计算机应用 2012, 32(03) 683-685 DOI: 10.3724/SP.J.1087.2012.00683 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

基于PUF的高效低成本RFID认证协议

贺章擎[1,2],郑朝霞[1],戴葵[1],邹雪城[1]

1.华中科技大学 电子科学与技术系,武汉430074;
2.湖北工业大学 电气与电子工程学院,武汉 430068

摘要: 已提出的针对低成本RFID系统的安全机制,要么存在安全缺陷,要么硬件成本太高。为此设计了一个基于物理不可克隆功能(PUF)的RFID安全认证协议,利用PUF和线性反馈移位寄存器(LFSR)实现了阅读器和标签之间强的安全认证,解决了已有安全协议存在的问题。安全性分析表明:该协议成本低、安全性高,能够抵抗物理攻击和标签克隆,并有极强的隐私性。

关键词: 射频识别 安全认证协议 物理不可克隆功能 线性反馈移位寄存器 加密

Low-cost RFID authentication protocol based on PUF

HE Zhang-qing[1,2], ZHENG Zhao-xia[1], DAI Kui[1], ZOU Xue-cheng[1]

1.Department of Electronic Science and Technology, Huazhong University of Science and Technology, Wuhan Hubei 430074,China;
2.School of Electrical and Electronic Engineering, Hubei University of Technology, Wuhan Hubei 430068, China

Abstract: The available security mechanisms for the low-cost Radio Frequency IDentification (RFID) systems are either defective or high-cost. Therefore, this paper proposed an efficient security authentication protocol for low-cost RFID system based on Physical Unclonable Function (PUF) and Linear Feedback Shift Register (LFSR). The protocol provides strong security and can resist physical attack and tag clone with strong privacy.

Keywords: Radio Frequency IDentification (RFID) security authentication protocol Physical Unclonable Function (PUF) Linear Feedback Shift Register (LFSR) encryption

收稿日期 2011-08-30 **修回日期** 2011-11-20 **网络版发布日期** 2012-03-01

DOI: 10.3724/SP.J.1087.2012.00683

基金项目:

武汉市重点科技攻关计划项目(201150699190)。

通讯作者: 贺章擎

作者简介: 贺章擎(1980-),男,湖北天门人,讲师,博士研究生,主要研究方向:信息安全、嵌入式系统;郑朝霞(1975-),女,重庆人,讲师,博士,主要研究方向:大规模数字集成电路设计;戴葵(1968-),男,湖北恩施人,教授,博士,主要研究方向:高性能处理器系统、计算机系统结构、信息安全;邹雪城(1965-),男,湖北监利人,教授,博士,主要研究方向:大规模集成电路设计。

作者Email: ivan_hee@126.com

参考文献:

[1]JUELS A, WEIS S A. Authenticating pervasive devices with human protocols[C]// CRYPTO 2005: Proceedings of 25th Annual International Cryptology Conference, LNCS 3621. Berlin: Springer-Verlag, 2005:293-308.[2]SARMA S, WEIS S, ENGELS D. Radio frequency identification: Secure risks and challenges[J]. RSA Laboratories Cryptobytes, 2003,6(1):2-9.

[3]WEIS S A, SARMA S E, RIVEST R L, et al. Security and privacy aspects of low-cost radio frequency

identification systems [C]// Proceedings of the 1st International Conference on Security in Pervasive Computing, LNCS 2802. Berlin: Springer-Verlag,2004:201-212.

[4]OHKUBO M, SUZUKI K, KINOSHITA S. Hash-chain based forward-secure privacy protection scheme for low-cost RFID[C]// SCIS 2004: Proceedings of the 2004 Symposium on Cryptography and Information Security.Berlin: Springer-Verlag,2004:719-724.

[5]MOLNAR D, WAGNER D. Privacy and security in library RFID: Issues, practices, and architectures [C]// CCS'04: Proceedings of the 1th ACM Conference on Computer and Communications Security. New York: ACM Press,2004:210-219.

[6]RHEE K, KWAK J, KIM S, et al. Challenge-response based RFID authentication protocol for distributed database environment[C]// SPC 2005: Proceedings of the 2nd International Conference on Security in Pervasive Computing, LNCS 3450. Berlin: Springer-Verlag,2005: 70-84.

[7]丁振华,李锦涛,冯波.基于Hash函数的RFID安全认证协议研究[J].计算机研究与发展,2009,46(4):583-592.

[8]CHIEN H Y. SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity[J]. IEEE Transactions on Dependable and Secure Computing, 2007,4 (4):337-340.

[9]YUKSEL K. Universal hashing for ultra-low-power cryptographic hardware applications[D]. Worcester: Worcester Polytechnic Institute, Electrical & Computer Engineering Department, 2004.

[10]FELDHOFER M, DOMINIKUS S, WOLKERSTORFER J. Strong authentication for RFID systems using the AES algorithm[C]// Proceedings of CHES. New York: ACM Press, 2004:85-140.

[11]SUH G E, DEVADAS D. Physical unclonable functions for device authentication and secret key generation[C]// DAC'07: Proceedings of the 44th Annual Design Automation Conference. New York: ACM Press, 2007:9-14.

[12]GASSEND B, CLARKE D, van DIJK M, et al. Silicon physical random functions[C]// Proceedings of the 9th ACM Computer and Communication Security. New York: ACM Press, 2002: 148-160.

[13]杨灵,闰大顺. 基于PUF的低成本RFID系统安全协议[J].计算机工程,2010,36(15):148-155.

[14]LEONID B, GABRIEL R. Physically unclonable function-based security and privacy in RFID Systems [C]// PerCom'07: Proceedings of the 5th Annual IEEE International Conference on Pervasive Computing and Communications. Piscataway, NJ: IEEE Press,2007: 211-220.

[15]RUHRMAIR U, MUNCHEN T, DROR G, et al. Modeling attacks on physical unclonable functions[C]// Proceedings of the 17th ACM Conference on Computer and Communications Security. New York: ACM Press, 2010:237-249.

本刊中的类似文章

1．柳欣.具有分布式打开权威的隐藏身份签名方案[J]. 计算机应用, 2012,32(03): 699-704

2．丁治国 朱学永 雷迎科 王心灵.基于启发式函数的多叉树防碰撞算法[J]. 计算机应用, 2012,32(03): 665-668

3．夏秀峰 赵龙.基于三层存储模型的RFID数据压缩存储方法[J]. 计算机应用, 2012,32(03): 625-628

4．魏江宏 刘文芬 胡学先.全安全的属性基认证密钥交换协议[J]. 计算机应用, 2012,32(01): 38-41

5．李志强 严迎建 段二朋.差分能量攻击样本选取方法[J]. 计算机应用, 2012,32(01): 92-94

6．胡韬 魏国珩.基于低成本标签的RFID匿名双向认证协议[J]. 计算机应用, 2012,32(01): 111-114

7．杜成阳 文光俊 雷滨滨.基于射频识别技术的出租车防伪管理系统的设计与实现[J]. 计算机应用, 2012,32 (01): 284-287

8．冯娜 潘伟杰 李少波 杨观赐.基于新颖跳跃式动态搜索的RFID防碰撞算法[J]. 计算机应用, 2012,32(01): 288-291

9．陈勤 马丹丹 张金漫 党正芹.隐藏访问策略的属性基加密机制[J]. 计算机应用, 2011,31(11): 2969-2972

10．郑洪英 李文杰 肖迪.基于时空混沌系统的图像分组加密算法[J]. 计算机应用, 2011,31(11): 3053-3055

11．张亮亮 陈秀宏.基于人类视觉系统和离散小波变换的彩色图像水印[J]. 计算机应用, 2011,31(11): 3056-3059

12．王明辉 王建东.高效的RFID双向认证协议[J]. 计算机应用, 2011,31(10): 2694-2696

13. 刘立群.集中式无线局域网分离介质访问控制的CCMP设计[J]. 计算机应用, 2011,31(08): 2159-2161
14. 廖琪男.切延迟椭圆反射腔映射系统混沌序列的改进与彩色图像加密算法[J]. 计算机应用, 2011,31(08): 2178-2182
15. 孙文胜 胡玲敏.基于后退式搜索的自适应多叉树防碰撞算法[J]. 计算机应用, 2011,31(08): 2052-2055
16. 贺洪江 丁晓叶 翟耀绪.标签运动状态下的RFID系统反碰撞算法[J]. 计算机应用, 2011,31(08): 2048-2051
17. 刘君昌 张曦煌.KNXnet/IP协议安全性分析与改进[J]. 计算机应用, 2011,31(07): 1912-1916
18. 乐鸿辉 李涛 石磊.应用Henon超混沌系统改进的图像加密[J]. 计算机应用, 2011,31(07): 1909-1911
19. 邓绍江 黄桂超 陈志建 肖潇.基于混沌映射的自适应图像加密算法[J]. 计算机应用, 2011,31(06): 1502-1504
20. 易磊 仲红 袁先平 赵玉.支持容错检索的数据共享方案[J]. 计算机应用, 2011,31(06): 1525-1527
21. 任晓霞 廖晓峰 熊永红.基于细胞神经网络超混沌特性的图像加密新算法[J]. 计算机应用, 2011,31(06): 1528-1530
22. 张月华 张新贺 刘鸿雁.AES算法优化及其在ARM上的实现[J]. 计算机应用, 2011,31(06): 1539-1542
23. 白茹雪 刘鸿雁 张新贺.基于ARM920T的AES算法实现方案[J]. 计算机应用, 2011,31(05): 1295-1297
24. 卢丹华 钟诚 杨锋.基于多核多线程的AES保密模式[J]. 计算机应用, 2011,31(04): 1003-1005
25. 廖志委 王晓明.基于秘密共享的广播加密方案[J]. 计算机应用, 2011,31(04): 978-980
26. 顾国生 刘富春.基于混沌映射的图像Contourlet编码加密算法[J]. 计算机应用, 2011,31(03): 771-773
27. 邓强东 王立斌.Molnar协议的安全性证明[J]. 计算机应用, 2011,31(03): 798-800
28. 谢川.结合Hash函数和密钥阵列的RFID安全认证协议[J]. 计算机应用, 2011,31(03): 805-807
29. 吴升 郭新宇 肖伯祥 陆声链 温维亮.基于非均匀B-样条曲线的加密算法[J]. 计算机应用, 2011,31(02): 517-519
30. 余永红 柏文阳.基于加密技术的外包数据库服务集成安全[J]. 计算机应用, 2011,31(01): 110-114
31. 郝文宁 赵恩来 刘玉栋 黄亚 刘军涛.异构数据库加解密系统的关键技术研究与实现[J]. 计算机应用, 2010,30(9): 2339-2343
32. 柯于义 夏士雄 汪楚娇.XML加密数据查询方法的研究与设计[J]. 计算机应用, 2010,30(4): 1099-1102
33. 贾伟尧 盛利元 陈亚丽.TD-ERCS混沌系统的几个短周期轨道及其稳定性[J]. 计算机应用, 2010,30(3): 680-684
34. 罗松江 朱路平.基于分段非线性混沌映射的流密码加密方案[J]. 计算机应用, 2010,30(11): 3038-3039
35. 皮明峰 邓飞其.面向制造业的RFID复杂事件处理[J]. 计算机应用, 2010,30(10): 2768-2770
36. 陈天娥 程载和.基于冲突树的RFID自适应防碰撞算法[J]. 计算机应用, 2010,30(07): 1728-1730
37. 肖迪 赵秋乐.一种基于Logistic混沌序列的图像置乱算法的安全分析[J]. 计算机应用, 2010,30(07): 1815-1817
38. 王灿 秦志光 冯朝胜 彭静.面向重复数据消除的备份数据加密方法[J]. 计算机应用, 2010,30(07): 1763-1766
39. 卢辉斌 刘海莺.基于耦合混沌系统的彩色图像加密算法[J]. 计算机应用, 2010,30(07): 1812-1814
40. 唐晓东 付松龄 何连跃.基于eCryptfs的多用户加密文件系统设计和实现[J]. 计算机应用, 2010,30(05): 1236-1238
41. 张涛.基于混沌的序列密码算法[J]. 计算机应用, 2010,30(05): 1221-1223
42. 陈泉泉 王如龙 彭昂 张锦 段智敏.面向移动设备的可配置RFID中间件设计与实现[J]. 计算机应用, 2010,30(05): 1321-1323
43. 陈礼青.基于公钥广播加密的安全组播方案[J]. 计算机应用, 2009,29(11): 2948-2951
44. 张健 于晓洋 任洪娥.基于Arnold cat变换的图像位置均匀置乱算法[J]. 计算机应用, 2009,29(11): 2960-2963
45. 周志刚 李苏贵.基于变参数混沌系统的数字图像隐藏技术[J]. 计算机应用, 2009,29(11): 2972-2976
46. 倪凯斌 姚国祥 官全龙.安全增强型虚拟磁盘加密系统技术[J]. 计算机应用, 2009,29(11): 2987-2989
47. 秦雪丽 程明 李伟.基于钟控非线性序列的RFID伪随机数发生器设计[J]. 计算机应用, 2009,29(11): 2998-3000
48. 阴晓加 鞠时光 王英杰.基于复杂事件处理机制的RFID数据流处理方法[J]. 计算机应用, 2009,29(10): 2786-2790
49. 胡宏银 姚峰 何成万.一种基于文件过滤驱动的Windows文件安全保护方案[J]. 计算机应用, 2009,29(1): 168-171
50. 丁国良 李志祥 尹文龙 赵强.高级数据加密标准的差分电磁分析[J]. 计算机应用, 2009,29(08): 2200-2203
51. 赖师悦 廖晓峰 周庆.新的基于波传播的图像加密算法[J]. 计算机应用, 2009,29(08): 2210-2212

52. 马春阳 张亚玲.VRML文档的消隐数字签名安全模型[J]. 计算机应用, 2009,29(07): 1793-1795

53. 屈步云 刘连浩.利用双线性映射构建高效身份认证方案[J]. 计算机应用, 2009,29(07): 1779-1781

54. 周志刚 李苏贵 刘嫒.基于新的变参数混沌系统的图像加密[J]. 计算机应用, 2009,29(07): 1832-1835

55. 赵亮 廖晓峰 向涛 肖迪.对高维混沌系统的图像加密算法安全性和效率的改进[J]. 计算机应用, 2009,29(07): 1775-1778

56. 景征骏 王波 张天平 李秉璋.基于嵌入式技术的城市非机动车辆查询终端设计[J]. 计算机应用, 2009,29(07): 1985-1987

57. 胡宇 王世伦.基于混合体制的Kerberos身份认证协议的研究[J]. 计算机应用, 2009,29(06): 1659-1661

58. 廖翠玲 余昭平.[a,b]-缩减生成器[J]. 计算机应用, 2009,29(05): 1334-1338

59. 吕宁 孙广明 张宇.基于多混沌系统的图像分组密码设计[J]. 计算机应用, 2008,28(9): 2263-2266

60. 王立斌 马昌社 王涛.一种安全高效的RFID双边认证协议[J]. 计算机应用, 2008,28(9): 2236-2238

61. 王新锋 刘建国 蒋旭 刘胜利.移动型RFID安全协议及其GNY逻辑分析[J]. 计算机应用, 2008,28(9): 2239-2241

62. 陈宇环 易称福.基于时空混沌序列的视频加密设计与实现[J]. 计算机应用, 2008,28(8): 1936-1939

63. 张颇 崔喆.RFID系统中一种改进的防冲撞算法[J]. 计算机应用, 2008,28(8): 2141-2143

64. 冯全 肖媛媛 苏菲 蔡安妮.基于指纹的可撤销Fuzzy vault方案[J]. 计算机应用, 2008,28(7): 1816-1818

65. 邓辉舫 马启平 周尚伟.使用无线射频识别(RFID)技术进行室内定位[J]. 计算机应用, 2008,28(7): 1858-1860

66. 黄胜 蒋外文.网格中基于分层的身份加密系统研究[J]. 计算机应用, 2008,28(5): 1161-1163

67. 杨学俊 王灯国 黄徐徐.一个基于ID的可删除群签名方案[J]. 计算机应用, 2008,28(4): 918-920

68. 成修治 李宇成.RFID中间件的结构设计[J]. 计算机应用, 2008,28(4): 1055-1057

69. 袁益民 盛利元 尚芳.基于TD-ERCS混沌系统的图像加密方法[J]. 计算机应用, 2008,28(4): 906-909

70. 徐圆圆 曾隽芳 刘禹.基于Aloha算法的帧长及分组数改进研究[J]. 计算机应用, 2008,28(3): 588-590

71. 程东升 叶瑞松.基于四维混沌系统生成二值序列的方法及其加密应用[J]. 计算机应用, 2008,28(3): 677-679

72. 陈东方 张有清.基于提升方案小波和水印加密的盲水印算法[J]. 计算机应用, 2008,28(3): 615-619

73. 刘志远 杨秋伟 崔国华 洪帆.一种基于标识的隐私资源保护方案[J]. 计算机应用, 2008,28(2): 418-421

74. 张新方 徐秋亮.不使用对的基于身份的广播加密[J]. 计算机应用, 2008,28(2): 432-433,

75. 高洁 袁家斌 徐涛 齐艳珂.一种基于混合反馈的混沌图像加密算法[J]. 计算机应用, 2008,28(2): 434-436

76. 朱志良 张伟 于海.基于Lorenz混沌系统的MPEG视频加密算法[J]. 计算机应用, 2008,28(12): 3003-3006

77. 罗松江 丘水生 骆开庆.一种新的混沌伪随机序列及其性能分析[J]. 计算机应用, 2008,28(12): 3187-3189

78. 陈作新.一种基于AES和三素数RPrime RSA认证加密方案[J]. 计算机应用, 2008,28(12): 3199-3201

79. 徐圆圆 曾隽芳 陈琳 刘禹.EPC Gen2标准防碰撞方案的研究与改进[J]. 计算机应用, 2008,28(12): 3271-3273

80. 杨斌 熊选东 苏克军.基于仲裁者的身份加密方案研究[J]. 计算机应用, 2008,28(11): 2835-2836

81. 郭建华 杨海东 邓飞其.基于免疫网络的RFID入侵检测模型研究[J]. 计算机应用, 2008,28(10): 2481-2484

82. 蒋邵岗 谭杰.RFID中间件数据处理与过滤方法的研究[J]. 计算机应用, 2008,28(10): 2613-2615

83. 董贵山 卢显良 邓春梅 罗俊.一种Linux网络硬件加密高性能并发调度方法[J]. 计算机应用, 2008,28(1): 65-67,7

84. 朱贵良 马友.基于混沌的混合图元加密算法研究[J]. 计算机应用, 2008,28(1): 59-61

85. 韩凤英 朱从旭 胡玉平.一种基于高维混沌系统的彩色图像加密新算法[J]. 计算机应用, 2007,27(8): 1888-1890

86. 洪联系 李传目 卢明玺.扩散映射置乱与超混沌系统组合图像加密算法[J]. 计算机应用, 2007,27(8): 1891-1894

87. 何希平 朱庆生.基于混沌的图像小波域加密算法[J]. 计算机应用, 2007,27(8): 1895-1897

88. 段国文 王殊.基于RFID的无线传感器网络节能MAC技术[J]. 计算机应用, 2007,27(8): 1855-1857

89. 王保云 杨英杰 黄涛.一种二维防护的安全文件系统体系结构[J]. 计算机应用, 2007,27(7): 1616-1618

90. 李银 金晨辉.适合AES算法硬件实现的新S盒[J]. 计算机应用, 2007,27(4): 852-853

91. 杨小东 张贵仓 陆洪文.基于身份认证的手机支付系统的设计与实现[J]. 计算机应用, 2007,27(3): 584-586

92．张璐 张璟 井浩 李军怀.网络采购系统中安全机制的研究与实现[J]. 计算机应用, 2007,27(2): 318-320
93．李士达 胡玥 王兴秋 于真.一种基于ECC的SIP认证方案的提出与实现[J]. 计算机应用, 2007,27(2): 311-313
94．秋小强 蔡觉平.网络处理器高速AES协处理器设计[J]. 计算机应用, 2007,(12): 2957-2959
95．王亚奇 顾亦然 蒋国平.改进型的二进制搜索RFID系统反碰撞算法[J]. 计算机应用, 2007,27(11): 2877-2879
96．刘家胜 黄贤武 朱灿焰 张燕 吕皖丽 .基于m序列整数调制和置乱的图像加密算法[J]. 计算机应用, 2007,27(1): 118-121
97．杨建强 .基于Java ME的点到点短信加密应用[J]. 计算机应用, 2006,26(8): 1813-1816
98．阎磊 侯春萍 曹达仲 戴居丰 .基于3DES算法的电话加密研究及其FPGA实现[J]. 计算机应用, 2006,26(8): 1824-1826
99．李太勇 贾华丁 吴江 .基于三维混沌序列的数字图像加密算法[J]. 计算机应用, 2006,26(7): 1652-1654
100．孟健; 曹立明; 王小平; 姚亮.XML文档的加密访问控制与传输[J]. 计算机应用, 2006,26(5): 1061-1063
101．何希平;朱庆生.基于混沌映射的Hash函数及其在身份标识认证中的应用[J]. 计算机应用, 2006,26(5): 1058-1060
102．彭长根;李祥;罗文俊.可转换签密的几种改进方案[J]. 计算机应用, 2006,26(5): 1068-1070
103．孙飞显; 徐明洁; 杨进; 王铁方; 刘孙俊.基于Web的教务管理系统安全方案设计[J]. 计算机应用, 2006,26(5): 1198-1201
104．赵雪峰; 殷国富.基于复合混沌系统的数字图像加密方法研究[J]. 计算机应用, 2006,26(4): 827-829
105．韩磊 张虹 马海波 .散列树形搜索反碰撞算法的研究[J]. 计算机应用, 2006,26(12): 3019-3022
106．粟伟 崔喆 王晓京 .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
107．于淼;孙强.对超粒度混杂技术的改进：基于瘦虚拟机的指令集交替技术[J]. 计算机应用, 2005,25(12): 2808-2810
108．董军武; 邹候文; 裴定一.椭圆曲线软件及密码卡的设计与实现[J]. 计算机应用, 2005,25(11): 2549-2553
109．王燕.实现IPv6数据包分类的算法研究[J]. 计算机应用, 2005,25(11): 2502-2504
110．王文奇; 李伟华;史兴键;等.基于Agent的网络安全系统协同控制研究[J]. 计算机应用, 2005,25(10): 2280-2282
111．任德玲，韦卫，吕继强.代理可转换认证加密方案[J]. 计算机应用, 2005,25(09): 2086-2088
112．王菊芬，袁道华，王放，张帆.一种具有认证和加密功能的Ad hoc网络路由协议[J]. 计算机应用, 2005,25(09): 2070-2073
113．张锦，沈亚敏，董婷，朱望斌.传感器网络中一种双重安全路由算法[J]. 计算机应用, 2005,25(08): 1722-1725
114．胡宝芳，王红，张霞.基于移动代理的虚拟专用网安全系统[J]. 计算机应用, 2005,25(08): 1756-1759
115．王彩芬，于成尊，刘军龙，贾爱库.一种新的认证邮件协议[J]. 计算机应用, 2005,25(07): 1545-1547
116．闫晓东，王志秦，关榆君.一种基于有限域运算的半脆弱数字水印算法[J]. 计算机应用, 2005,25(06): 1294-1295
117．邵昱，萧蕴诗.基于文件系统过滤驱动器的加密软件设计[J]. 计算机应用, 2005,25(05): 1151-1152
118．孙瑜，范平志.射频识别技术及其在室内定位中的应用[J]. 计算机应用, 2005,25(05): 1205-1208
119．高铁杠，陈增强，袁著祉，顾巧论.一种基于混沌数字流的信息隐藏技术研究[J]. 计算机应用, 2005,25(04): 839-841
120．仇建平，崔杜武.基于射频识别的供应链管理系统[J]. 计算机应用, 2005,25(03): 734-736
121．彭飞，丘水生，龙敏.一种基于混合混沌动力系统的图像加密算法[J]. 计算机应用, 2005,25(03): 543-545
122．乔少杰，彭舰，郑学强，林红君.移动电子拍卖系统加密和签名特殊技术[J]. 计算机应用, 2005,25(02): 459-462
123．杨广铭，张志浩.基于XSLT的XML元素级加密技术及其应用[J]. 计算机应用, 2005,25(02): 407-408
124．马大伟，郑应平，王令群.一种基于混沌理论的多层次变密钥视频加密方法[J]. 计算机应用, 2005,25(02): 394-395
125．刘航，戴冠中，李晖晖，慕德俊.工作于CBC模式的AES算法可重配置硬件实现[J]. 计算机应用, 2005,25(01): 135-137
126．于为中，马红光，王令欢，赵星阳.基于一维混沌映射的图像加密方法[J]. 计算机应用, 2005,25(01): 141-143
