全国大学生电子设计竞赛
信息安全技术专题邀请赛
优秀作品选编（第三届）

全国大学生电子设计竞赛信息安全技术专题邀请赛组委会　编

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

全国大学生电子设计竞赛
信息安全技术专题邀请赛
优秀作品选编（第三届）

全国大学生电子设计竞赛信息安全技术专题邀请赛组委会　编

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

图书在版编目（CIP）数据

全国大学生电子设计竞赛信息安全技术专题邀请赛优秀作品选编：第三届/全国大学生电子设计竞赛信息安全技术专题邀请赛组委会编. —北京：北京理工大学出版社，2015.5

ISBN 978-7-5640-9986-2

Ⅰ.①全…　Ⅱ.①全…　Ⅲ.①高等学校-信息安全-安全技术-科技成果-中国　Ⅳ.①TP309

中国版本图书馆 CIP 数据核字（2014）第 275348 号

出版发行 /北京理工大学出版社有限责任公司
社　　址 /北京市海淀区中关村南大街 5 号
邮　　编 /100081
电　　话 /（010）68914775（总编室）
　　82562903（教材售后服务热线）
　　68948351（其他图书服务热线）
网　　址 /http：//www. bitpress. com. cn
经　　销 /全国各地新华书店
印　　刷 /三河市华骏印务包装有限公司
开　　本 /880 毫米×1230 毫米　1/16
印　　张 /13. 5
字　　数 /397 千字
版　　次 /2015 年 5 月第 1 版　2015 年 5 月第 1 次印刷
定　　价 /34. 00 元

责任编辑 /张慧峰
文案编辑 /张慧峰
责任校对 /周瑞红
责任印制 /李志强

全国大学生电子设计竞赛信息安全技术专题邀请赛（第三届）专家组名单

组　长： 傅丰林　西安电子科技大学教授

副组长： 罗森林　北京理工大学教授

成　员： （按姓氏拼音字母排序）

陈文智　浙江大学教授

韩　臻　北京交通大学教授

胡爱群　东南大学教授

胡　波　复旦大学教授

李　卫　西安交通大学教授

刘建伟　北京航空航天大学教授

刘　琚　山东大学教授

刘开华　天津大学教授

龙冬阳　中山大学教授

牛少彰　北京邮电大学教授

唐朝京　国防科技大学教授

薛　质　上海交通大学教授

岳继光　同济大学教授

赵　波　武汉大学教授

赵茂泰　武汉大学教授

赵有健　清华大学教授

朱茂镒　北京信息科技大学教授

祝跃飞　解放军信息工程大学教授

序

人类社会正进行的信息化发展是社会进化发展的一个必然的重要阶段。其核心发展机理仍是：矛盾对立运动促进发展，而矛盾就蕴含在社会本身之中，最理想的当然是和谐发展，但很不容易！其中解决日益尖锐的信息安全问题，不断提升安全水平是重要因素，而提升人文素质和利用前沿信息科技，是提升信息安全水平的一项重要因素。为此，前几年全国大学生电子设计竞赛专门设立了信息安全技术邀请赛，搭建了一个供优秀大学生实践的平台，以服务信息安全领域的高等教育发展之急需！

本作品集收集了2012年竞赛中部分优秀作品以资交流，也为今后竞赛发展收集反馈意见和批评建议。大学生信息安全技术邀请赛定将与时俱进，不断发展，下一次竞赛内容将添设模拟攻防环境，以体现信息安全问题中实际存在的对立矛盾，以及解决矛盾的各种方法和技术。希望得到各位老师、教育行政部门以及同学们的支持和参与！

王　越

前　言

随着全球信息化的快速发展，信息安全的重要性以及信息安全保障体系建设的紧迫性日益凸显。信息安全可理解为保障信息的机密性、完整性、可用性、真实性、可控性，它关涉一个国家的政治安全、经济安全和文化安全，对国家安全具有重大战略价值。

目前，信息攻击形式日益复杂化，可分为主动攻击和被动攻击。病毒技术、黑客攻击和信息恐怖主义的结合，直接威胁着我国的信息安全。信息技术的发展日新月异，各种新信息技术的应用如雨后春笋般涌现，引发新的信息安全风险。在当今信息安全领域的各种信息安全技术措施中，硬件的安全和操作系统的安全是基础，密码技术是关键，只有从整体上采取措施，特别是从底层采取措施，才能有效地解决信息安全问题。

信息安全产业作为关系到国计民生的战略性信息产业，市场空间巨大，不断产生新的发展空间。近年来我国信息安全产品市场容量持续以两位数速度增长。2012 年，市场规模达到 157.84 亿元，比 2011 年增长 20.3%，高于全球平均增速。

但是，目前我国信息安全人才严重不足。根据 2012 年权威机构的统计显示，我国信息安全专业人才的存量与实际需求比例已经达到 1∶10 的严峻形势。因此，提升我国信息安全专业人才培养水平、加快建立信息安全保障体系、提高信息安全管理能力，已成为我国各行业信息化建设过程中最为紧迫的任务。

鉴于以上情况，2008 年开始，由教育部高等教育司、工业和信息化部人事教育司主办全国大学生电子设计竞赛信息安全技术专题邀请赛，每隔两年举办一次。2012 年接受邀请的高校有 37 所，报名队数有 117 支队。本次竞赛继续得到了 TI 公司和 XiLinx 公司支持。竞赛分三类题型：TI 平台组、XiLinx 平台组和软件组。参赛学生 3 人 1 队，自选题目，充分发挥自己的聪明才智。报名参赛 TI 平台组的有 30 支队、XiLinx 平台组的有 32 支队、软件组的有 55 支队。评出第三届全国大学生电子设计竞赛信息安全技术邀请赛一等奖 11 个、二等奖 19 个、三等奖 43 个。通过竞赛，同学们得到了很好的锻炼，提高了创新精神、实践能力和综合素质。

本次竞赛涌现出了一些优秀作品，入选本书的作品只是学生参赛获奖作品的一部分，由于种种原因，这些作品不可能尽善尽美，编写本书的目的在于促进交流和学习，提升信息安全专业的教学水平。

本次竞赛得到了 TI 公司和 XiLinx 公司的大力支持，在此表示衷心的感谢！

傅丰林

全国大学生电子设计竞赛信息安全技术专题邀请赛（第三届）获奖名单

序号	组别	学校	参赛题目	指导老师	参赛学生	获奖等级
1	SOFT	北京航空航天大学	基于硬件指纹的密码生成系统	金天	彦晓宇，李胜曦，白璐	一等奖
2	TI	北京航空航天大学	侧信道攻击、防御和测评系统	金天	冯伯昂，黄羚，闫桂勋	一等奖
3	SOFT	北京理工大学	基于硬件虚拟化的网络通信监测系统	高平	贾丛飞，韦伟，王帅	一等奖
4	TI	北京理工大学	基于 OCF－Linux 的实时透明加密解密及云端文件管理系统	高平	何兴平，闫森，梁晓昀	一等奖
5	SOFT	上海交通大学	基于网络特征的恶意代码自动分析平台	邹福泰	白巍，贺宇轩，潘道欣	一等奖
6	XiLinx	上海交通大学	基于隐蔽信道检测的内网安全控制系统	宦飞	赖骏尧，许可，张文迪	一等奖
7	XiLinx	天津大学	基于 FPGA 的人脸识别身份认证系统	陈为刚	谢雪，赵亚洲，李静南	一等奖
8	SOFT	武汉大学	基于 android 的智能手机主动防护系统	彭国军	邵玉如，李晶雯，肖云倡	一等奖
9	SOFT	西安电子科技大学	免疫网络系统	胡建伟	吴一蔚，段瑾，马茗	一等奖
10	TI	西安电子科技大学	基于无线信道物理层特性的加密传输系统	郭万里	黄橙，赵楠，郭开泰	一等奖
11	XiLinx	西安电子科技大学	基于 Tate 对的无线医疗匿名监护系统	朱辉	邵杰，王娟，吴昊	一等奖
1	XiLinx	北京航空航天大学	基于超声波的空潜安全通信系统	金天	孙超，宋晨光，曲欣茹	二等奖
2	TI	北京交通大学	基于生物特征认证的安全支付系统	王升辉	刘明桦，张宸鸣，马晓璇	二等奖
3	XiLinx	北京交通大学	基于 FPGA 远程可重配置的云存储安全	张志飞	赵刘佳，郑杰，许华婷	二等奖
4	SOFT	北京邮电大学	基于云存储的远程集中式企业数据保护系统	崔宝江	何珊珊，黄强，王芃森	二等奖
5	SOFT	东南大学	网络语音碎片散射安全通信及原型系统	宋宇波	朱文远，顾实宜，邱林峥	二等奖
6	SOFT	桂林电子科技大学	远程端挂马检测系统	刘忆宁	颜聪，周永华，杨阳	二等奖
7	XiLinx	国防科技大学	防失密安全终端	张权	李中仁，白天，张兴	二等奖
8	TI	解放军信息工程大学	区域可控制无线通信系统	朱义君	蔡恒斌，杨宇，郭宇琦	二等奖
9	TI	南京大学	S2VIDEO 移动社交视频分享系统	王健	杜红阳，高晖，葛浩	二等奖

续表

序号	组别	学校	参赛题目	指导老师	参赛学生	获奖等级
10	XiLinx	南京大学	基于高帧视频的信息隐藏系统	袁杰	陈锡显，顾鹏，郭夏玮	二等奖
11	SOFT	山东大学	基于机器学习的非常态网络流量实时检测系统	刘磊	秦郑阳，宋丹，徐小程	二等奖
12	SOFT	上海交通大学	MWACS：恶意网站分析捕获系统	王轶骏	陆吉辉，姜望成，邵嘉炜	二等奖
13	TI	上海交通大学	主动智能视频监控系统	黄征	蔡韬，汪晟骢，李奇	二等奖
14	SOFT	四川大学	基于身份特征的零存储身份认证系统	刘嘉勇	王永恒，石刘洋，邓莅川	二等奖
15	SOFT	同济大学	基于手机动态密码的电脑使用权限管理系统	程久军	杨阳，赵子豪，胡长武	二等奖
16	XiLinx	同济大学	基于网络编码的同构HASH抗污染攻击系统	程久军	侯群磊，陈福臻，吴胤骏	二等奖
17	SOFT	武汉大学	基于DIFC的可信虚拟机环境构建	严飞	唐敬亚，熊胜超，胡文奕	二等奖
18	SOFT	西安电子科技大学	网络隐身系统	张卫东	张子兼，朱利军，高小青	二等奖
19	TI	中山大学	智能视频安全监控系统	卢伟	黄嘉斌，许国斌，陀得意	二等奖
1	SOFT	北京交通大学	基于PTM的可信虚拟平台	张大伟	于晓雪，马红霞，杨国忠	三等奖
2	SOFT	北京科技大学	基于rijndael的影像隐写加密系统	姚琳，陈红松	周雅慧，刘理博，王蕾	三等奖
3	SOFT	北京理工大学	基于数据流智能分析的内嵌式多层XSS Guaedian防护系统	苏京霞	叶子石，闫梓祯，王昕	三等奖
4	SOFT	北京邮电大学	基于Tcp Stream分析的网络进程连接监控系统	崔宝江	张小奕，靳梦泽，古恒	三等奖
5	TI	北京邮电大学	基于居民身份证与人脸特征的双因素身份识别系统	崔宝江	王焕骁，卢琼，杨守仁	三等奖
6	XiLinx	北京邮电大学	基于可信认证和信息加密的智能家居系统	崔宝江	邢亮，王骥腾，黄宇晴	三等奖
7	XiLinx	大连理工大学	基于NEXYS－3的RSA算法实现文件加解密	王开宇	厉超达，袭萌萌，周煜迪	三等奖
8	SOFT	电子科技大学	基于引导伪装的anti－bootkit程序	陈学英	秦皓，杨文玉，曹珩	三等奖
9	XiLinx	电子科技大学	基于击键习惯自学习的身份识别系统	许都	刘末洋，周末，杨慧然	三等奖
10	XiLinx	东北大学	基于FPGA的网络行为记录系统	王明全	王艳召，张壬申，杨启会	三等奖
11	SOFT	东南大学	GSM移动通信安全监测系统	宋宇波	朱筱赟，谭杭波，张皓月	三等奖
12	TI	东南大学	基于触摸认知的门禁系统	宋宇波	王有东，王国鹏，蓝骥	三等奖
13	SOFT	国防科技大学	安全加固的蓝牙即时信息交换系统	夏戈明	贾周阳，谢宗生，成朝勃	三等奖

续表

序号	组别	学校	参赛题目	指导老师	参赛学生	获奖等级
14	TI	国防科技大学	自主安全便携存储设备的设计与实现	赵文涛	刘雍，朱莉珏，邬会军	三等奖
15	SOFT	杭州电子科技大学	HDUSec－移动智能终端安全通话系统	张帆	周雷雷，于东壮，朱宇彬	三等奖
16	SOFT	杭州电子科技大学	基于笔迹验证的透明文件加解密系统	吴震东	吴姜苇，李昌志，高鑫	三等奖
17	XiLinx	杭州电子科技大学	HDUSec－安全隔离网闸	王小军	王华，蔡云龙，易际胜	三等奖
18	SOFT	华北电力大学	基于云计算的智能电网数据存储安全的设计与实现	张少敏	仇晶，张和琳，林雄	三等奖
19	SOFT	华中科技大学	基于多因素认证的声纹保密实时语音通信系统	钟国辉	徐峥，梁嘉骏，周朝进	三等奖
20	TI	华中科技大学	多方式实验室认证系统	肖看	何家乐，王明亮，林军	三等奖
21	XiLinx	华中科技大学	自适应多级别身份认证系统	王贞炎	李杨，常俊峰，罗广镇	三等奖
22	SOFT	解放军空军工程大学	基于数据漂移的动态云安全存储系统	王晓东	常沙，贾俊，杨成臻	三等奖
23	SOFT	解放军空军工程大学	基于文档透明存储的虚拟安全环境	陈超	赵绪，罗承昆，崔啸	三等奖
24	XiLinx	解放军信息工程大学	safe engine－可重构高速网络信息模式匹配引擎	单征	杨鑫，龚乔宜，张扬清	三等奖
25	SOFT	南京邮电大学	火眼金睛－恶意无线钓鱼接入点的检测技术	陈伟	孙明阳，蔡震寰，叶翰嘉	三等奖
26	TI	南京邮电大学	基于 UBIFS 的文件自粉碎技术研究与实现	杨一涛	申璐迪，乔安然，傅寒峰	三等奖
27	XiLinx	南开大学	基于噪声引导的二维超混沌身份认证系统的 FPGA 实现	李涛	刘保成，李文哲，李传军	三等奖
28	SOFT	四川大学	网络图片鉴别与溯源系统	刘亮	郝晨曦，刘尚奇，胡平	三等奖
29	TI	四川大学	基于 android 的多因子身份认证及加密系统	李智	王艺涵，傅雪梅，王文浩	三等奖
30	XiLinx	四川大学	LED 白光保密数据传输系统	李智	罗里，史慧萍，冯云勃	三等奖
31	SOFT	天津大学	基于 PC 平台的 android 安全评估系统	金志刚	刘志勇，姚贵丹，黄港膑	三等奖
32	TI	天津大学	基于射频识别技术的移动支付系统	马永涛	马驰，陆鸣，郭龙华	三等奖
33	TI	同济大学	语音信息安全系统	程久军	郭栋，林晓明，鄢晨丹	三等奖
34	TI	武汉大学	面向泄密追踪的数字水印在线嵌入系统	胡瑞敏	常迪，林霞，吴越	三等奖
35	XiLinx	武汉大学	基于 PUF 技术的硬件木马检测系统	唐明	杨建康，陈彦昊，孙伟晋	三等奖

续表

序号	组别	学校	参赛题目	指导老师	参赛学生	获奖等级
36	SOFT	西安交通大学	基于动态密钥的智能电网 zigBee 无线通信加密系统	刘烃	刘杨，毛亚珊，刘敏	三等奖
37	SOFT	西安邮电学院	基于 Android 的移动终端安全及取证系统	浩明	高家升，南玉哲，牛晨	三等奖
38	XiLinx	西安邮电学院	深度包检测技术的研究与 FPGA 设计	杜慧敏	张宽哲，王辉，韩玉青	三等奖
39	TI	浙江大学	月球车远程图像加密传输系统	马洪庆	毛宇毅，李顺斌，汪恒智	三等奖
40	SOFT	中山大学	基于可信计算的进程完整性度量监视器	蔡国杨	郭昂，王秉楠，翁时涛	三等奖
41	SOFT	重庆大学	基于语义的网络舆情监控与分析系统	桑军	王志伟，黄攀，刘锐	三等奖
42	TI	重庆大学	基于 TI 的抗 DDOS 防御系统设计	王毅	冯先，邓艺娜，王婷	三等奖
43	XiLinx	重庆大学	基于 FPGA 平台的自适应 IPS 设计	黄杨帆	冯海龙，李乾，吴锦	三等奖

目 录

软 件 组

TI 组

XiLinx 组

软件组

基于硬件指纹的密码生成系统

北京航空航天大学　彦晓宇　李胜曦　白　璐
指导老师：金　天

摘　要

当登录不同的网站时，为了便于记忆，用户要么使用一个或者两个强度较高的密码，要么使用多个弱密码，因此，如果网站数据库被泄露之后，用户不得不更改其他应用场合的密码，2011 年年底 CSDN 网站密码以明文形式泄露就是一个典型的例子。针对于此，本作品结合用户独有硬件指纹利用 SHA－512 单向散列函数的特性，用户只需记忆简单字符串，通过简单改变，就可以生成不同的高强度密码，应用在不同场合，保证泄露一个不至于影响个人全部密码，提高了互联网时代个人密码体系的安全性。

关键词：硬件指纹；密码生成；SHA-512；密码强度

Password Generation System Using Hardware Fingerprint

Abstract

When login different websites, users would like to use one complex password or use several simple passwords, in order to remember. Therefore, users have to modify the other similar passwords if one of their passwords has been leaked, for a typical example, the CSDN website's database being leaked in the year-end of 2011. Aiming at this situation, using the one-way hash feature of SHA-512, our project combines the initial password, special words and hardware fingerprint to generate a medium password, and then cut, join in and replace some bits of the medium password in order to meets user's requirements according to a rule. On the other words, users only need to remember simple initial password, and then, different complex passwords can be generated when a little change has been done. Naturally, strength of the personal password system in the Internet era has been improved.

Key words: hardware fingerprint; password generation; SHA-512; password strength

在我国，随着人们生活水平的不断提高，互联网应用在人们的生活之中扮演着越来越重要的角色。在使用不同的互联网服务时，使用者往往需要注册账号。但是当使用者需要注册的账号越来越多时，如何保证个人密码的安全性就显得尤为重要。尤其是在 2011 年 12 月 21 日 CSDN 网站 600 万用户资料被公开之后，个人密码体系的安全性就更加值得重视。作者以硬件指纹结合相关函数，设计出一种可用于提高个人密码体系安全性的系统，针对目前个人用户的密码体系缺陷进行修补，从而提高个人密码体系的安全性。

1　常见的个人密码体系分析及系统综述

1.1　CSDN 网站密码泄露事件分析

2011 年 12 月 21 日，国内最大的程序员社区 CSDN 中 600 万用户资料被公开，黑客公布的文件中包

含有用户的邮箱账号和密码。与此同时，人人网、开心网等诸多网站也要求用户更改密码。在当前的个人密码体系之下，如果某个网站受到攻击或者因为其他原因，使得其用户数据被公开，用户的账号也就随之泄露，账号中用户的个人信息很容易在各种渠道被传播。

1.2 常见的个人密码体系

在当今这个网络时代，每个用户都会拥有很多网络账户和密码。大多数用户为了便于管理和记忆，习惯只用一个常用的网络用户名、邮箱和密码；或者使用某些简单的弱密码，即位数较短、包含符号较为单一的密码，来登录一些用户认为不是很重要的网站。这样，如果其中的任一网站泄露用户的常用复杂密码，所有的网站账户都面临着安全威胁。同时，如果使用简单易记的密码，则容易被字典攻击；如果使用多个复杂的密码，则很难记忆。

综合个人对密码需求的分析，可以得出一组较安全的用户密码的特征为：

（1）便于使用者记忆；

（2）复杂程度高，即密码位数长、包含字符种类多；

（3）这一组密码相互之间差别大；

（4）不慎丢失密码后可以找回；

（5）具有隐私性，不含有包括使用者个人电子邮箱或身份证号等信息。

1.3 系统综述

针对上述个人密码的安全问题，设计出基于 ARM 的个人密码加强系统。该系统具有以下特色：

（1）软件植入硬件中，保证了系统本身的安全性；

（2）创新了一种个人密码保护体系，使用者只需记住一个密码（A 串），体系可以在不同网站生成不同密码，提高了安全性；

（3）通过读取 U 盘 ID，保证了只有 U 盘的持有者才能生成具有 U 盘特征的密码；

（4）安全中心具有数据备份、恢复的功能，数据备份是指在可信任终端之上，以加密形式存储备份 U 盘 ID 的数据。数据恢复是指当 U 盘丢失之后，可进入可信任终端，读取备份文件并更改绑定的U 盘；

（5）安全中心具有强度测试的功能，绑定的数据库中存储着常见的弱密码以及 CSDN 中的用户密码，通过强度测试可以给出相关的密码设定建议。

2 系统方案设计

本系统通过用户输入简单的记忆串，选择所需登录的网站，以及 U 盘 ID 的识别，将这三者作为初始值，通过安全散列算法——SHA-512 生成加强的密码，这是本系统的登录端。同时本系统的安全中心具有备份、还原、密码强度测试等功能。安全中心的备份功能将 U 盘 ID 以 AES 加密的形式存储。还原功能在 U 盘丢失后发挥作用，还原功能可以自动填写 U 盘 ID，从而使用户登录网站后，用新的 U 盘生成新的密码，将原密码修改成新的密码。密码强度测试功能基于本系统所捆绑的数据库，该数据库中存储着大量的常见密码，如果用户的密码与数据库中的密码有重复的，则提供相应的建议。

在算法上采用 SHA－512 进行密码的生成，保证了输入字符串的微小变化可以使得生成密码发生很大不同，再对 SHA－512 生成的串进行后期的处理，在特定位置上实现了字符的修改和替换，使得密码的强度进一步提高。这样，就可以通过记忆简单的字符串，生成复杂的、无规律的、高强度的密码。同时硬件指纹的引入可以保证在简单字符串泄露的情况下，仍然保证别人无法生成原有密码。密码的恢复功能通过在可信任设备上应用 AES 256 加密存储硬件指纹，可以在硬件丢失的时候，完成密码恢复工作。

2.1 纯电脑端系统方案

2.1.1 纯电脑端生成密码的实现方法

1）将初始密码和特征串，以及插入硬件的硬件指纹相拼接。

2）对拼接好的字符串进行 SHA-512 散列运算，生成原始密码串。

3）对生成的原始密码串进行字符替换，并根据设置实现是否添加特殊字符。

4）显示生成的最终密码。

2.1.2 **纯电脑端备份硬件指纹以及恢复密码的实现方法**

1）在电脑上插入硬件并提取插入硬件的硬件序列号，通过 AES 加密存储在可信任设备上。

2）恢复密码时，先将加密存储的硬件指纹解密，再与初始密码和特征串拼接。

3）重复密码生成和处理过程。

2.2 ARM 板系统方案

2.2.1 **结合 ARM 板的密码生成的实现方法**

1）电脑上将输入的初始密码和特征串拼接，确定生成位数和是否包含特殊符号。

2）电脑端软件通过串口通信将生成密码所需要的信息发送至 ARM 板，ARM 板将其上插入硬件的硬件指纹提取，并和传输来的数据进行拼接。

3）ARM 板端软件通过 SHA-512 进行计算和处理。

4）ARM 板通过串口将生成的密码传输到电脑。

5）电脑接收并显示生成的密码，并自动复制到剪贴板。

2.2.2 **结合 ARM 板的备份硬件指纹以及恢复密码的实现方法**

1）在 ARM 板上插入硬件并提取插入硬件的硬件序列号，通过 AES 加密存储在可信任的设备上。

2）恢复密码时，先将加密存储的硬件指纹解密，再与电脑端传输的初始密码和特征串拼接。

3）重复密码生成和处理的过程。

4）ARM 板通过串口将生成的密码传输到电脑。

5）电脑接收并显示生成的密码，并自动复制到剪贴板。

3 系统软硬件实现

3.1 密码生成的实现过程

3.1.1 **PC 端生成密码过程**

当用户打开登录端后，会有三个文本框，分别为初始密码，网站特征码，生成结果。初始密码栏要求用户输入 6 ~ 32 位的密码，网站密码栏要求用户输入与网站相关的数字或字母，若这两者中的任一者的输入值不符合要求，点击生成密码按钮时，都会相应地弹出对话框，提示用户初始密码或网站特征码太短，需要重新输入。除此之外，生成密码还需要插入 U 盘以读取 U 盘 ID，如果没有插入 U 盘，就点击了生成密码按钮，则会弹出对话框，提醒用户插入 U 盘。

3.1.2 **ARM 板生成密码过程**

当用户在 PC 端输入初始密码，网站特征码，生成的位数，是否有特征字符串等信息，通过串口通信，将信息传给 ARM 板，ARM 板将以上信息以及读取到的移动设备 ID 综合起来，生成最终的密码。再通过串口通信将生成的密码传给 PC 端，PC 端接收到信息后将密码显示在界面中。

生成密码的过程如图 1 所示。

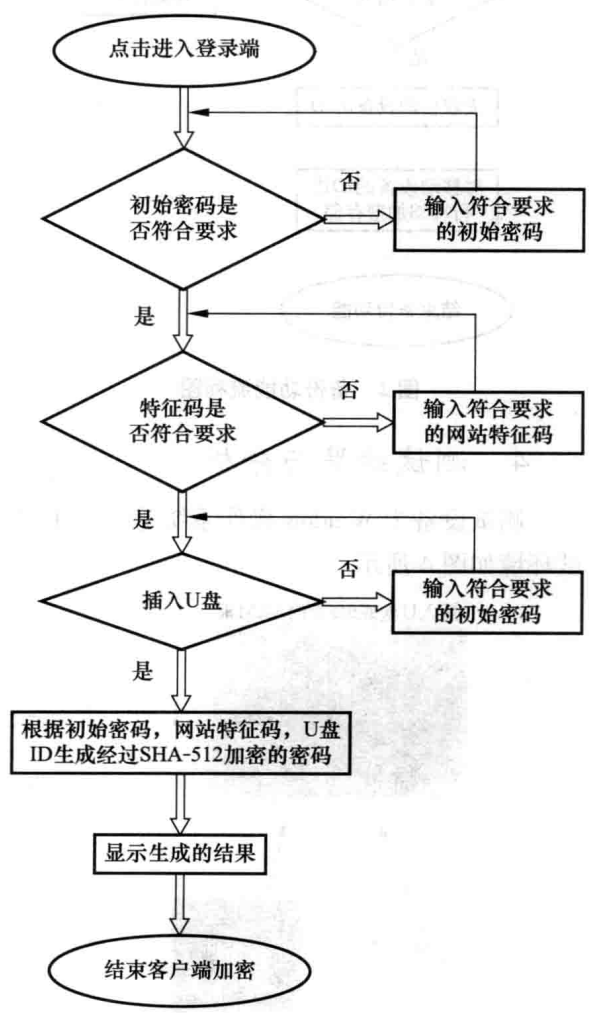

图 1 PC + ARM 端生成密码流程图

3.2 备份、恢复功能的实现过程

备份和恢复功能是为了避免当用户丢失移动设备后，无法读取移动设备的 ID 而导致无法生成密码。当用户打开安全中心，点击备份硬件指纹按钮时，系统会读取移动设备的 ID 并以 AES 加密的形式存储。

而当用户丢失移动设备后，进入安全中心，点击恢复密码按钮，则会弹出恢复密码的对话框，恢复密码的界面利用已存储的硬件指纹恢复用户密码。其中的初始密码、网站特征码需要输入，而在恢复功能下，不需要插入移动设备，在恢复密码界面中，点击恢复密码按钮后，系统会自动读取以加密形式存储的移动设备的 ID 并进行解密，解密出的移动设备的 ID 与初始密码、网站特征码一起生成最终的 SHA-512 加密的密码。

备份以及恢复功能的流程图如图 2 和图 3 所示。

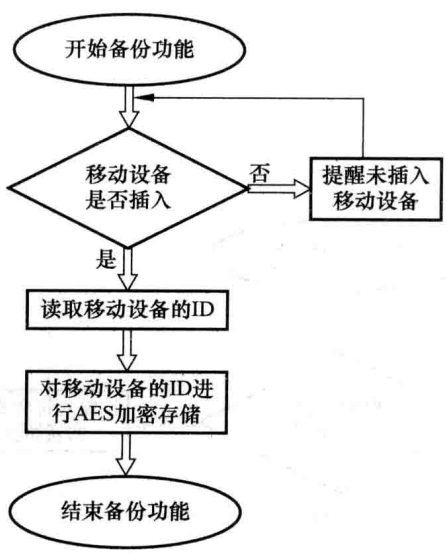

图 2　备份功能流程图

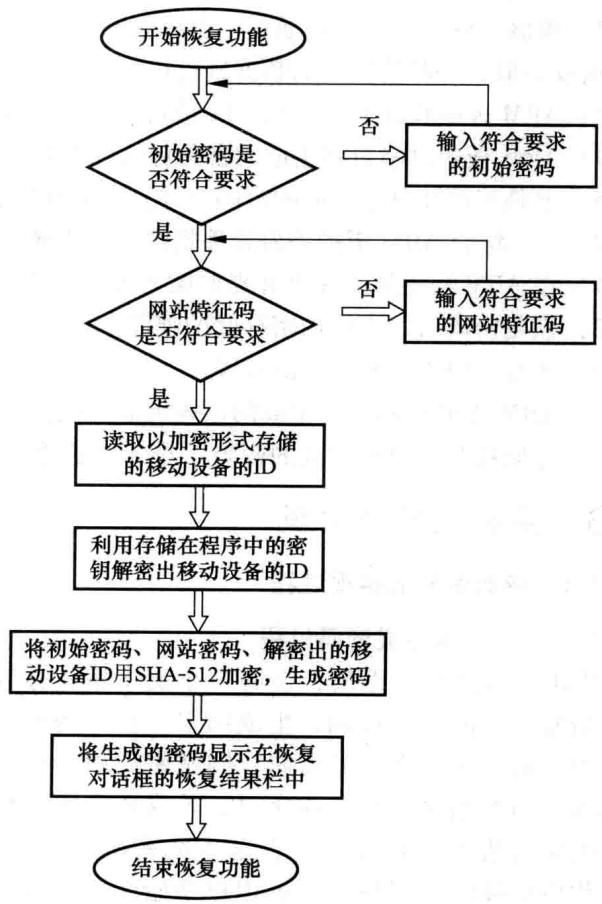

图 3　恢复功能流程图

4　测试结果与分析

测试设备为 Window 操作系统笔记本 1 台，ARM 板一块，数据线一条，SD 卡两个，U 盘一个。测试环境如图 4 所示。

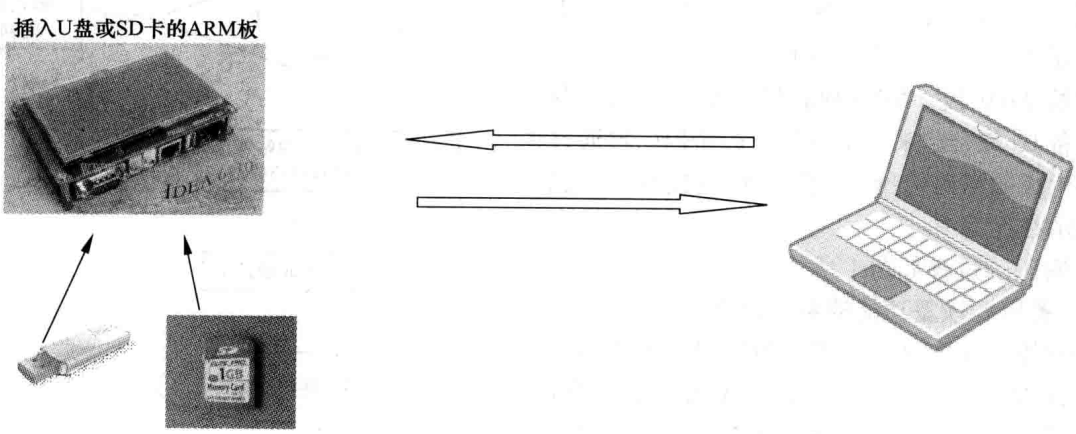

图 4　测试环境示意图

最终测试结果列表如表1和表2所示。

表1　纯电脑端密码生成测试结果

测试编号	实验说明	初始密码	特征串	硬件设备	特殊符号	生成密码	说　明
1	密码生成	123456	126. com	U盘	否	yQ49sRF1697df4b1	16位
2	密码生成	123456	126. com	U盘	是	"Q+9sRF1697df4b1	16位
3	密码恢复	123456	126. com	U盘	否	yQ49sRF1697df4b1	与测试1相同
4	密码恢复	123456	126. com	U盘	是	"Q+9sRF1697df4b1	与测试2相同

表2　PC+ARM端密码生成测试结果

测试编号	实验说明	初始密码	特征串	硬件设备	特殊符号	生成密码	说　明
1	密码生成	123456	163. com	SD卡1	是	5-G1i6C570*ecJQe	16位
2	密码生成	123456	163. com	SD卡2	是	/A16SDuY-4r08f8*	与测试1不同
3	密码生成	123456	163. com	U盘	是	4-y4T8BA（faYdX&v	与测试1不同
4	密码生成	123456	163. com	手机	是	（W+11Q985048b6bc	与测试1不同
5	密码生成	123456	feixin	SD卡1	是	m. 5v%2F76W142e81	与测试1不同
6	密码恢复	123456	163. com	SD卡1	是	5-G1i6C570*ecJQe	与测试1相同

5　总结

5.1　作品特色

1）本作品组合应用SHA-512算法和AES-256算法。SHA-512算法是安全散列算法，为一种单向散列函数，由输出不太可能推算出输入，这就保证了由最终密码无法得到初始密码。另一方面，以现今最为强大的计算机为标准，破解AES密钥的时间约为几十亿年，这保证了加密数据的安全性。

2）本作品结合了硬件指纹，将硬件指纹作为原始串的一部分，硬件设备可以作为身份的象征，确保了本系统的安全性。

3）将网站特征码作为原始串的一部分，这样对应于不同的登录网站或者登录软件，可以生成不同的高强度的密码，实现了一个简单串衍生出多个复杂强密码的功能。

4）可以进行碰撞测试，保证密码的安全性；为用户提供了多达60多万条的弱密码，以防止最终的密码是一个弱密码，进一步确保了密码的强度。建立起一套比较完备的密码生成体系。

5）用户只需要记忆简单的字符串，便于用户使用，系统的易用性很强。

6）本作品有两个版本，可以在只有电脑的环境下使用，也可以将电脑与ARM开发板结合生成密码，在只有电脑的环境下使用安全性不强，电脑上的程序可能被黑客进行代码分析、破解。所以另一版本将系统移植到ARM板中，以硬件为媒介确保了系统的安全性。

5.2　应用前景分析

本系统主要可用于以下三个方面：

1）用于加强个人密码体系，对于个人而言，使用本系统用户可以针对不同网站和应用程序，通过改变特征串，生成不同密码，防止一个密码泄露后全部个人密码泄露，用户只需记住一个简单串，就足以保证每个网站的密码都足够复杂并且有很大的区分度。

2）用于保密单位的密码更换，保密单位要求每十四天更换一次密码，并且对密码强度有较高的要求。无疑增加了员工的记忆负担。而使用本系统，通过特定硬件和输入，可以生成完全无规律的、差异很大的密码，同时便于记忆。为保密单位提供方便、足够复杂的密码保护。

3）防御字典攻击，本系统可以对最后生成的密码进行评价并与CSDN库进行碰撞，保证生成的密码不会是弱密码达到防御字典攻击的目的。

本系统的备份与恢复功能保证了SD卡或者U盘等硬件设备丢失后仍可以登录账户，使整个体系更加全面。

就未来的应用前景而言，可以将本系统开发为一个嵌入在手机中的应用系统，将手机的存储卡的序列号作为硬件指纹，方便使用。

专家点评

作品针对传统个人密码易于泄露问题，利用SHA-512单向散列函数的特性，将初始密码、特征码