电密钥生成器和混合函数两部分构成.上电密钥生成器由比特生成器阵列构成,混合函数则由低成本流加密算法构成,其作用是隐藏密钥生成器,以提高安全性.此外,本文还提出了择多模块和多寻认证协议来改善PUF响应及其在RFID系统中的稳定性.实验表明,该PUF的硬件成本低并且具有很好的稳定性,非常适用于RFID系统等资源受限的应用场合.

关键词: 物理不可克隆函数; RFID系统; 择多模块; 多寻认证协议
中图分类号: TN492 **文献标识码:** A **文章编号:** 0372-2112 (2016)07-1772-05
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.07.036

Design and Implementation of a Low-Cost Physical Unclonable Function and Its Application in RFID

LIU Wei-qiang, CUI Yi-jun, WANG Cheng-hua
(*Key Laboratory of Radar Imaging and Microwave Photonics (Ministry of Education), College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, Jiangsu* 210016, *China*)

Abstract: Physical unclonable function (PUF) is a kind of new encryption primitive, which has the properties of anti-counterfeiting, unclonability and unpredictability. In this paper, a low-cost PUF design is presented along with its application into RFID systems. The PUF structure includes two parts: a key generator and a low-cost stream cipher that is used to hide the key. A novel post-processing module i. e., majority voting, and a new multi-query protocol are introduced to improve the stability and reliability. The proposed reliable and low-cost PUF solution is well suitable for RFID applications.

Key words: physical unclonable function; RFID; majority voting; multi-query protocol

1 引言

随着社会信息化发展的进一步深入,信息安全问题越来越受到人们的关注.物理不可克隆函数(Physical Unclonable Function,PUF)作为一种新型的加密组件日渐受到研究者的关注.PUF的原理是通过提取集成电路在制造过程中由于工艺限制而引入的随机差异来生成加密信息(通常称为响应)[1].当设备上电的时候PUF的响应信号就自动生成,当设备断电时响应信号自动湮灭.PUF具有原理结构简单、功耗低、物理不可克隆和不可预测等特点.利用PUF可以有效提高RFID(Radio Frequency Identification)抵御恶意攻击的能力,例如,传统的存储密钥存储手段是将密钥信息存储在非易失性存储器中,这样的存储方式容易被篡改或破坏.而PUF的加密信息是存储在电路结构中,且PUF只有在上电后才生成加密信息,掉电后自动湮灭.因此,PUF难以通过传统的克隆和物理篡改等手段进行攻击.如果将PUF的响应信号作为密钥,则无须使用存储器存储,从而改善了密钥存储的安全性.PUF在设备授权与认证、IP核保护、密钥生成等信息安全领域具有广阔的应用前景[2].

PUF的概念可以追溯到Pappu等人提出的物理单向函数(Physical One-Way Function)[3],他们利用随机

收稿日期:2014-12-30;修回日期:2015-04-30;责任编辑:孙瑶
基金项目:国家自然科学基金(No.61401197);江苏省自然科学基金(No.BK20151477);南京航空航天大学人才引进启动基金

掺杂光散射粒子的透明晶体作为单向函数实现了光 PUF,也是第一种 PUF 结构. 在此之后 Gassend 等人提出了基于硅的 PUF[4],通过提取电路内部晶体管或连线间因工艺原因引入的随机差异而产生的偏差(例如:不同门电路或连接线间在信号传输延时、电压或电流等电气特性上的偏差)来生成二进制加密信息. 即使完全相同的电路结构,在不同集成电路实体上生成的响应值也是不同的. 硅 PUF 的优势是它可以直接与标准数字电路相连接,易于集成. 目前已经提出的基于硅的 PUF 中比较经典的结构有仲裁器 PUF、环形振荡器(Ring Oscillator,RO)PUF、SRAM PUF、蝶形 PUF 等[2,5]. 但是传统的 PUF 由于需要较多的硬件资源,因此在低成本的约束下很难实现一个具有足够安全性的加密应用,如 RFID 系统等[6]. 为了解决这个问题,本文提出了上电密钥产生器同流加密算法相结合的方式,实现了一种新型的低成本 PUF 结构,并且非常适合 RFID 系统的应用. 该 PUF 在改善 RFID 安全性的同时,也兼顾了 RFID 设备对资源消耗方面的严苛限制.

2　新型低成本 PUF 结构

2.1　上电密钥生成器

本文提出了一种基于与非门交叉耦合构成的比特生成器,它是由一对与非门构成的双稳态环,如图 1 所示. 当 CTL 信号设置为“0”时,两个与非门的输出都为“1”,当 CTL 信号设置为“1”时,由于两个与非门是配置成交叉耦合的形式,输出信号可能是“0”也可能是“1”. 由于加工工艺的限制,两个与非门在晶体管的阈值电压上有细微的差别,导致两个与非门的输出最后稳定在某一个状态,而且这个差别是随机出现的,因而最终输出值 0 或者 1 也是随机的. 相比于其它的上电 ID 结构,本文提出的比特生成器具有结构简单,硬件资源消耗少,易于 FPGA 实现等优势. 多位比特产生器组成了本研究中的上电密钥生成器.

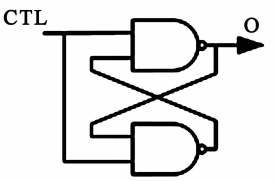

图1　比特生成器

2.2　本文提出的 PUF 结构

实现一个有实用价值的 PUF 需要产生大规模的随机序列,假如完全用上电密钥生成器来生成这些随机序列,理论上需要大规模的比特生成器阵列[1],实际实施的硬件成本将会非常高. 根据 PUF 的特点,可以将上电密钥生成器同传统的轻量级流加密算法相结合,构成一种新型的低成本 PUF 结构. 这样既能保持 PUF 结构的物理不可克隆和防篡改等特性,又能使该结构具有较高的安全性和实际的应用价值. 新的 PUF 结构如图 2 所示,这种 PUF 的基本结构主要包括上电密钥生成器和混合函数两个主要模块.

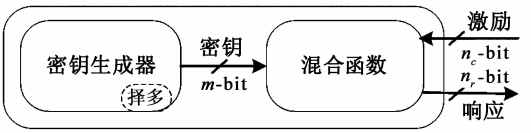

图2　本文提出的PUF结构

密钥生成器主要由 PUF 比特生成器阵列构成,生成的密钥也可以作为一个集成电路实体基于各自内部结构差异而生成的 ID 号,这样的 ID 号同传统存储在 SRAM 中的 ID 相比具有更高的安全性,降低了物理克隆或恶意篡改的可能性[1]. 然而直接使用密钥进行 RFID 设备的认证时,因为密钥的长度(比特数)相对较小,容易被入侵者攻击. 因而引入混合函数来对密钥生成器进行保护.

如图 2 所示,PUF 将密钥生成器生成的信号作为混合函数的输入密钥. 若混合函数需要的输入密钥为 m bit,则密钥生成器由 m 个比特生成器组成. 1-bit 的比特生成器采用图 1 中的结构. 混合函数在密钥的作用下,对输入的 n_c bit 的激励信号进行加密运算,生成随机的 n_r bit 输出响应信号. 本文提出的 PUF 结构,其输出的加密信号(响应信号)是通过混合函数生成的,这与其他文献中的 PUF 直接通过 PUF 本身来生成响应信号不同,因此它是一种新的 PUF 结构,可以有效解决传统 PUF 结构资源消耗大的问题.

本文采用的混合函数为欧洲 eSTREAM 工程中提出的适用于硬件的低成本流密码算法:Grain[7]. Grain 算法是由 Hell 等人提出的一种轻量级加密算法,由非线性反馈移位寄存器、线性反馈移位寄存器和输出函数构成. 该算法的工作流程可分为初始化和密钥流生产两个步骤,且每个时钟周期产生 1 比特随机数.

2.3　择多模块

由于环境、工艺和材料等原因的限制,PUF 比特生成器并不能保证百分之百的稳定输出. 如何让 PUF 产生稳定的输出,目前是 PUF 研究的一个热门方向,比较常见的解决方案就是通过编码的方式,对 PUF 输出进行检错纠错,例如在文献[8]中,Meng-Day Yu 等人探讨了利用 IBS-ECC 编码的方式来提高 PUF 的输出稳定性. 在文献[9]中,Merli 使用了 BCH 编码来降低 PUF 输出的出错概率.

如果采用上述纠错方式,所需要的硬件资源较多,不适合于资源受限的 RFID 系统. 为了减少硬件资源的消

耗,本文提出了一种新型的纠错方法,采用少数服从多数的原则. 如某一个 PUF 比特生成器重复生成输出信号,在一定次数内,统计生成“0”的次数,如果多于生成“1”的次数,则确定该比特生成器的最终输出有效值为“0”. 这种纠错方法通过图 2 中的择多决策模块来实现.

择多模块的实现流程如图 3 所示,*cnt* 为采样计数器,即规定了每次决策时对比特生成器采样的次数;*cand* 为采样得到的比特生成器输出信号;*maj* 表示根据统计结果确定的多数信号为“0”或“1”;*mark* 多数标记,用于统计多数信号出现的次数. 其工作流程为:开始时,将 *cnt*、*mark* 初始化为‘0’;在第一次采样时,将获得的 *cand* 作为 *maj*,同时 *mark* 加一;接下来的过程中,如果生成的信号同 *maj* 相同,*mark* 加一,反之 *mark* 减一;假如 *mark* 减到 0 时,若 *cand* 与 *maj* 不同,则 *maj* 更新为此时获得的 *cand*;当采样结束时,即 *cnt* 溢出时,*maj* 就是择多模块决定的有效输出信号.

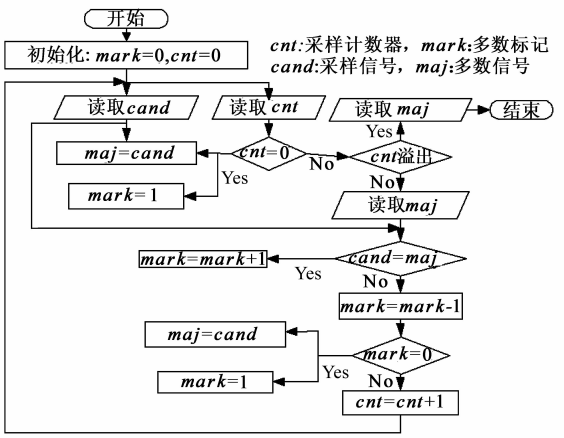

图3 择多模块流程图

3 RFID 应用及多寻认证协议

随着物联网的迅速发展,RFID 系统在人们生活工作中的应用越来越广泛,它对自身的资源和体积有非常严格的限制,在保证 RFID 应用的稳定性和有效性的同时需要尽可能地降低 RFID 设备的资源消耗. 但现有的 RFID 设备存在安全性不高,容易受到入侵者攻击的问题[10,11]. 本文提出的 PUF 为解决 RFID 系统的安全性问题,提供了一种合理可行的解决方案.

根据 RFID 系统的特点,本文提出了一种新型的基于低成本 PUF 的认证协议,即多寻认证协议,如图 4 所示. 该协议定义了 PUF 设备(待认证的 RFID 设备)、RFID 阅读器以及后台数据存储设备(数据库)三个设备间的信息交换方式.

在基于 PUF 应用的认证协议中,主要使用激励/响应对(Challenge/Response Pairs,CRPs)来进行设备的认证,这种认证方式需要密钥生成器能产生稳定的输出. 每一台待认证设备根据输入的激励信号都会生成一个与之唯一对应的响应信号. 如果待认证设备生成的 CRP 与后台数据中存储的 CRP 一致,则认证通过,反之认证失败. 密钥生成器中如果存在某一位位比特生成器的输出不稳定都将导致认证失败. 虽然通过一系列的纠错模块如本文提出的择多模块等后期处理方式能大幅的改善密钥生成的稳定性,但还是不能保证密钥生成是完全稳定的. 为了进一步降低系统认证过程中出现错误接受和错误拒绝的概率,本文提出了多寻认证协议,如图 4 所示. 图 4 中带有 PUF 组件的 RFID 设备能通过阅读器同整个认证系统进行信息交换. 数据库中存储有每个 PUF 实体的大量 CRP,这需要在 PUF 出厂前进行初始化.

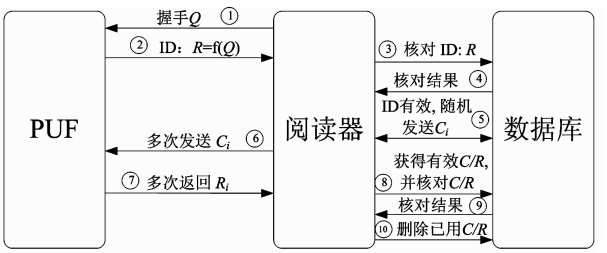

图4 多寻认证协议

多寻认证协议的操作流程为:①首先由阅读器发出一个握手信号;②待认证设备接收到信号后反馈自身的身份标识号;③阅读器收到身份标识号后将其发送给数据库;④数据通过身份标识号核对该设备是否存在数据库中,并且将查询结果返回给阅读器;⑤假如该设备存在与数据库中,则由数据库发送一个激励信号给阅读器;⑥阅读器将收到的这个激励信号,按一定次数重复发给待认证设备;⑦待认证设备每接收一次激励信号,就计算激励信号加密一次,并将加密后的信号反馈给阅读器;⑧阅读器根据接收到的信号中选取一种出现次数最高的信号作为响应信号,并将此激励响应对一同发送给数据库;⑨通过检查该对此激励响应对是否存在于数据库中来决定此时认证是否通过,并将结果反馈给 RFID 阅读器;⑩若认证通过后,RFID 阅读器通知数据库将此次使用的激励响应对删除.

该协议的主要特点是整个认证过程不是依赖于一次 CRP 的校验来完成一次认证,而是在每一次认证的过程中多次地对待认证设备返回的响应值进行校验,最后根据比对的结果来决定是否通过认证,例如:在校验通过的次数远大于校验失败的情况下,表示认证通过,反之认证失败. 当认证结束后,使用过的 CRP 将在数据库中删除,防止重复使用,以保证系统的安全性.

4 实验结果分析

在本研究中,密钥生成器由图 1 中的比特生成器构

成,混合函数模块由低成本的流加密 Grain 算法构成. Grain 算法需要的密钥长度为 80 bits,因而密钥生成器中比特生成器的数量为 80 个. 此外 Grain 的输入激励信号为 64 bits,输出响应长度也是 64 bits,即每生成 64 bits 后输出一次响应. 密钥生成器、混合函数、择多模块和通讯(RS-232)等四个模块在 130nm 的 Xilinx Virtex II-Pro FPGA 上进行了实现验证,多寻认证协议在上位机通过应用程序模拟实现.

4.1　资源消耗

为了合理地评估不同 PUF 结构的资源消耗,本文提出的低成本 PUF 结构与其他 PUF 结构在实现时需要的硬件资源进行了对比,结果如表 1 所示. 其中 PUF 核为上电密钥生成器部分的资源消耗;"其它"为除了 PUF 核以外其它模块的资源消耗,包括纠错电路、通讯电路、控制和混合函数等模块;总体为整个电路消耗总的资源. 由于之前的文献大都只提供 PUF 核这部分的数据,因此表中列出的主要是 PUF 核的资源消耗数据. 然而,要实现一个真正的能用的 PUF 结构,其他辅助的电路("其他")也是必不可少的,因此在表 1 中做了相应的说明.

表 1　PUF 加密组件资源消耗对比

PUF 结构	资源消耗(门资源)		
	PUF 核	其它	总体
文献[9]	9,197*	38,628*	47,825*
文献[12]	N/A	N/A	147,336*
文献[13]	2691	9,092*	11,783*
文献[14]	1853*	N/A	N/A
本文结构	836	2207	3043

注:* 为根据文章中作者提供的数据和技术推断得到,原始文献没有提供数据并且无法通过推断得到的数据用 N/A 表示

表 1 的结果显示,本文提出的 PUF 结构总资源消耗最少,因此非常适合在资源受限的 RFID 系统中使用.

对于本文提出的纠错方法—择多模块的资源消耗同传统的纠错编码进行了对比,如表 2 所示. 本文提出的择多模块的寄存器使用数量最少,和现有最低成本的纠错模块[15]相比,需要的寄存器数减少了 69%,进一步证明了本文提出的 PUF 结构具有低成本的特性.

表 2　纠错模块的资源消耗对比

纠错方法	寄存器数
文献[15]	69
文献[16]	471
文献[17]	6400
择多模块	21

4.2　稳定性测试

为了测试 PUF 比特生成器的稳定性,在 Xilinx 公司的 Virtex II-Pro FPGA 开发板上实现了 1023 个比特生成器,且对每个比特生成器生成的信号重复采样 100 次. 在表 3 中统计了各个比特生成器在 100 次采样中生成"0"的次数. 表 2 中 i 表示每个比特生成器生成"0"的次数,$i \leqslant 100$;n 表示比特生成器的个数,$n \leqslant 1023$.

表 3　比特生成器生成"0"的次数统计

i	0	1	2	3	4	5	14	20	24	
n	481	2	2	1	1	5	1	1	1	
i	36	87	91	94	95	96	97	98	99	100
n	1	2	1	1	1	1	1	1	3	518

从表 3 中统计的结果可知,在总共 1023 个比特生成器中,有 481 个比特生成器的输出信号稳定在"1",有 518 个比特生成器的输出信号稳定在"0",因而,97.6% 的比特生成器能产生稳定的输出信号. 剩下的比特生成器虽然不能保持稳定的输出,但是输出的值都有各自的偏向性(倾向于生成"0"或"1"),可以通过统计手段来确定比特生成器的输出值,同时也进一步说明了采用择多模块进行纠错的合理性.

根据在三块不同的 FPGA(FPGA 型号完全相同)开发板上测试时发现,在没有添加择多模块时,最差的情况下密钥生成器生成的信号中有 28% 是不稳定的. 然而,通过添加择多模块后,对比特生成器产生的信号进行后期处理后,不稳定的输出下降到 2% 以内,择多模块对密钥生成器的稳定性具有非常大的提升. 根据择多模块仿真的结果显示,添加择多模块比不添加择多模块多约 $5 + cnt$ 个时钟开销,cnt 为 2.3 节中定义的采用计数器. 当 cnt 值较小时,对密钥生产的实时性影响较小,例如本实验中采用 cnt 值为 7.

在不同温度下的稳定性测试也是 PUF 性能评估的一个重要方面,在本研究中测试了 FPGA 实现的 PUF 结构在 25℃ ~85℃之间的稳定性. 如图 5 所示,该 PUF 结构总体上产生不稳定输出的比例低于 2%,具有较高的可靠性. 实验表明,使用本文中提出的多寻认证协议,几乎可以消除所有的不稳定输出.

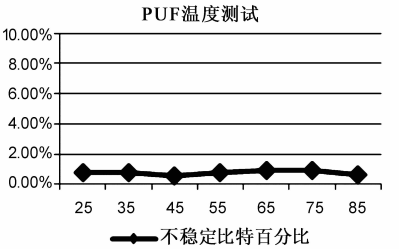

图5　本文PUF结构的温度测试

5　结束语

本文提出了一种新型的低成本 PUF 结构,可适于 RFID 系统. 在该 PUF 中使用了一种基于与非门对交叉

耦合的结构作为上电比特生成器,它能提取两个与非门之间的加工偏差来生成一个随机的响应输出. 通过使用多个相同的比特生成器构成密钥生成器,用于密钥的生成. 为了进一步保护密钥,通过混合函数来对密钥进行隐藏. 此外本文提出了择多模块及多寻认证协议两种方式来提高系统的稳定性. 该 PUF 结构的资源消耗和稳定性两个方面的实验结果表明该 PUF 具有低成本和高稳定性的优点,非常适合应用于 RFID 系统等资源受限的应用.

参考文献

[1] Rührmair U, Holcomb D. PUFs at a glance[A]. Proceedings of Design, Automation and Test in Europe[C]. Dresden, Germany: IEEE, 2014. 1 – 6.

[2] Maes R. Physically Unclonable Functions: Constructions, Properties and Applications [M]. Berlin Heidelberg: Springer, 2013.

[3] Pappu R, Recht B, Taylor J, et al. Physical one-way functions[J]. Science, 2002, 297(5589): 2026 – 2030.

[4] Gassend B. Physical Random Functions[D]. USA: Massachusetts Institute of Technology, 2003.

[5] Herder C, Yu M, Koushanfar F, et al. Physical unclonable functions and applications: A tutorial[J]. Proceedings of the IEEE, 2014, 102(8): 1126 – 1141.

[6] 王晨旭,韩良,等. 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, et al. A secure cipher implementation suitable for RFID-tags[J]. Acta Electronica Sinica, 2014, 42(8): 1465 – 1473. (in Chinese)

[7] Hell M, Johansson T, Maximov A, et al. A stream cipher proposal: Grain-128[A]. Proceedings of IEEE International Symposium on Information Theory [C]. Seattle, WA, USA: IEEE, 2006. 1614 – 1618.

[8] Yu M, Devadas S. Secure and robust error correction for physical unclonable functions[J]. IEEE Design & Test of Computers, 2010, 27(1): 48 – 65.

[9] Merli D, Stumpf F, Eckert C. Improving the quality of ring oscillator PUFs on FPGAs[A]. Proceedings of the 5th ACM Workshop on Embedded Systems Security [C]. Scottsdale, AZ, USA: ACM, 2010. 1873548-1873557.

[10] 郭奕旻,李顺东,等. 一种轻量级隐私保护的 RFID 群组证明协议[J]. 电子学报, 2015, 43(2): 289 – 292.
Guo Yi-min, Li Shun-dong, et al. A lightweight privacy-preserving grouping proof protocol for RFID systems[J]. Acta Electronica Sinica, 2015, 43(2): 289 – 292. (in Chinese)

[11] 李辉,侯义斌,黄樟钦,刘宏珍,何坚,陈锐. 一种智能攻击模型在 RFID 防伪协议中的研究[J]. 电子学报, 2009, 37(11): 2565 – 2573.
Li Hui, Hou Yi-bin, Huang Zhang-qin, Liu Hong-zhen, He Jian, Chen Rui. Research on the attack model for RFID anti-counterfeit protocol[J]. Acta Electronica Sinica, 2009, 37(11): 2565 – 2573. (in Chinese)

[12] Lee J, Lim D, Gassed B, et al. A technique to build a secret key in integrated circuits for identification and authentication application[A]. Proceedings of the Symposium on VLSI Circuits[C]. Honolulu, HI, USA: IEEE, 2004. 176 – 159.

[13] Suh G, O'Donnell C, Sachdev I, et al. Design and implementation of the AEGIS single-chip secure processor using physical random functions[A]. Proceedings of the 32nd International Symposium on Computer Architecture[C]. Madison, WI, USA: IEEE, 2005. 25 – 36.

[14] Su Y, Holleman J, Otis B. A digital 1.6pJ/bit chip identification circuit using process variations[J]. IEEE Journal of Solid-State Circuits, 2008, 43(1): 69 – 77.

[15] Yu M, M'Raihi D, Sowell R, et al. Lightweight and secure PUF key storage using limits of machine learning [A]. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems (CHES)[C]. Nara, Japan: ACM, 2011. 358 – 373.

[16] Suh G, O'Donnell C, Devadas S. AEGIS: A single-chip secure processor[J]. Information Security Technical Report, 2005, 10(2): 63 – 73.

[17] Devadas S, Yu M. Secure and robust error correction for physical unclonable functions[J]. IEEE Design & Test of Computers, 2010, 27(1): 48 – 65.

作者简介

刘伟强 男,1983 年 3 月出生,山东东营人. 副教授、硕士生导师、IEEE 高级会员、中国电子学会高级会员. 2006 年和 2012 年分别在南京航空航天大学和英国贝尔法斯特女王大学获得工学学士和博士学位. 现担任 IEEE 计算机会刊副主编,主要从事数字信号处理及加密算法的 VLSI 实现、高性能算术运算单元以及新兴计算硬件等方面的研究工作.
E-mail: liuweiqiang@nuaa.edu.cn

崔益军 男,1988 年 8 月出生,江苏海安人. 2010 年毕业于南京航空航天大学信息工程专业获工学学士学位,同年保送进入南京航空航天大学攻读通信与信息系统方向研究生,现为硕博连读生,从事硬件加密系统和 RFID 系统等方面的研究.