

**毕业设计(论文)教学档案**

|  |  |
| --- | --- |
| 题 目： | 基于椭圆曲线数字签名的二维码生成与验证系统 |
| 姓 名： | 陈露 |
| 学 院： | 计算机科学与技术学院 |
| 专 业： | 信息安全 |
| 班 级： | 04041502 |
| 学 号： | 2015211891 |
| 指导老师： | 于洪 |

**重庆邮电大学教务处制**

**二O一 年 月**

**重庆邮电大学本科毕业设计（论文）任务书**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 题 目 | 基于椭圆曲线数字签名的二维码生成与验证系统 | | | |
| 学生姓名 | 陈露 | | 学 号 | 2015211891 |
| 指导教师 | 于洪 | | 所在单位 | 计算机科学与技术学院 |
| 题目类型 | □应用型□研究型☑综合型□其它 | | | |
| 是否需要在实验、实习、工程实践和社会调查等社会实践中完成（ □是 ☑否 ） | | | | |
| 一、研究目标 | | | | |
| 随着移动支付、便捷支付的出现和发展，二维码应运而生。二维码的出现极大的满足了收付款效率、办事效率和与软件配套使用的服务的速度效率提升的迫切需求。其便捷性，使得二维码现已经在很多方面得到广泛的运用。但另一方面，二维码的具体结构，导致了二维码实际上不能为人所辨识判断，这一点极有可能被不法分子或者黑客利用。他们可以通过伪装等方式，诱使二维码用户在不知情的情况下进行不合乎本意的操作甚至损害自身权力利益等。  因此，本设计主要目标是运用基于椭圆曲线的数字签名，嵌入在二维码的生成中，制作一个简易的可靠二维码生成系统，并在系统中，附加二维码的验证，以便使用户了解某二维码的签名作者具体是谁，做出二维码是否相对安全的建议。 | | | | |
| 二、主要研究内容和方法 | | | | |
| **1.研究内容**   1. 椭圆曲线数字签名算法的生成和封装。 2. 签名算法在原始二维码生成算法中的嵌入。 3. 二维码数据的存放。 4. 待验证二维码的扫描，解密和验证。 5. 系统的集成和可视化。   **2.研究方法**   1. 结合密码学椭圆曲线数字签名相关知识，实现主要核心算法的封装。 2. 对开源的QR二维码生成算法进行修改和编辑，使之能生成具有数字签名标识的二维码。 3. 借助c++实现可视化系统，并扫描待二维码结构，解密数字签名，与mysql数据库进行读写交互，得出比较结果告知用户。 | | | | |
| 三、主要考核要求或指标 | | | | |
| 1. 掌握基本的数字签名算法及二维码生成时的嵌入方法。 2. 制定系统功能模块，编程完善各个功能。 3. 测试系统功能。 4. 编码规范方面： 5. 尽量使用完整的英文描述符。 6. 采用相关领域的术语命名。 7. 采用大小写混合使名字可读。 8. 尽量少使用缩写，但如果用了，要明智地使用，且在整个工程中统一。避免使用长的名字、类似的名字和下划线。 | | | | |
| 四、主要参考文献 | | | | |
| 1. Jeremy Lam. United States Patent Application Publication [J]. 2016, 05-22.   黄文培．一种基于信息隐藏的图像二维码设计［D］ ．成都: 西南交通大学， 2015． ..  闫涛, 游福成, 刘福平. 基于数字签名的QR码水印认证系统[J]. 信息安全研究, 2016, 2(3):258-263.  谭德林, 李均利. 一种具有数字签名的二维码技术[J]. 计算机技术与发展, 2018(3):143-145.  Sadikin M A, Sunaringtyas S U. Implementing digital signature for the secure electronic prescription using QR-code based on Android smartphone[C]//Technology of Information and Communication (ISemantic), International Seminar on Application for. IEEE, 2016: 306-311.  Zhang J, Liu S J, Pan J S, et al. Digital Certificate Based Security Payment for QR Code Applications[C]//The Euro-China Conference on Intelligent Data Analysis and Applications. Springer, Cham, 2017: 88-97.  Melgar M E V, Santander L A M. An alternative proposal of tracking products using digital signatures and QR codes[C]//Communications and Computing (COLCOM), 2014 IEEE Colombian Conference on. IEEE, 2014: 1-4. | | | | |
| 指导教师签字： 年 月 日 | | | | |
| 专业负责人意见：  □同意立题  □不同意立题   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | 负责人签字： | |  | | | | |  | 年 |  | 月 |  | 日 | | | 学院意见：  □同意立题  □不同意立题   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | 负责人签章： | |  | | | | |  | 年 |  | 月 |  | 日 | | | |

备注：1.此任务书由指导教师填写，并于毕业设计（论文）选题结束后尽快下达给学生。

2.任务书一经审定，指导教师和学生不得随意更改，如因特殊情况确需变更，应在完成开题报告之前，填写《重庆邮电大学毕业设计（论文）更改题目审批表》，报专业负责人审核、学院复核批准后执行，并报教务处备案。