

**北京大学软件与微电子学院信息安全工程**

**题目：基于汉字的图形口令**

**组员：陈波波 吴诗晨 杨晨 \*\***

**指导老师：孙惠平**

**2017年10月24日**

目录

[一、选题背景 3](#_Toc496649203)

[二、产品现状 3](#_Toc496649204)

[三、研究现状 3](#_Toc496649205)

[四、主要思路 4](#_Toc496649206)

[五、项目分工 5](#_Toc496649207)

[六、项目计划 6](#_Toc496649208)

# 一、选题背景

在身份认证方案中，口令的空间与口令的易记忆性往往是矛盾的，图形密码作为一种新兴的身份认证技术克服了传统字符口令的诸多缺点，能够在口令的安全性和可用性之间达到较好的平衡。考虑到国人对自己的母语--汉字有着天生的敏感度，而汉字这门古老又复杂的语言有着较高的信息熵（冗余度小），因此是否存在一种身份认证方式能够将图形认证与汉字相结合，利用汉字的特性（比如汉字的书写构造，汉字之间的关联与表意等）来构造一种新的图形密码认证，使得口令的安全性和可用性都能达到一个较高的水平。

# 二、产品现状

目前汉字图形大多数都是用来做图形验证码，较少见用做口令做身份验证的产品。

# 三、研究现状

目前关于图形口令的研究主要可分为两大类：基于回忆（又可分为无提示和有提示）的图形口令和基于识别的图形口令。其中基于回忆的图形口令主要要求用户重复以前设定的一个过程，比如事先要求用户在一个图形上按预先顺序点击一些位置，身份认证时重复此过程。而基于识别的图形口令主要是由系统从图案库中随机产生一组图片，用户从中选择并记住某些图片，认证时需要识别曾经记住的图形。图形口令的设计需要同时考虑的安全性和可用性，因此目前很多的方案也都是在理论阶段，并未投入使用。

关于汉字图形口令，目前还没在国内找到相关的研究，需要类比已有方案自行探索。

# 四、主要思路

研究思路主要分为汉字特性、图形认证、安全性、可用性和实现五大模块展开。首先分析汉字的特点，可分为研究汉字的部件构造（比如左右结构、上下结构等），以及研究汉字的关联表意（汉字与汉字组成的词语、成语等有意义的词）。通过研究汉字的特点来寻觅中文图形密码应具有的特性；其二，查询现有的国内外文献中有关图形密码的内容，比如图形密码可以分为识别型（单点触控、多点触控）、回忆型（无提示、有提示）、混合型三大模型，这三种模型下又可继续细分为许多具体的图形密码，通过分析比对这些图形密码的特征，并考虑其与汉字结合的可能性（目前已发现的可结合的种类有TAPI、CCP、MIBA和Pass-Go）；其三，安全性。密码的安全性是信息安全至关重要的一环，需要充分考虑其口令空间的大小，口令空间大小又可以从理论口令空间和有效口令空间两个方面去分析与论述，同时还要考虑不同攻击下的鲁棒性，比如暴力破解、字典攻击、肩窥攻击、社会工程等攻击下口令遭受破译的可能性；其四，可用性。可用性是与安全性相对的一个指标，本项目的重点就是要在两者之间找到一个平衡点，并使二者尽量都高一些。所以安全性可以考虑用户密码的记忆复杂度、用户选择热点的可能性、认证时间大小、成功率等等；最后，实现，通过以上过程找到一个可行方法后尽可能做一个Demo，并进行相关用户实验，这是后期工作，具体技术细节前期不涉及。



# 五、项目分工

汉字构造和图形密码的安全性和可用性是每个人都要做的。每个人从现有的图形认证方式出发，研究其与汉字结合的可能性：

A: TAPI

B:CCP&&MIBA

C:PASS-GO

D:其他

以上是四个不同图形认证的出发点(目前发现的可行的)，每名成员完成各自的分析后进行一个汇总，形成一篇总结报告，同时通过头脑风暴探讨出一个综合型的最优方案来进行实现(目前实现方面还未分工)。

# 六、项目计划

项目旨在研究汉字图形密码的可能性，因此会从多角度出发横纵向对比不同方案的优势和不足，最后完成一个完整的综述性报告。主要侧重点在于汉字图形的可能性，实现是其次，项目后期完成综述报告后，会尽可能对其中一个较成熟的方案进行实现，做一个DEMO。