**第十届中国大学生服务外包创新创业大赛**

****

**Ankh多方安全计算平台**

**详细设计**

团队：1900156-我的队名不让你看

赛题：A11-多方数据安全计算平台的设计与实现

团队成员：丁峥元 赵大燕 黄怡 郭延鹏 向云帆

指导老师：杨柳 陈帆

二零一九年十二月——二零二零年五月

**目 录**

[**第一章 项目概述** 1](#_Toc41419049)

[**1.1 项目背景** 1](#_Toc41419050)

[**1.2 项目目标** 1](#_Toc41419051)

[**1.3 系统亮点** 1](#_Toc41419052)

[**第二章 解决思路** 3](#_Toc41419053)

[**2.1 问题描述** 3](#_Toc41419054)

[**2.2 解决思路** 3](#_Toc41419055)

[**2.3 解决方案** 4](#_Toc41419056)

[**第三章 系统设计** 6](#_Toc41419057)

[**3.1 放贷用户模块** 6](#_Toc41419058)

[**3.2 平台管理员模块** 8](#_Toc41419059)

[**3.3 政府管理员模块** 10](#_Toc41419060)

[**3.4 贷款用户模块** 11](#_Toc41419061)

[**3.5 数据模型** 13](#_Toc41419062)

[**3.6 数据库接口设计** 17](#_Toc41419063)

[**第四章 技术方案** 21](#_Toc41419064)

[**4.1 CKKS加密运算全同态方案** 21](#_Toc41419065)

[**4.2 MAX，MIN函数处理——百万富翁问题** 24](#_Toc41419066)

[**4.3多方安全计算端开发方案** 27](#_Toc41419067)

[**4.4政府端及计算端部署** 28](#_Toc41419068)

[**4.5加密方案性能及安全性分析** 31](#_Toc41419069)

[**4.6前端设计方案** 32](#_Toc41419070)

[**第五章 组织管理** 44](#_Toc41419071)

[**5.1 组织结构** 44](#_Toc41419072)

[**5.2 角色与职责** 44](#_Toc41419073)

[**5.3 协作与沟通** 45](#_Toc41419074)

[**5.4 项目日程** 46](#_Toc41419075)

[**5.5 开发模型** 46](#_Toc41419076)

[**第六章 测试计划** 47](#_Toc41419077)

[**6.1简介** 47](#_Toc41419078)

[**6.2 参考资料** 47](#_Toc41419079)

[**6.3 测试安排** 47](#_Toc41419080)

[**6.4测试资源** 48](#_Toc41419081)

[**6.5测试策略** 49](#_Toc41419082)

[**6.6测试风险和优先级** 50](#_Toc41419083)

[**6.7 测试标准** 50](#_Toc41419084)

[**第七章 商业分析** 52](#_Toc41419085)

[**7.1 市场背景** 52](#_Toc41419086)

[**7.2 市场分析** 52](#_Toc41419087)

[**7.3 资源投入** 53](#_Toc41419088)

[**7.4 SWOT分析** 54](#_Toc41419089)

[**7.5 竞争策略** 55](#_Toc41419090)

[**7.6 风险分析** 56](#_Toc41419091)

[**7.7 推广方案** 56](#_Toc41419092)

[**7.7 盈利模式** 58](#_Toc41419093)

**第一章 项目概述**

**1.1 项目背景**

随着大数据、人工智能等数字经济时代新兴技术日益成熟，在日常生活中已经得到广泛应用，各行各业沉淀下来的数据背后所蕴含的潜在价值越来越受到大家的高度重视，数据已成为企业和国家具有战略价值的核心资产。

从数据价值角度来看，数字经济时代，越来越多的企业或组织需要与产业链上下游业务伙伴在数据流通和交易领域进行深度合作。因为只有通过各方数据协同计算，才能避免“数据孤岛”——数据之间由于各种原因产生的壁垒(政府数据由于保密政策不能对外公布，运营商、互联网收集客户的数据信息，但他们不会将这些数据透露给第三者），才能更好地释放数据更大的价值，提升生产效率，推进产业创新。数据共享和流通将成为刚性业务需求。

从安全性角度来看，保证个人信息、商业机密或独有数据资源等隐私信息在数据处理、流转过程中不会泄露，是企业或组织参与数据共享和流通合作的前提条件。 这样才能避免“数据泄露”——隐私安全问题严重；facebook的数据泄露事件影响很大，原因就是facebook单方面将用户的个人数据提供给了第三方机构，这为个人数据的拥有权敲响了警钟。

因此，目前急需一个既能保护数据隐私又能实现数据流动起来最大化其价值的解决方案——多方数据安全计算平台。

**1.2 项目目标**

多方数据安全计算平台的开发主要目标在于：利用政府端提供的加密数据，根据对应的风控模型公式采用同态加密算法构造密文运算流程，对密文数据进行计算，从而在保证用户隐私数据不被泄露的前提下，获得有价值的数据。

此外，该平台可入驻贷款机构，为贷款用户提供便利的一站式申请平台。

**1.3 系统亮点**

1）利用微软的Seal库中CKKS算法的方案实现数据的加密，并设计一套运算库，可对密文进行四则运算，实现整个实数域内的全同态加密运算。

2）核心计算端拥有智能的交互机制，实现数据提供方与多方安全计算平台的完美交互，包括密文的传输，一般公式计算以及大小比较时数据传递等。

3）完美处理风控模型中MAX或MIN函数，通信交互并结合Pailliar加密算法，在保证数据隐私性的前提下，实现数据大小的比较。

4）多方安全计算平台可以自动识别处理输入的部分类型风控模型公式，能够自动解析风控模型公式中运算符机器中优先级，不同的运算符自动调用对应的密文运算法则。

5）支持多用户同时使用多方安全计算平台，在线查询计算数据。并能合适地处理冲突，当服务器端负载过大时，返回等待信号，维持系统良好运行。

6）完善的系统体系，为贷款用户及放贷机构提供在线办理、快速审批的一站式服务平台，节约人力成本。

7）服务器可以防御CSRF攻击，更好地维护用户隐私数据安全。

**第二章 解决思路**

**2.1 问题描述**

安全多方计算旨在解决一组互不信任的参与方之间保护隐私的协同计算问题，为数据需求方提供不泄露原始数据前提下的多方协同计算能力。体现在系统流程中主要分为一下几个方面：

1）实现政府或数据提供方明文数据同态加密加密传输，传统加密方案只能实现加密无法直接操作密文计算。

2）数据完全保密，要求明文数据完全保留在政府或数据提供方数据库中，达到在保护机密的前提下实现数据共享。

3）实现运算同态，针对加密算法实现随密文直接计算的运算法则，保证密文结果解密后与按照相同运算公式的明文结果相同并且控制计算复杂度以及密文大小。

4）风控模型部署，实现风控模型翻译，将公式编译为计算平台可以计算的程序。

5）管理方便，实现数据端方便管理数据使用，实现风控模型部署端方便管理以及安装风控模型。

1. 界面友好，实现用户方便查看计算结果等。
2. 服务器端一对多应用，能够实现多用户同时使用计算平台计算。

**2.2 解决思路**

1）利用CKKS加密算法加密数据，其安全性建立在理想格上的最短向量(SVP)问题，该问题可以量子规约到R-LWE问题。

2）针对加密算法专门设计一套计算库，提供密文计算的四则运算

3）设计一个优秀多方安全计算平台，能够自动解析风控模型公式中运算符机器中优先级，不同的运算符自动调用对应的密文运算法则。

4）设计一个完整交互流程，实现数据提供方与多方安全计算平台的完美交互，包括密文的传输，一般公式计算以及大小比较时数据传递等。

5）设计一个完整的多方数据大小比较方案，处理风控模型中MAX或MIN函数。

6）优化服务器，实现服务器端程序多线程运行，能够支持多用户同时使用给计算平台。

7）处理冲突，当服务器端负载过大时，返回等待信号，维持系统良好运行。

**2.3 解决方案**

2.3.1系统架构

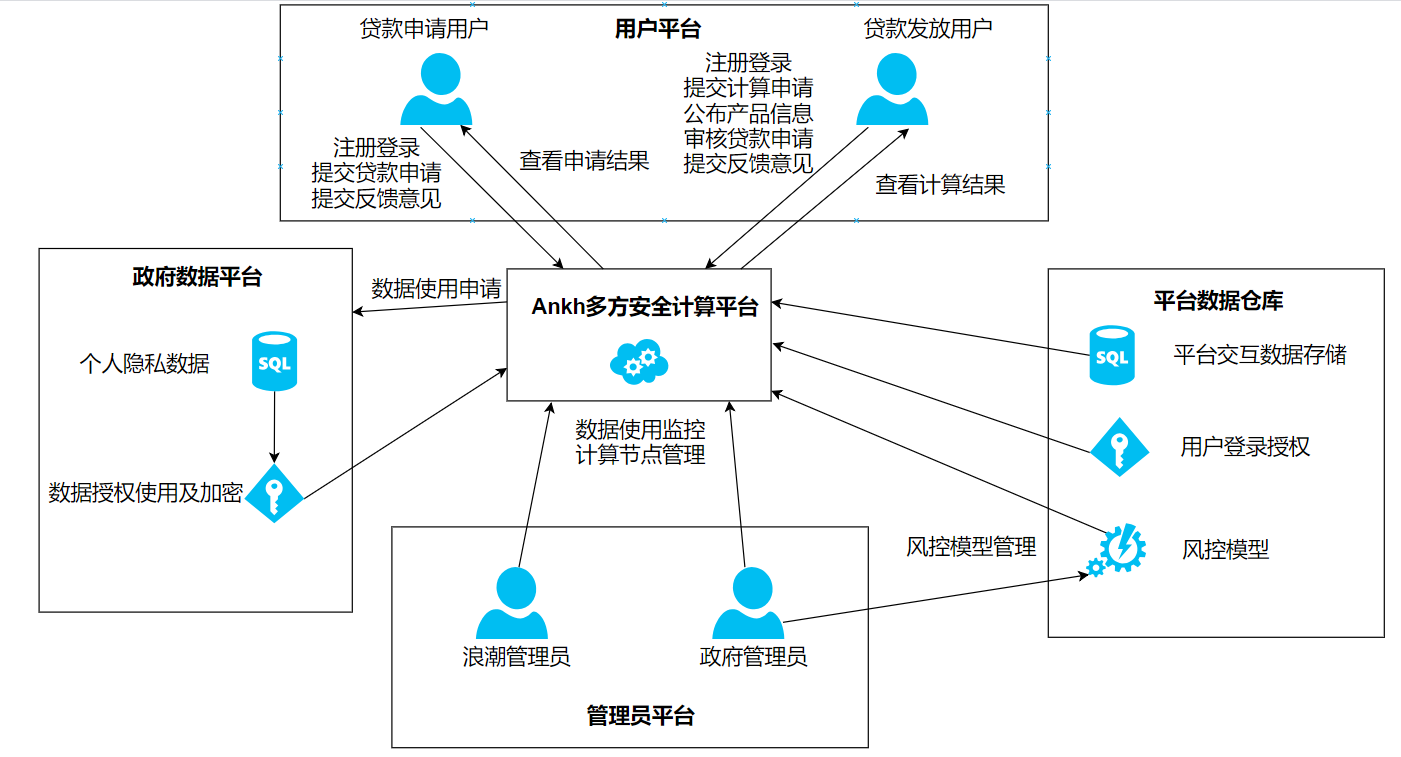


图2-1 系统架构图

2.3.2组织部署

1）政府数据平台

构建数据库，存放用户数据信息。在收到数据请求后，验证请求方信息，若得到授权则按一定加密算法对相关数据进行加密，并将加密公钥公开。同时，政府端授权一受信方对部分中间结果进行加/解密及其他数据交互处理。此外，最终的数据结果，也经由该方交付。

2）Ankh多方安全计算平台

分为核心计算模块以及服务器模块。计算部分接入风控模型进行对密文的运算操作以及比较操作，得到计算申请结果。服务器模块完成平台其余各项数据交互以及对前端页面的支持。

3）平台数据仓库

存放平台交互以及计算所需数据，用于支持平台注册、登录、身份认证以及贷款申请等功能。

4）管理员平台

对平台数据使用情况进行实时监控，对各使用量进行可视化显示，以及查看模型历史数据，并可完成风控模型部署。

5）用户平台

可实现用户注册登录。作为贷款申请用户可以提交贷款申请，查看贷款结果，提交反馈等操作。作为提供贷款的企业或银行可以管理产品，提交计算请求，提交申请审核结果以及提交反馈等操作。

2.3.3服务对象

本多方安全计算平台面向四个服务对象，分别为政府，放贷机构用户，贷款申请用户及平台管理人员，具体服务内容如下表所示。

表2-1 服务对象表

|  |  |
| --- | --- |
| 服务对象 | 具体服务内容 |
| 政府 | 1. 数据库管理 2. 数据使用授权 3. 数据加密传输，解密及少量数据计算 |
| 放贷机构用户 | 1. 平台注册与登录，以及企业注册信息的查看与修改 2. 企业提供的贷款产品的部署与管理 3. 管理贷款用户对于产品的申请请求，并向计算平台发起计算申请 |
| 贷款申请用户 | 1. 平台的注册和登录，以及用户注册信息的查看与修改 2. 查看各放贷用户提供的贷款产品，并对放贷方的产品发起申请请求，查看申请结果 |
| 管理人员 | 1. 政府管理员登录政府管理端实现风控模型的部署和管理、历史数据查看 2. 浪潮管理员登录平台管理端查看平台使用情况、计算节点管理以及查看和处理平台使用的反馈信息 |

**第三章 系统设计**

**3.1 放贷用户模块**

3.1.1 描述

放贷用户模块面向的用户角色为银行等提供放款的企业，为放贷用户提供了一个可以处理贷款用户申请和管理贷款产品的平台，是计算平台中计算请求的发起端。当贷款用户申请了某一项贷款产品时，放贷用户会收到请求。

3.1.2 功能

1）平台注册和登录功能

①注册：放贷用户申请注册账户，填写邮箱密码、企业法人信息和统一企业信用代码等企业信息就可以成功申请账号。

②登录：注册过的用户直接输入账号密码登录。

2）管理贷款申请功能

查看待处理申请、申请计算授信，同意或拒绝已计算申请，撤销已处理申请。

①查看待处理申请：贷款用户的申请在待处理申请列表中显示。

②申请计算授信：放贷用户可以对每一条待处理申请进行申请计算授信操作。

③查看授信计算结果：由计算平台计算的申请在已计算申请列表中显示，每一条申请的授信计算值将会被显示。

④同意或拒绝申请：根据授信计算值，可以对每一条申请进行同意申请或者拒绝申请处理。

⑤查看已处理申请：已处理过的申请在已处理申请列表中显示，每一条申请记录显示授信计算值和处理结果。

⑥撤销已处理申请：对已处理的申请可以撤回操作，同时记录会从已处理申请列表中消失而再次在已计算申请列表中显示。

3）管理贷款产品功能

查看贷款产品信息，新增或删除贷款产品，修改产品的状态、风控模型参数等信息。

①查看贷款产品信息：在产品列表中可以看到所有产品的主要信息和状态。点击每一项产品对应的操作可以查看详细信息页，详细的信息包括：产品编号、产品名称、贷款类型、贷款金额、年龄限制、授信年限、产品利率、还款方式、贷款用途、产品介绍、产品优势、申请所需材料、产品对风控模型以及风控模型种的具体参数和产品状态。

②修改产品信息：查看每一条产品的详细信息后可以进行修改，上述详细信息都可以进行修改。 但产品编号不可有重复。

③新增产品：完整填写产品的详细信息以新增产品。

④新增删除：在详细信息页删除某一个贷款产品。

4）查看修改用户信息功能

①查看或修改信息：在用户信息中查看注册时填写的信息并修改。

②修改密码：通过修改密码项修改密码。

5）意见反馈功能

在意见反馈中向计算平台反馈使用中遇到的问题，描述意见主题，内容，选填联系方式。

6）接受消息通知功能

计算平台对风控模型做出了任何变更时，会向各放款用户端发出通知公告。通过消息通知查看。

3.1.3 流程逻辑

该模块的流程逻辑图如下：

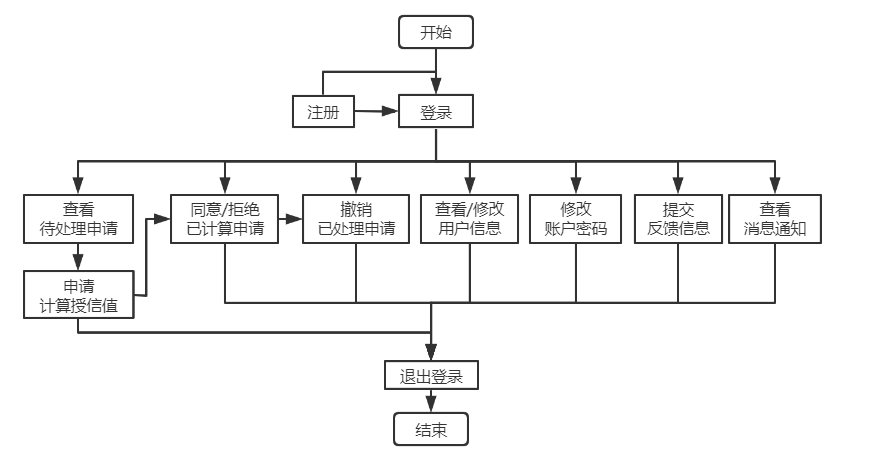


图3-1 放贷机构用户流程图

* + 1. 文件清单

表3-1 放贷机构用户网页文件

|  |  |
| --- | --- |
| 文件名称（相对路径） | 说明 |
| /templates/crt-bank.html | 注册页面 |
| /templates/login.html | 登录页面 |
| /templates/bank.html | 后台首页页面 |
| /templates/bank\_applylist.html | 待处理申请页面 |
| /templates/bank\_resultlist.html | 已计算申请页面 |
| /templates/bank\_donelist.html | 已处理申请页面 |
| /templates/bank\_product.html | 产品管理页面 |
| /templates/bank\_productPagex.html | 产品详细信息页面 |
| /templates/bank\_userinfo.html | 用户信息页面 |
| /templates/Edit\_pwd.html | 修改密码页面 |
| /templates/bank\_feedback.html | 意见反馈页面 |
| /templates/bank\_notice.html | 消息通知页面 |

**3.2 平台管理员模块**

3.2.1 描述

平台管理员模块面向的用户角色为浪潮方负责监督和管理计算平台的管理人员，为浪潮方管理员提供了一个可视化监管的平台，能够进行计算历史记录数据查询以及计算节点管理等。

3.2.2 功能

1）平台登录功能

登录：平台管理员根据浪潮公司内部提供的账号和初始密码直接通过登录页面登录。

2）查看平台使用情况功能

①查看数据记录总览：可以看到每一条申请记录的详细信息和状态，详细信息包括：风控模型种类，申请方，申请产品，申请时间，计算人姓名，身份证号码（出生日期不可见），状态包括：已计算、未计算。

②分类查看数据：对于所有的数据可以根据时间、风控模型种类进行分类查询，时间可以查看本日内，7天内，一个月内的数据，风控模型种类可以选择个人授信或企业授信公式。数据列表的排序方式可以根据申请时间、风控模型种类、申请方、计算人姓名（首字母）进行排序。

3）计算节点管理功能

①实时任务量监控：曲线图显示一天之中每个时刻的计算量。

②平台任务量统计：柱状图显示本月内每一天的总计算量。统计本日内的计算次数，统计平台总计算量，请求来源个数，当前正在等待的计算量。

③计算模块状态监控：显示正常、繁忙。

④显示当前待计算队列：显示还在等待中未计算的队列，显示请求的基本信息和当前已等待时间。

⑤处理计算异常的请求：等待中未计算的队列，如果等待时间过长，则可以对申请进行重新请求计算。

4）查看平台反馈信息功能

查看反馈：在意见反馈中查看放贷用户及政府端对计算平台进行的反馈。

修改反馈状态：处理反馈后，可对反馈信息进行状态修改，并向放贷用户及政府端发放消息公告。

5）查看和修改密码功能

①在账户信息中查看本账号和账号编码。

②通过修改密码项修改密码。

6） 发送消息通知功能

当反馈被解决，以及平台做变更后，会向各放款用户端或政府管理员端发出通知公告。

3.2.3 流程逻辑

该模块的流程逻辑图如下：

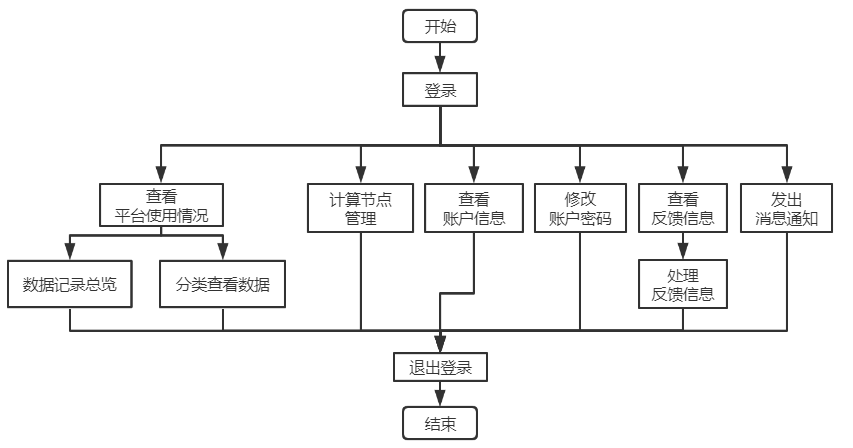


图3-2 平台管理员流程图

* + 1. 文件清单

表3-3 平台管理员网页文件

|  |  |
| --- | --- |
| 文件名称（相对路径） | 说明 |
| /templates/login.html | 登录页面 |
| /templates/admin\_langchao.html | 后台首页页面 |
| /templates/admin\_record.html | 数据记录总览页面 |
| /templates/admin\_recordsort.html | 分类查看数据页面 |
| /templates/admin\_nodemanage.html | 计算节点管理页面 |
| /templates/admin\_feedback.html | 查看反馈信息页面 |
| /templates/admin\_feedbackX.html | 处理反馈信息页面 |
| /templates/admin\_userinfo.html | 查看账户信息页面 |
| /templates/admin\_Editpwd.html | 修改密码页面 |
| /templates/admin\_notice.html | 消息通知页面 |

**3.3 政府管理员模块**

3.3.1描述

政府管理员模块面向各政府部门中参与本项目的工作人员，为政府人员提供数据使用情况的监督以及对风控模型的创建修改删除等。政府管理员创建各类风控模型以供放贷用户选择，当需要对风控模型进行修改时，需提前公告通知放贷用户。

3.3.2功能

1）平台登录功能

政府管理员账号无需注册，当平台与政府达成合作后将由平台方提供。

政府管理员可直接输入账号密码进行登录操作。

2）查看及修改用户个人信息功能

①可在个人信息中查看管理员个人信息。

②可在个人信息中修改个人信息。

③可在修改密码中修改账号密码。

3）意见反馈功能

当对平台功能有意见或建议时，可通过此功能向平台方提出，描述意见主题，意见具体内容等,平台方会酌情采纳。

4）发布公告功能

当需要对风控模型进行操作时（如修改内容和状态、删除），需提前对放贷用户发布公告进行告知，以便其调整使用了该风控模型的贷款产品的信息。

也可发布其他主题的公告。发布公告时可选择公告接受对象。

5）查看风控模型使用记录功能

政府管理员可通过此功能查看各个风控模型的使用情况，如何时何公司采用了何种风控模型计算，申请使用了谁的何种信息等。

6）管理风控模型功能

政府管理员可通过此功能选择修改已有风控模型的状态（启用或是禁止使用），删除风控模型。

也可以创建新的风控模型，风控模型所需信息如下：模型类型、模型所需数据、模型公式、模型描述、模型状态、模型创建人（由系统自动填写）。

创建完成后将由平台方自动完成模型的算法实现。

3.3.3流程逻辑

该模块流程逻辑图如下：

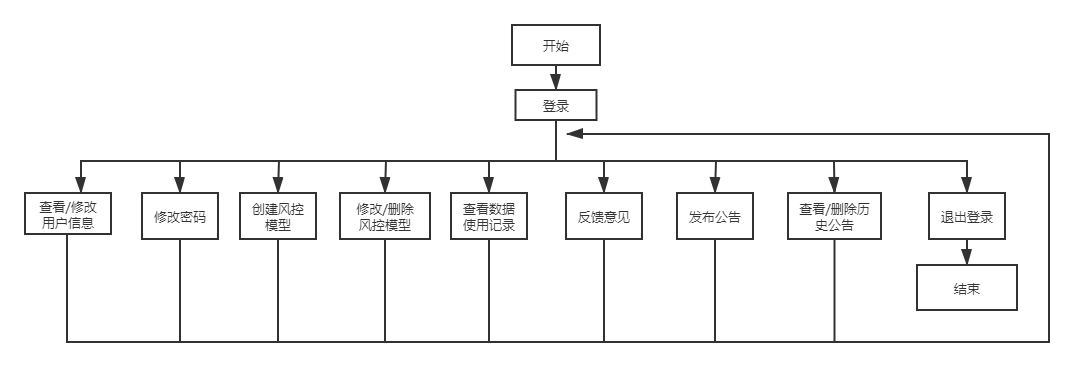


图3-3 政府管理员流程图

3.3.4文件清单

表3-3 政府管理员网页文件

|  |  |
| --- | --- |
| 文件名称（相对路径） | 说明 |
| /templates/login.html | 登录界面 |
| /templates/Zadmin\_index.html | 管理员后台首页 |
| /templates/Zadmin\_info.html | 管理员个人信息界面 |
| /templates/Zadmin\_Edit\_pwd.html | 修改密码界面 |
| /templates/Zadmin\_Feedback.html | 意见反馈界面 |
| /templates/Zadmin\_Model\_Compile.html | 已有风控模型修改界面 |
| /templates/Zadmin\_Model\_New.html | 创建新风控模型界面 |
| /templates/Zadmin\_Model\_View.html | 风控模型及数据申请使用记录界面 |
| /templates/Zadmin\_newsH.html | 历史发布公告界面 |
| /templates/Zadmin\_newsR.html | 发布新公告界面 |

**3.4 贷款用户模块**

3.4.1描述

贷款用户模块面向所有需要贷款的用户，为用户提供与平台合作的各大合法放贷的银行与公司提供的贷款产品。用户注册时需阅读平台协议，用户可以通过平台申请相应的贷款产品，平台得到用户的授权之后会向政府方申请授信计算所需的数据。整个过程安全可靠，不会透露用户任何隐私信息。用户信息对平台保密。用户可在产品详情页面与产品经理获得联系，更加详细具体地了解贷款信息。

3.4.2功能

1）平台登录功能

①贷款用户可通过注册平台账号获取平台服务。

②注册完成的用户可通过输入账号密码登录平台。

2）查看及修改用户个人信息功能

①可在个人信息中查看用户个人信息。

②可在个人信息中修改个人信息。

③可在修改密码中修改账号密码。

3）意见反馈功能

当对平台功能有意见或建议时，可通过此功能向平台方提出，描述意见主题，意见具体内容等,平台方会酌情采纳。

4）查看公告功能

当平台方或政府方或放贷方有消息需要通知用户时，用户能通过该功能知晓最新的信息。

5）浏览贷款产品功能

平台会向用户提供各种贷款产品，用户可通过金额大小或贷款年限筛选自己所需的产品。

6）申请贷款产品功能

用户看到心仪的产品时，可点进产品详情页面具体了解该产品，也可根据提供的产品经理信息与产品经理详细沟通。上传放贷方所需的资料，即可点击申请。

申请完成后，可在我的申请中查看申请状态（是否通过），也可撤销申请。

3.4.3流程逻辑

该模块流程逻辑图如下：

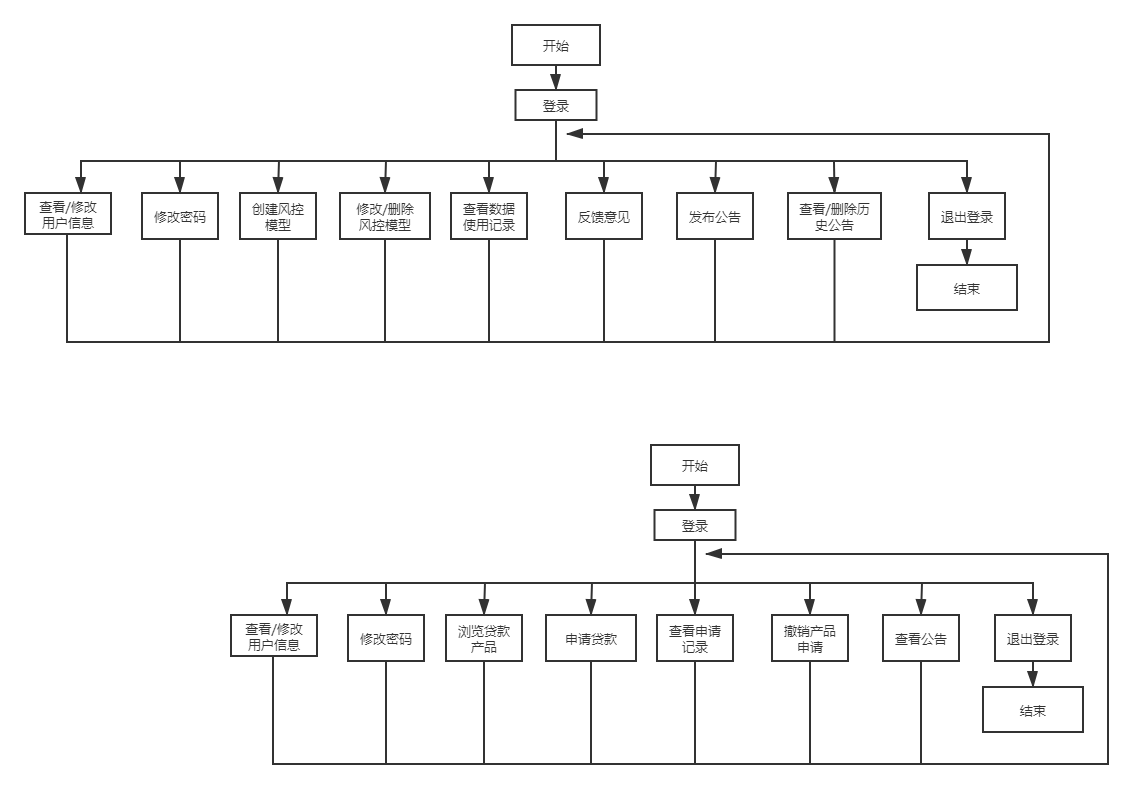


图3-4贷款用户流程图

3.4.4文件清单

表3-4 贷款用户网页文件

|  |  |
| --- | --- |
| 文件名称（相对路径） | 说明 |
| /templates/crt\_user.html | 注册页面 |
| /templates/login.html | 登录界面 |
| /templates/user\_index.html | 贷款用户后台产品页面 |
| /templates/user\_info.html | 贷款用户个人信息界面 |
| /templates/user\_Edit\_pwd.html | 修改密码界面 |
| /templates/user\_Feedback.html | 意见反馈界面 |
| /templates/user\_news.html | 消息查看界面 |
| /templates/user\_productPage.html | 产品详细信息页面 |
| /templates/user\_Application.html | 申请贷款记录页面 |

**3.5 数据模型**

3.5.1用户信息（sys\_user）

主要用于登录，具体用户信息放置在不同角色各自的表中。

表3-5 用户信息表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 属性名 | 数据类型 | 约束 | 含义 | 备注 |
| id | int | 主键 | 用户编号 | 自动生成 |
| email | varchar(45) | 唯一、非空 | 用户邮箱 | 用于登录 |
| password | varchar(45) | 非空 | 用户密码 | 加密存储 |

3.5.2角色信息(sys\_role)

共有4种角色：贷款申请用户，放贷机构，平台管理员以及政府管理员。

表3-6 角色信息表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 属性名 | 数据类型 | 约束 | 含义 | 备注 |
| id | int | 主键 | 角色编号 | 自动生成 |
| name | varchar(45) | 非空 | 角色名 | 用于区分角色权限 |

3.5.3用户-角色对应信息（sys\_user\_role）

存放每个用户与角色的对应关系。

表3-7 用户角色对应表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 属性名 | 数据类型 | 约束 | 含义 | 备注 |
| user\_id | int | 主键、外键 | 用户编号 |  |
| role\_id | int | 主键、外键 | 角色编号 |  |

3.5.4贷款用户信息（commonuser）

表3-8 贷款用户信息表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 属性名 | 数据类型 | 约束 | 含义 | 备注 |
| user\_id | int | 主键、外键 | 用户编号 |  |
| name | varchar(45) | 非空 | 用户姓名 |  |
| identity\_id | varchar(20) | 非空 | 身份证号 |  |
| sex | varchar(6) | 非空,默认‘male’ | 性别 |  |
| card\_id | varchar(20) |  | 银行卡号 | 注册后补充 |
| tel | varchar(15) |  | 电话联系方式 | 注册后补充 |
| addr | varchar(45) |  | 通讯地址 | 注册后补充 |
| estate | varchar(10) |  | 房产信息 | 注册后补充 |

3.5.5贷款机构用户信息（bank）

表3-9 贷款机构用户信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 属性名 | 数据类型 | 约束 | 含义 | 备注 |
| user\_id | int | 主键、外键 | 用户编号 |  |
| name | varchar(45) | 非空 | 负责人姓名 |  |
| tel | varchar(15) | 非空 | 负责人电话 |  |
| identity\_id | varchar(20) | 非空 | 负责人身份证号码 |  |
| sex | varchar(6) | 非空,默认‘male’ | 负责人性别 |  |
| credit\_code | varchar(45) | 非空 | 统一社会信用代码 |  |
| corp\_name | varchar(10) | 非空 | 机构名称 |  |

3.5.6产品信息（product）

放贷机构发布的贷款产品。

表3-10 产品信息表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 属性名 | 数据类型 | 约束 | 含义 | 备注 |
| id | int | 主键 | 产品编号 | 自动生成 |
| kind | varchar(15) | 非空 | 产品类型 |  |
| model | varchar(15) | 非空 | 风控模型类型 |  |
| amount | varchar(15) | 非空 | 贷款额度范围 |  |
| duration | varchar(15) | 非空 | 贷款期限 |  |
| state | varchar(15) | 非空 | 产品状态 | ‘使用中’、‘暂停使用两个状态’ |
| bank\_id | int | 外键、非空 | 所属机构编号 |  |
| age | varchar(15) |  | 适用年龄段 |  |
| payback | varchar(15) |  | 还款方式 |  |
| rate | varchar(10) |  | 利率 |  |
| objective | varchar(30) |  | 目的 |  |
| info | varchar(100) |  | 产品详细信息 |  |
| advantage | varchar(100) |  | 产品优势及推广标语 |  |
| material | varchar(20) |  | 需要客户提交的信息 |  |

3.5.7申请信息（application）

贷款申请用户提交的贷款信息。

表3-11 申请信息表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 属性名 | 数据类型 | 约束 | 含义 | 备注 |
| id | int | 主键 | 申请编号 | 自动生成 |
| model | varchar(15) | 非空 | 模型类型 |  |
| applicant | varchar(10) | 非空 | 申请者姓名 |  |
| product | varchar(45) | 非空 | 产品名 |  |
| amount | varchar(10) | 非空 | 申请额度 |  |
| time | varchar(20) | 非空 | 申请时间 |  |
| ctime | varchar(20) |  | 最新处理时间 |  |
| state | varchar(10) | 非空 | 状态 | ‘未处理’、‘正在计算’、‘已计算’、‘已处理’四个状态 |
| value | int |  | 授信额度 |  |
| comment | varchar(10) |  | 申请结果 |  |
| user\_id | int | 外键，非空 | 申请者编号 |  |
| bank\_id | int | 外键，非空 | 银行编号 |  |

3.5.8反馈信息（feedback）

存放平台用户的反馈。

表3-12 反馈信息表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 属性名 | 数据类型 | 约束 | 含义 | 备注 |
| id | int | 主键 | 反馈编号 | 自动生成 |
| theme | varchar(20) | 默认“空主题” | 主题 |  |
| content | varchar(100) | 非空 | 具体内容 |  |
| time | varchar(20) | 非空 | 反馈日期 |  |
| contact | varchar(20) |  | 联系方式 | ‘未解决’、‘已解决’两个状态 |
| state | varchar(5) | 非空 |  |  |

3.5.9风控模型信息（rc\_model）

存放风控模型具体信息。

表3-13 风控模型信息表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 属性名 | 数据类型 | 约束 | 含义 | 备注 |
| id | int | 主键 | 模型编号 | 自动生成 |
| formula | varchar(80) | 非空 | 公式 |  |
| function | varchar(20) | 非空 | 模型类型 |  |
| var\_num | int | 非空 | 可改参数个数 | 可以提供放贷机构指定不同的系数 |

3.5.10参数信息（param）

用于存放放贷用户指定的系数以及模型默认系数，指定最多5个可改参数。

表3-14 参数信息表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 属性名 | 数据类型 | 约束 | 含义 | 备注 |
| pro\_id | int | 主键 | 产品编号 | 若为0则是默认参数 |
| rc\_id | int | 主键，外键 | 模型编号 |  |
| param1 | decimal(10,2) | 非空 | 系数1 |  |
| param2 | decimal(10,2) |  | 系数2 |  |
| param3 | decimal(10,2) |  | 系数3 |  |
| param4 | decimal(10,2) |  | 系数4 |  |
| param5 | decimal(10,2) |  | 系数5 |  |

3.5.11公告信息（notice）

表3-15 公告信息表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 属性名 | 数据类型 | 约束 | 含义 | 备注 |
| id | int | 主键 | 公告编号 | 自动生成 |
| theme | varchar(20) | 默认“空主题” | 主题 |  |
| content | varchar(100) | 非空 | 具体内容 |  |
| time | varchar(20) | 非空 | 发布日期 |  |
| source | varchar(20) |  | 公告来源 | 区分平台管理员和政府管理员 |

**3.6 数据库接口设计**

数据库操作使用Mybatis持久层框架完成，针对每一张表设计如下数据库操作接口。

3.6.1用户信息（sys\_user）

表3-16 用户信息接口设计表

|  |  |
| --- | --- |
| 包名 | com.example.demo.dao |
| 涉及实体 | SysUser |
| 接口名 | SysUserMapper |
| 方法 | **功能描述** |
| selectById | 根据用户编号查询 |
| selectByEmail | 根据邮箱查询 |
| insert | 插入用户信息 |
| updatePwd | 修改密码 |

3.6.2角色信息(sys\_role)

表3-17 角色信息接口设计表

|  |  |
| --- | --- |
| 包名 | com.example.demo.dao |
| 涉及实体 | SysRole |
| 接口名 | SysRoleMapper |
| 方法 | 功能描述 |
| selectById | 根据角色编号查询 |

3.6.3用户-角色对应信息（sys\_user\_role）

表3-18 用户角色对应信息接口设计表

|  |  |
| --- | --- |
| 包名 | com.example.demo.dao |
| 涉及实体 | SysUserRole |
| 接口名 | SysUserRoleMapper |
| 方法 | 功能描述 |
| listByUserId | 根据用户编号查询 |
| insert | 插入信息 |

3.6.4贷款申请用户信息（commonuser）

表3-19 贷款申请用户信息接口设计表

|  |  |
| --- | --- |
| 包名 | com.example.demo.dao |
| 涉及实体 | CommonUser |
| 接口名 | CommonUserMapper |
| 方法 | 功能描述 |
| selectById | 根据用户编号查询 |
| insert | 插入贷款申请用户信息 |
| update | 更新信息 |

3.6.5放贷机构用户信息（bank）

表3-20 放贷机构用户信息接口设计表

|  |  |
| --- | --- |
| 包名 | com.example.demo.dao |
| 涉及实体 | Bank |
| 接口名 | BankMapper |
| 方法 | 功能描述 |
| selectById | 根据用户编号查询 |
| insert | 插入放贷机构用户用户信息 |
| update | 更新信息 |

3.6.6产品信息（product）

表3-21 产品信息接口设计表

|  |  |
| --- | --- |
| 包名 | com.example.demo.dao |
| 涉及实体 | Product |
| 接口名 | ProductMapper |
| 方法 | 功能描述 |
| select | 根据放贷机构编号查询 |
| selectAll | 查询所有产品 |
| selectbyProId | 根据产品编号查询 |
| insert | 插入产品信息 |
| updateState | 更新产品状态 |

3.6.7申请信息（application）

表3-22 申请信息接口设计表

|  |  |
| --- | --- |
| 包名 | com.example.demo.dao |
| 涉及实体 | Application |
| 接口名 | ApplicationMapper |
| 方法 | 功能描述 |
| select | 根据放贷机构编号查询 |
| selectAll | 查询所有申请 |
| selectByUid | 根据贷款申请用户编号查询 |
| insert | 插入申请信息 |
| updateState | 更新产品状态 |
| updateStateandValueandcTime | 更新状态、授信计算值及处理时间 |
| deletebyId | 根据申请编号删除 |

3.6.8反馈信息（feedback）

表3-23 反馈信息接口设计表

|  |  |
| --- | --- |
| 包名 | com.example.demo.dao |
| 涉及实体 | Feedback |
| 接口名 | FeedbackMapper |
| 方法 | 功能描述 |
| selectAll | 查询所有反馈 |
| selectbyId | 根据编号查询反馈 |
| insert | 插入反馈信息 |
| updateState | 更新反馈状态 |

3.6.9风控模型信息（rc\_model）

表3-24风控模型信息接口设计表

|  |  |
| --- | --- |
| 包名 | com.example.demo.dao |
| 涉及实体 | RcModel |
| 接口名 | RcModelMapper |
| 方法 | 功能描述 |
| selectAll | 查询所有模型 |
| selectbyId | 根据模型编号查询 |
| selectbyFormula | 根据公式查询 |
| selectbyFunction | 根据模型种类（功能）查询 |
| insert | 插入模型 |
| update | 更新模型信息 |

3.6.10参数信息（param）

表3-25 参数信息接口设计表

|  |  |
| --- | --- |
| 包名 | com.example.demo.dao |
| 涉及实体 | Parameter |
| 接口名 | ParameterMapper |
| 方法 | 功能描述 |
| selectbyProId | 根据产品编号查询 |
| selectbyProIdandRcId | 根据产品编号以及模型编号查询 |
| insert | 插入参数信息 |
| update | 更新参数 |

3.6.11公告信息（notice）

表3-26 公告信息接口设计表

|  |  |
| --- | --- |
| 包名 | com.example.demo.dao |
| 涉及实体 | Notice |
| 接口名 | NoticeMapper |
| 方法 | 功能描述 |
| selectAll | 查询所有公告 |
| selectbyId | 根据编号查询公告 |
| insert | 插入公告 |

**第四章 技术方案**

**4.1 CKKS加密运算全同态方案**

4.1.1 CKKS方案简介

目前，主流的全同态加密方案（HE）有DGHV、BGV、Bra12、GSW13几种方案。其中BGV方案是目前最有影响力的方案，也是目前效率最高的方案。以上几种方案均是针对整数的层次型全同态加密方案（FHE），而我们的应用场景需要浮点数的科学运算，便采用了近似数的全同态加密CKKS方案。

CKKS的加密方案的具体构造是基于BGV方案和通过提高密文模的乘法方法。CKKS方案运算效率很高，性能与BGV方案相当。采用了模交换技术与密钥交换技术，这是一种无须启动Boostrapping的层次型全同态加密方案。CKKS方案建立在环-LWE 上，相比其他建立在LWE上的方案参数和效率上更优。

4.1.2 CKKS方案的特色

1）相比以前的近似数的全同态加密方案（HE）需要有指数大的密文模与电路深度，CKKS方案密文模的比特大小增长与电路深度成线性关系。

2）CKKS方案精度几乎是最优的，CKKS方案的计算结果精度损失最多比未加密的浮点数计算结果多一位。

4.1.3 CKKS方案实现流程

CKKS是针对实数加密的全同态方案。通过CKKS算法加密后的密文数据可以进行四则运算，解密后与明文计算结果相符。

整个加密计算的流程图4-1如下所示

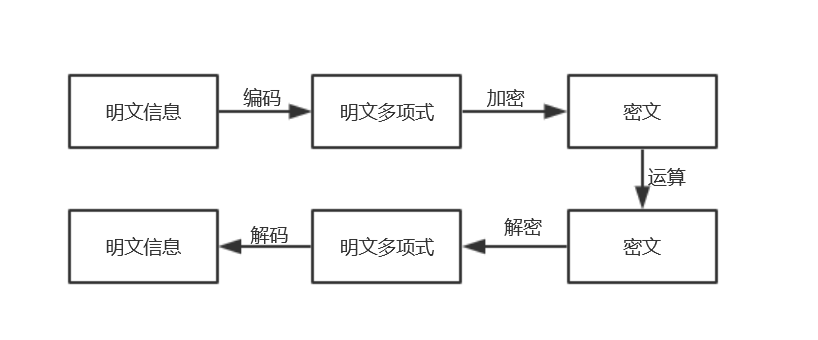


图4-1 CKKS加密计算流程

整个流程如下：

1）设置合适的CKKS的加密参数（CKKS中的乘法导致了规模在密文中成长。需要通过放缩位数保证密文稳定在一定的位数。参数的合理设置尤为重要）

a.选择一个60位素数作为coeff\_modules（系数模块）中的第一个素数。这将在解密时提供最高的精度;

b.选择另一个60位素数作为coeff\_modules的最后一个元素，因为它将被用作特殊素数，并且应该与其他素数中最大的素数一样大;

c.选择中间素数，彼此之间相近。

2）根据设置的加密参数，生成密钥生成算法、加密算法、评估算法和解密算法。

KeyGenerator keygen(context);

auto public\_key = keygen.public\_key();

auto secret\_key = keygen.secret\_key();

auto relin\_keys = keygen.relin\_keys();

Encryptor encryptor(context, public\_key);

Evaluator evaluator(context);

Decryptor decryptor(context, secret\_key);

3）将明文编码成明文多项式。通过encoder.encode()函数进行编码，编码同时需要放缩的尺寸。

4）将明文多项式加密成密文。通过encryptor.encrypt()函数进行加密。

5）对密文进行计算。通过evaluator.add()、evaluator.multiply()对密文实现加法和乘法的运算，减法和除法同理。

a.加法

密文加法之后，密文的位数没有变化，不需要做额外处理。

b.乘法

密文乘法之后，密文的位数产生了变化，需要进行放缩操作，维持密文位数的稳定。乘法之后，首先需要通过evaluator.relinearize\_inplace()函数重线性化，再通过evaluator.rescale\_to\_next\_inplace()函数对密文位数放缩维持稳定。

c.加法乘法混合使用（计算多项式）

加法乘法混合使用的时候，各项虽然进行过放缩处理位数还是有略微差异的，而且每项所使用的加密参数是不同的，而加密的加法和减法要求输入的level相同，并且加密参数(parms\_id)匹配。如果不匹配，Evaluate将抛出异常。最通常的解决方法是设置相同的比例，再匹配相同的参数，即可再对各项的密文进行加法运算。可以通过下列x1\_encrypted.scale() = pow(2.0, 40)设置放缩的尺寸，再通过evaluator.mod\_switch\_to\_inplace()函数将加密参数匹配。

6）将密文计算结果解密成明文多项式。通过decryptor.decrypt()函数进行解密，得到明文多项式。

7）将明文多项式解码成明文信息。通过encoder.decode()进行解码，得到最终的明文计算结果。

4.1.4 方案比较与分析

CKKS方案采用了BGV方案类似的做法。CKKS的参数重点是设置阶梯模的大小，而模的大小与深度L和安全参数 相关，整个电路计算复杂度为，密文的长度为。如果最后额外再进行一次维数约减，可以进一步约减密文的大小，最终密文的长度可以与Regev05方案的密文长度相同，但是不能再进行同态计算了。如果上述层次全同态加密方案，再使用启动技术即可获得“纯”的全同态方案，电路的计算复杂度为 。

目前主流的全同态加密方案有四种:DGHV、BGV、Bra12、GSW13。CKKS方案是基于BGV方案的浮点数全同态方案。我们对四种主流方案的噪声形式、性能和安全性三个方面进行比较，从而可以看出基于BGV方案改造的CKKS方案的优越性。

* 1. 噪声形式对比

四个方案的噪声形式对比如表1所示。对于同样电路深度 L，噪声增长最快的是 DGHV 方案，其密文乘积的噪声等于噪声的乘积。BGV 方案的噪声增长形式是最慢的，这是使用了噪声管理技术后的结果，由于每次密文计算后都用模交换把噪声拉回原来的值，所以噪声在计算过程中几乎保持不变，这是以模改变为代价的，直到最后将模消耗到最小值。Bra12 方案与 GSW13 方案的噪声增长形式很像，这种形式的噪声只要设置合适的参数就能够获得无须启动的层次型全同态加密方案。上述这些方案都可以通过启动技术实现全同态加密。

表4-1 四种方案的噪声形式

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 初始噪声 | 电路深度 | DGHV方案 | BGV方案 | Bra12方案 | GSW13方案 |
|  |  |  |  |  |  |

* 1. 性能对比

四个方案的性能如表2所示。对于启动框架，性能最好的是 BGV 方案，因为这里陈述的 BGV 方案使用的基是环-LWE，本身环-LWE 就 比 LWE 在参数与效率方面更优。Bra12 和GSW13 使用的基本都是 LWE，在启动框架下 GSW13 方案略优于Bra12 方案。在 GSW 方案中 。如果单从性能上比较，BGV 方案性能是最好的。表2中的ω < 2.3727。

表4-2 四种方案的性能比较

|  |  |  |  |
| --- | --- | --- | --- |
| 方案 | 启动 | 模交换 | 近似向量 |
| *DGHV* |  |  |  |
| *BGV* |  |  |  |
| *Bra12* |  |  |  |
| *GSW13* |  |  |  |

* 1. 安全性对比

四个方案的安全性如表 3 所示。除了 DGHV 方案，其他三个方案其安全性都可以基于 LWE 或者环-LWE 问题。在安全指标行中，除了 DGHV 方案，给出的是格上的标准困难问题GapSVP 的近似因子。

表4-3 四种方案的安全性

|  |  |  |
| --- | --- | --- |
| 方案 | 安全基 | 安全指标 |
| DGHV | 近似GCD | 公钥尺寸至少为 |
| BGV | 环-LWE | 量子规约 |
| Bra12 | LWE | 经典规约 |
| GSW13 | LWE | 经典规约 |

**4.2 MAX，MIN函数处理——百万富翁问题**

多方安全计算最初始原型就是姚期智院长提出的百万富翁问题，院长提出的方案采用乱码电路结合不经意传输协议的方案解决百万富翁问题，由于我们在研究算法的过程中将注意力集中在研究加密算法，所有我们应用一种基于Paillier加密算法构造的一套协议解决大小比较问题。

1）Paillier加密算法

Paillier加密系统是一种满足加同态的公钥机密系统，其同态特性表现在加密后可直接对密文进行加法，减法以及数乘运算，其运算结果与明文对应的运算结果一致，其概率特性表现为，对于相同的明文，可以通过不同的加密过程得到不同额密文，从而保证密文的语义安全。

加密过程：

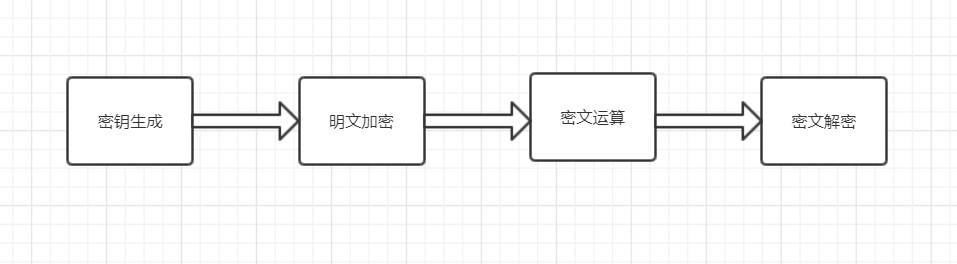


图4-2 Paillier加密流程

以下为具体的算法详解：

密钥生成:随机选取两个较大质数*p*和*q*，计算他们的乘积*N*，以及*p-1*，*q-1*的最小公倍数**,然后随机选取一个整数，且*g*满足

 (4-1)

其中函数，函数用于计算两个数之间的最大公约数，为小于的整数集合，而为中与互质的整数集合。（N,g）作为公钥将明文加密并公开，作为私钥用于密文解密，保留在数据持有方的一端。

加密过程：

随机选取一个整数，对于任意一个明文，利用公钥（N,g）加密后得到对应密文*c*

加密公式：

 (4-2)

根据Paillier加密系统的性质，对于任意密文，当利用同一个公钥加密时只要*m*不同同一个明文加密之后得到的密文就不同，从而保证了密文的予以安全。

解密过程：

利用私钥对密文*c*解密后即可得到对应的明文*m*

解密公式：

 (4-3)

加法同态实现：

同态乘法性质：对于任意两个明文**，，，，对用密文满足

 (4-4)

解密后得到

 (4-5)

由于*N*为很大的质数，所有最终得到的结果就是，之和。

2）大小比较协议

利用上述算法构造一个类似不经意传输的协议。

1. 对保密数据编码

为了在比较大小的监护过程中不透露双方的数据，我们将上方的数据分别混合在一个数据集合向量中进行传输。

假设A,B两方数据分别时*x,y*,分别在双方各随机生成一个数组*a*和*b*，数组要求在一定规模以上，我们以50个混淆数据为例，随机数生成的范围要包括待比较的*x*,*y*。

数组生成后在双方分别按照从小到大的顺序排序各得到一个有序数组。A将*a*传输给B，由于数据混淆在一个集合之中所以保证了A的数据安全。在B端将数组*a*和*b*合并成一个新的有序数组*c*并记录*y*在数组*c*中的下标n。将数组*c*传送会A端，A记录*x*在数组*c*中的下表*m*，将数组编码。

编码规则：

 (4-6)

1. 加密及计算判断大小

按照Paillier加密算法将编码后的数组*c*加密得到密文数组*Ctxt*，并将该密文数组传输给B端。

在B端使用Paillier加密系统的加法规则计算密文数组

计算公式：

 (4-7)

将数据传输到A端解密。

根据h的大小可以得到*x*与*y*的大小关系:

 (4-8)

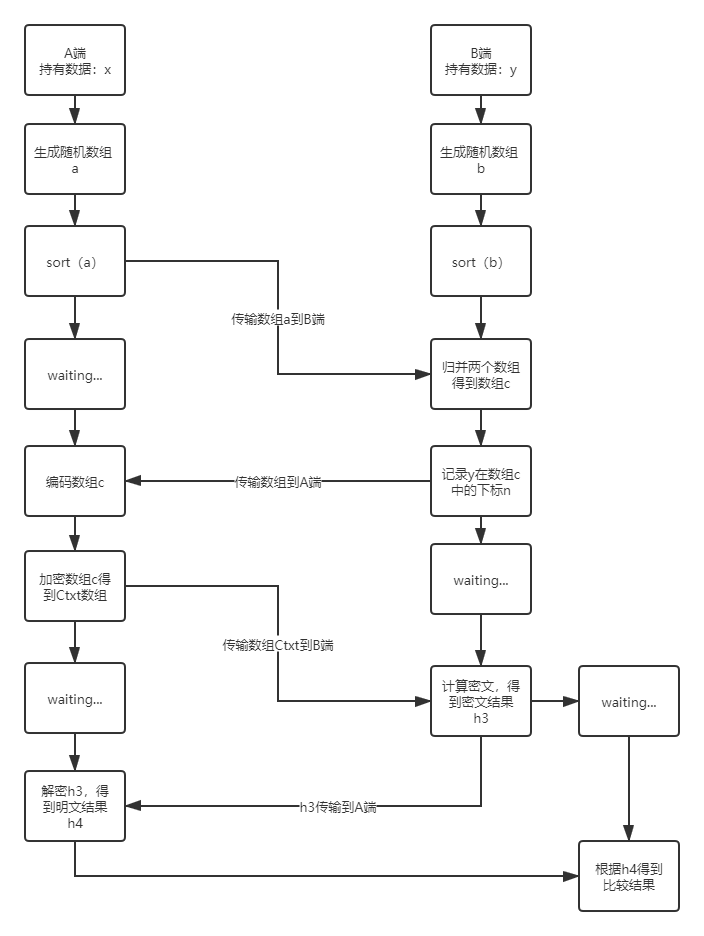


图4-3 协议流程图

**4.3多方安全计算端开发方案**

4.3.1风控模型部署

通过企业端指定已经在浪潮平台安装好的风控模型，将风控模型公式中的常量数据通过公钥加密后和运算符一同导入计算端的编译器中。向政府端（数据提供端）发送请求，在政府数据库中调用该风控模型指定的变量数据，并将数据加密传输到计算端。

4.3.2模型编译

在第一步模型部署过后在计算端相当与是密文数据和运算符组合的中缀表达式，其中密文数据包括政府端的用户数据以及风控模型公式中的常量数据，运算符包括：加，减，乘，除，括号以及MAX，MIN。通过中缀表达式求值原则处理公式中的优先级，按照各运算符优先级的顺序调用数据以及对应的方法进行计算。

其中加减乘除运算符的处理方法直接调用CKKS库中对应密文运算符的计算方法，详见5.1。MAX，MIN函数的处理方法调用大小比较协议进行政府端与计算端的交互，计算端根据政府端返回的信号执行相应处理，详见5.2。

4.3.3结果处理

在第二部模型编译后得到密文的计算结果，将密文计算结果传输到政府端通过私钥解密得到明文结果，政府端将明文数据传输到用户端。到此用户端得到请求的结果。

**4.4政府端及计算端部署**

我们整个系统一共三个服务器，负责存储个人隐私数据以及数据加密的政府端服务器，负责加密计算以及中间数据交互的计算端服务器，以及负责平台管理，企业个人用户管理的web服务器。

政府端服务器部署：

政府端服务服务器一共两个任务，用户数据库查询，以及数据加密。政府端主线程启动后监听4600端口，待计算端接入后，启动socket通信线程与计算端形成TCP连接。政府端会先接收到启动本次线程的用户ID，然后线程根据计算端发送的指令提供对应服务。

表4-4 政府端指令集

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 指令 | 参数 | 返回值 | 功能 | 注释 |
| J | 用户属性A | 对应属性的密文 | 查询数据库，将该用户属性A的值通过CKKS算法加密后发送到计算端 | 也用于检查该用户ID，属性是否在数据库中真实存在 |
| P | 任意实数 | 返回密文 | 将计算端发送来的实数加密，返回密文给计算端 |  |
| G | 数据密文 | 返回大小比较结果 | 多方大小比较协议 |  |
| X | 两个数据密文 | 返回大小比较结果 | 两个密文的大小比较，在政府端将这两个密文解密成明文后比较大小，只返回大小比较结果。 |  |
| N | 数据密文 | 返回明文数据 | 密文解密 | 政府端限制该功能，该功能只用于解密最终密文结果，当该功能执行完毕后政府端主动结束本次连接 |

指令J流程：

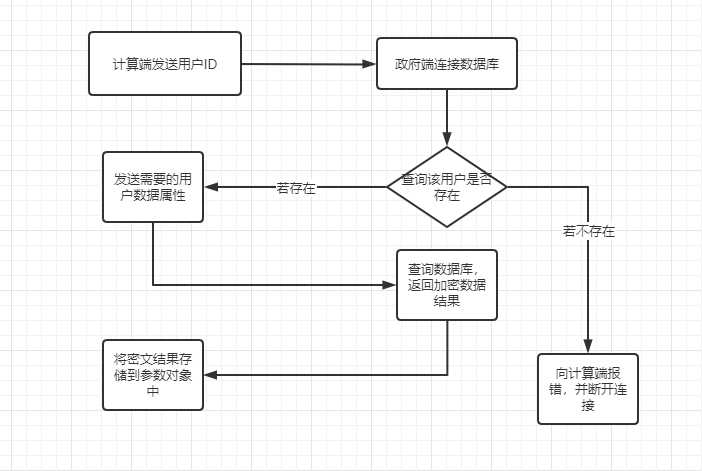


图4-4 指令J流程

政府端服务器主要通过以上指令即实现加密服务。

计算端部署：

计算端服务器以及web服务器全部部署在浪潮方，但是由于后端平台使用java语言编程，计算端加密算法库采用C++实现，虽然我们可以使用java语言封装接口调用底层C++加密库，但是为了保证加密算法的高效性，我们采用将计算端与后端平台分离，使用socket通信联通后端平台与计算端，后端平台负责所有的任务管理，权限管理以及数据仓库管理，计算端只负责加密计算以及与政府端的数据通信。

计算端有两种计算模式，模型模式以及通用计算器模式。

对于较复杂或追求性能稳定的风控模型，可以直接与浪潮合作专门为风控模型设计一套加密程序安装在计算端中，只需要在银行前端更改风控模型公式中参数即可，在用户调用时也只需要存数据库中将公式中需要的参数发送到计算端计算即可。

我们利用模式一为赛题提供的公式设计了一套专门的加密程序。

公式原式：*Math.max(Math.min(Math.max(A \* 0.8，B \* 15) \* 10，150000)，50000)。*将公式中的几个参数改为变量形式param\_1,param\_2,param\_3,param\_4,param\_5后加密程序计算的式子即为:*Math.max(Math.min(Math.max(A \* param\_1，B \* param\_2) \* param\_3，param\_4)，param\_5)*其中A，B在计算端中自动转换为实际用户属性。web端需要将这五个参数的实际值与用户ID发送到计算端。

而通用计算器模式向计算端中发送整个风控模型公式，计算端自动识别公式中的运算符，运算符的优先级以及其中的参数等。此类风控模型数据直接保存在银行账户下的数据库中，包括风控模型公式，公式中的参数以及公式中的用户数据属性。

程序启动时与政府端服务器相似，计算端服务器启动主进程监听8866端口，待web后端发起计算请求后，启动计算端线程开始任务。Web端发起请求时会通知计算端启动对应模式。对于第一种模式，计算端将参数输入到参数变量中并联通政府端通信，开始计算。对于第二种模式，计算端第一步处理传入的参数。计算端封装专门的参数类存储参数。对于数值型参数设定参数类中的标识符为0，代表不用加密可以直接使用，并将参数名和数值存入参数类对象中，对于用户属性数据则设定标识符为1，表示该数据需要加密后使用，在此步只存储参数名，等待政府端加密后再存储数据。

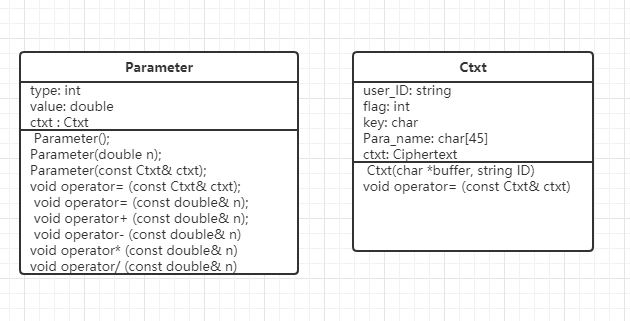


图4-5 参数类，密文类

第二步连通政府端遍历参数表，将需要加密的对象加密。先发送Ctxt类中的用户ID，之后的参数只需要参数名即可。计算端将返回的密文值存储到参数对象中，等待计算过程中查找。

第三步处理公式，将max函数和min函数转换为*@*和*$*方便符号读取以及运算符优先级处理。计算端中内嵌中缀表达式算法用于识别输入的公式，对于运算符通过中缀表达式自动识别运算符优先级，运算符计算调用对应密文计算函数计算。对于识别到的参数则取参数表中查找对应参数名的数值。当整个计算端完成计算后，将密文结果发送给政府端解密，此时与政府端的通信结束，然后将明文结果返回给web端，此时与web端的通信结束，该计算线程任务完成，释放资源。

**4.5加密方案性能及安全性分析**

4.5.1 CKKS加密方案

CKKS的加密方案的具体构造是基于BGV方案和通过提高密文模的乘法方法。BGV 方案是目前最有影响力的方案，也是目前效率最高的方案。BGV 方案采用模交换技术与密钥交换技术，是一种无须启动的层次型全同态加密方案。BGV 方案既可以建立在 LWE 上，也可以建立在环-LWE 上，环-LWE 上的全同态加密方案比 LWE 上的方案效率要高。我们采用的CKKS方案便是建立在环-LWE 上的全同态加密方案

1）性能分析

CKKS方案采用了BGV方案类似的做法。CKKS的参数重点是设置阶梯模的大小，而模的大小与深度L和安全参数 相关，整个电路计算复杂度为，密文的长度为。如果最后额外再进行一次维数约减，可以进一步约减密文的大小，最终密文的长度可以与Regev05方案的密文长度相同，但是不能再进行同态计算了。如果上述层次全同态加密方案，再使用启动技术即可获得“纯”的全同态方案，电路的计算复杂度为 。

2）安全性证明

其安全性建立在理想格上的最短向量(SVP)问题，该问题可以量子规约到R-LWE问题。近似因子为。

4.5.2大小比较协议

我们的大小比较协议需要通过多次通信来完成密文数据的比较。

1）性能分析

本协议是基于CKKS全同态加密算法来解决max、min的计算问题。一次大小比较需要通过3次通信进行，并结合CKKS编码解码自身的运算次数，可得到最终的计算复杂度。

2）安全性证明

安全性以CKKS同态加密算法的安全性为基础，在半诚实模型下，大小比较协议是安全的。

证明过程如下：我们通过构造两个模拟器 S1，S2来证明我们协议的安全性

1. S1接受输入，根据的值构造,使得*C(x，y')=C(x，y)*，用 *x*，*y'*进行模拟． 首先按照协议构造向量*A=(a1，a2，…am ).*
2. 加密向量 A 得到*E( A) = ( E( a1 )，E( a2 )，…E( am ) ).*
3. 选择一个随机数，作如下计算

(4-9)

解密*E( v') 得到v'.*

1. 在本协议中*．*令*．*因为，CKKS 同态加密算法是语义安全的，则*v = v'*，*≡ .*

所以可以构造出以下式子成立

(4-10)

(4-11)

因此可以证明比较协议的安全性，此多方计算是保密的。

**4.6前端设计方案**

4.6.1前端设计原则

1、功能完整，结构清晰，可以实现该平台的所有功能，以及实现不同角色的使用者的功能。

2、结构清晰、导航方便，充分利用导航栏，尽量将所有的导航都安排在一个分层格式中，方便显示应用内的当前位置。

3、突出首要任务，不需要在屏幕上添加任何冗余的东西，尽量做到简洁，突出首要功能。

4.6.2前端设计方案

1）贷款用户端网页

贷款用户端是贷款用户申请企业贷款产品的平台。放贷企业用户注册账号、登录后，进入功能界面。分为查看产品、已有申请、用户信息、意见反馈四个功能子页面。

2）放贷用户端网页

放款用户端是银行等放贷企业用户管理贷款用户申请及企业产品的可视化平台。放贷企业用户注册账号、登录后，进入功能界面。分为申请管理、产品管理、用户信息、意见反馈四个功能子页面。

3）政府管理员端网页

政府管理员端是政府管理员管理风控模型及查看数据记录的平台。政府人员输入账户和密码登录后，进入功能页面。分为风控模型管理、消息公告、管理员信息、意见反馈四个功能子页面。风控模型管理分为风控模型使用记录、编辑已有风控模型和新增风控模型三个子项。

4）平台管理员端网页

平台管理员端是计算品台管理员查看平台数据记录的可视化平台。平台管理人员输入账户和密码登录后，进入功能页面。分为平台使用情况、计算节点管理、平台反馈信息、账户信息四个功能子页面。平台使用情况分为数据记录总览和数据分类查看两个子项。

4.6.3部分页面设计展示

1）登录界面

在此界面可进行登录操作，并有主页、注册以及忘记密码页面的链接



图4-6 登录界面

2）用户注册界面



图4-7 贷款用户注册界面



图4-8 放贷企业注册界面

3）放贷企业用户

首页可以查看近期申请信息和累计的贷款相关信息



图4-9 放贷企业首页

处理申请流程：待处理申请🡪申请计算🡪根据授信结果和材料(点击申请人姓名可以打开申请人信息页面并下载文件)同意/拒绝申请，如图4-10、图4-11、图4-12所示

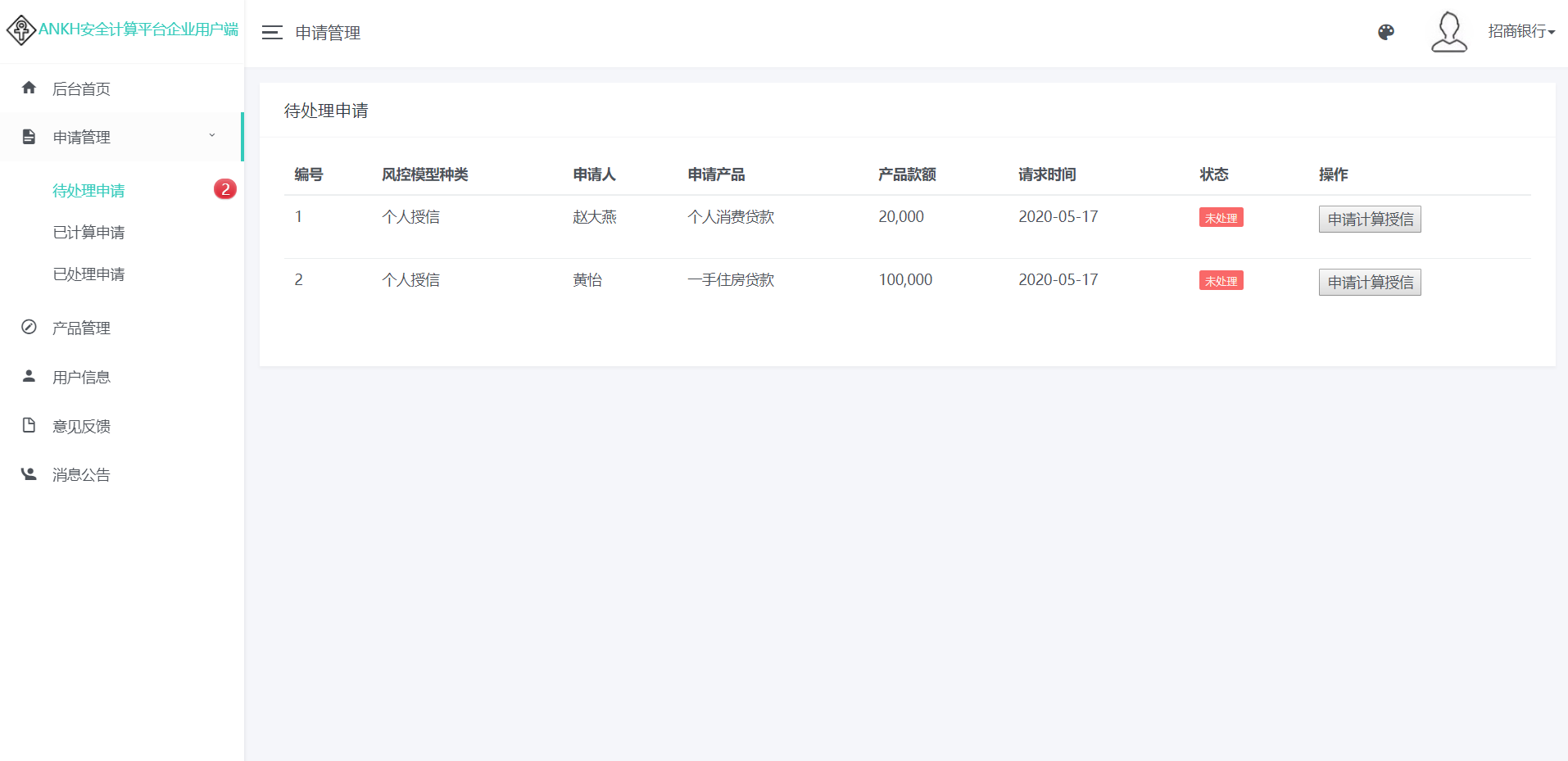


图4-10 待处理申请页面

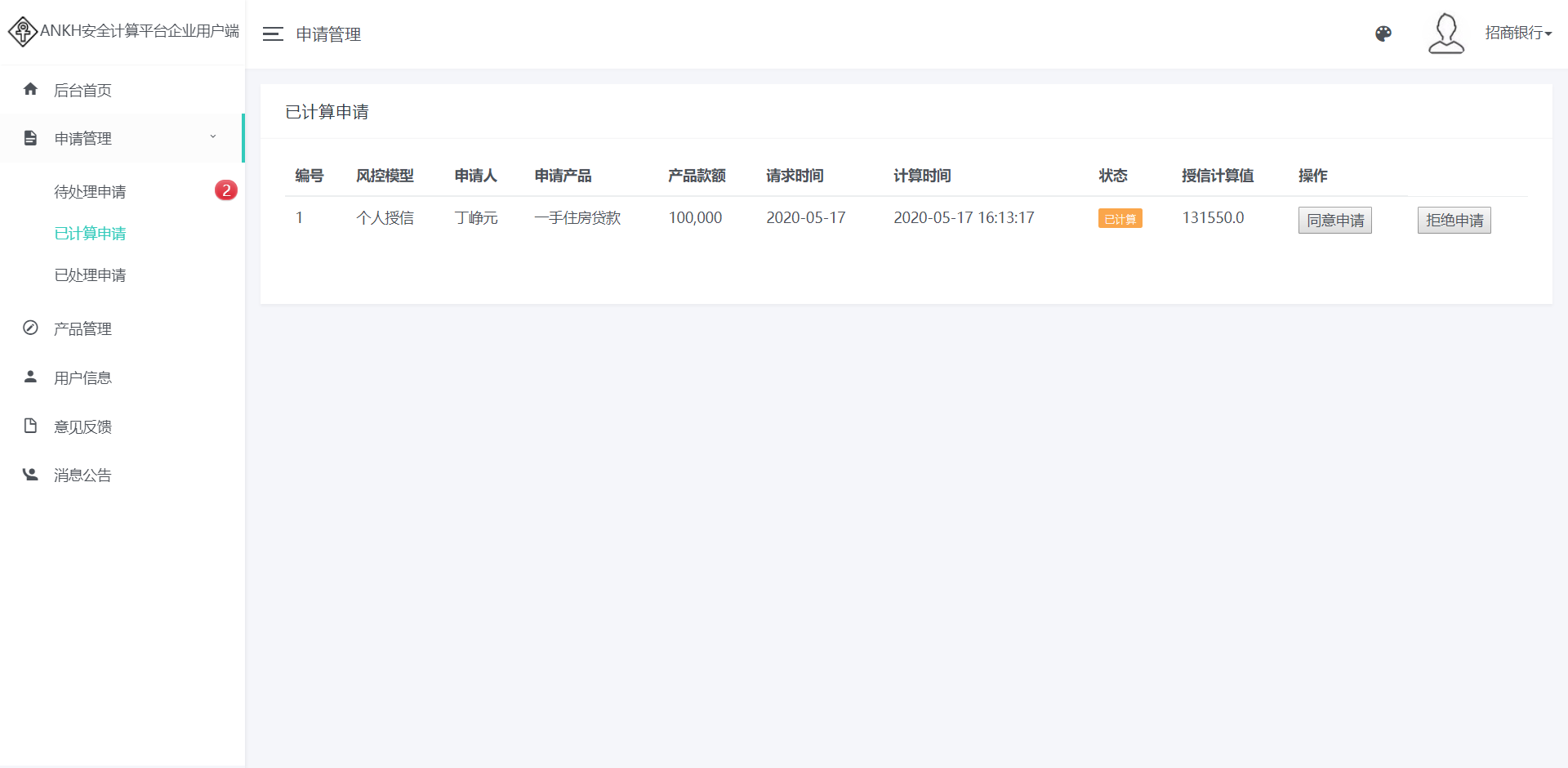


图4-11 已计算申请页面

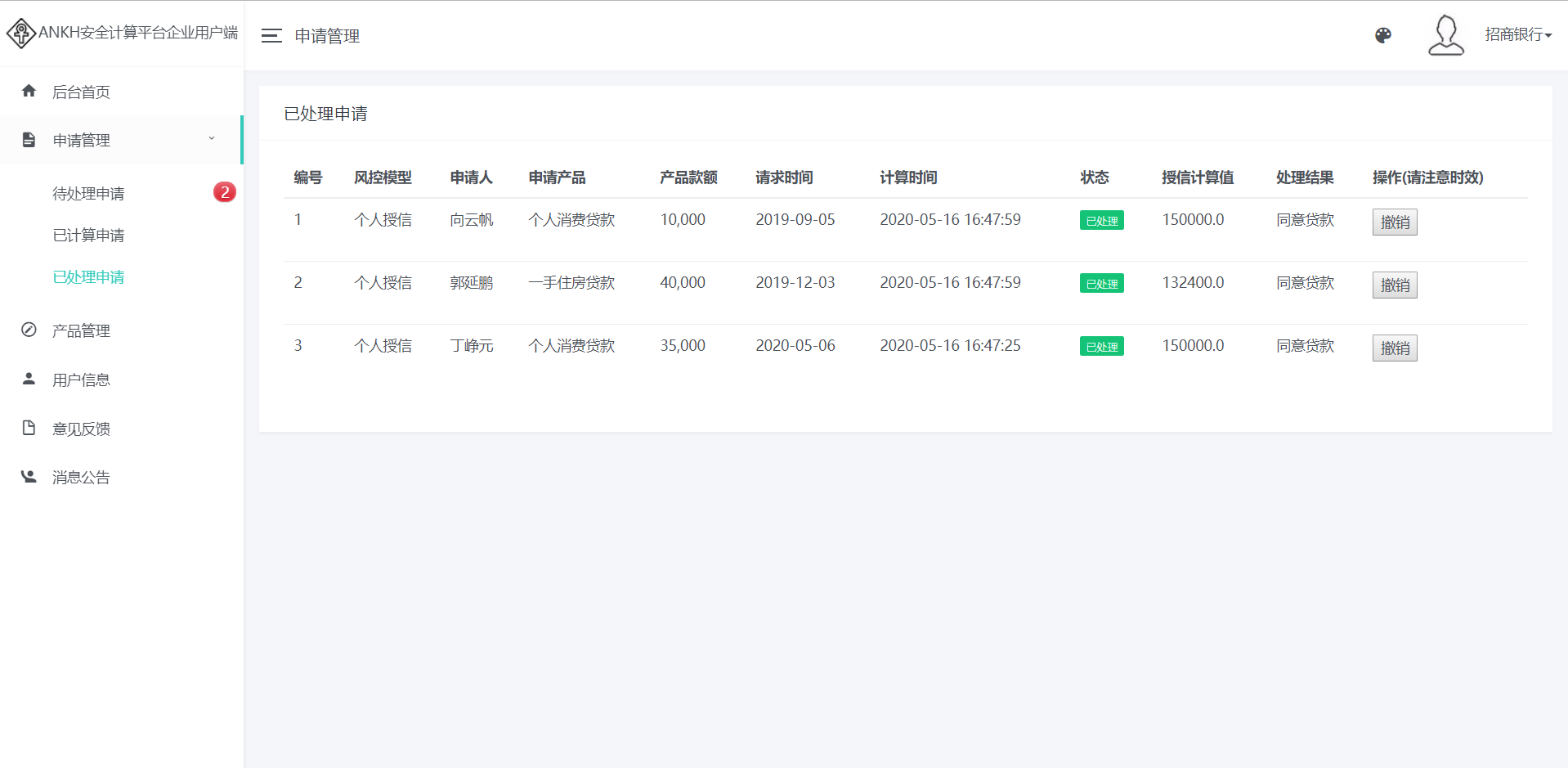


图4-12 已处理申请页面



图4-13 产品管理页面



图4-14 消息公告页面

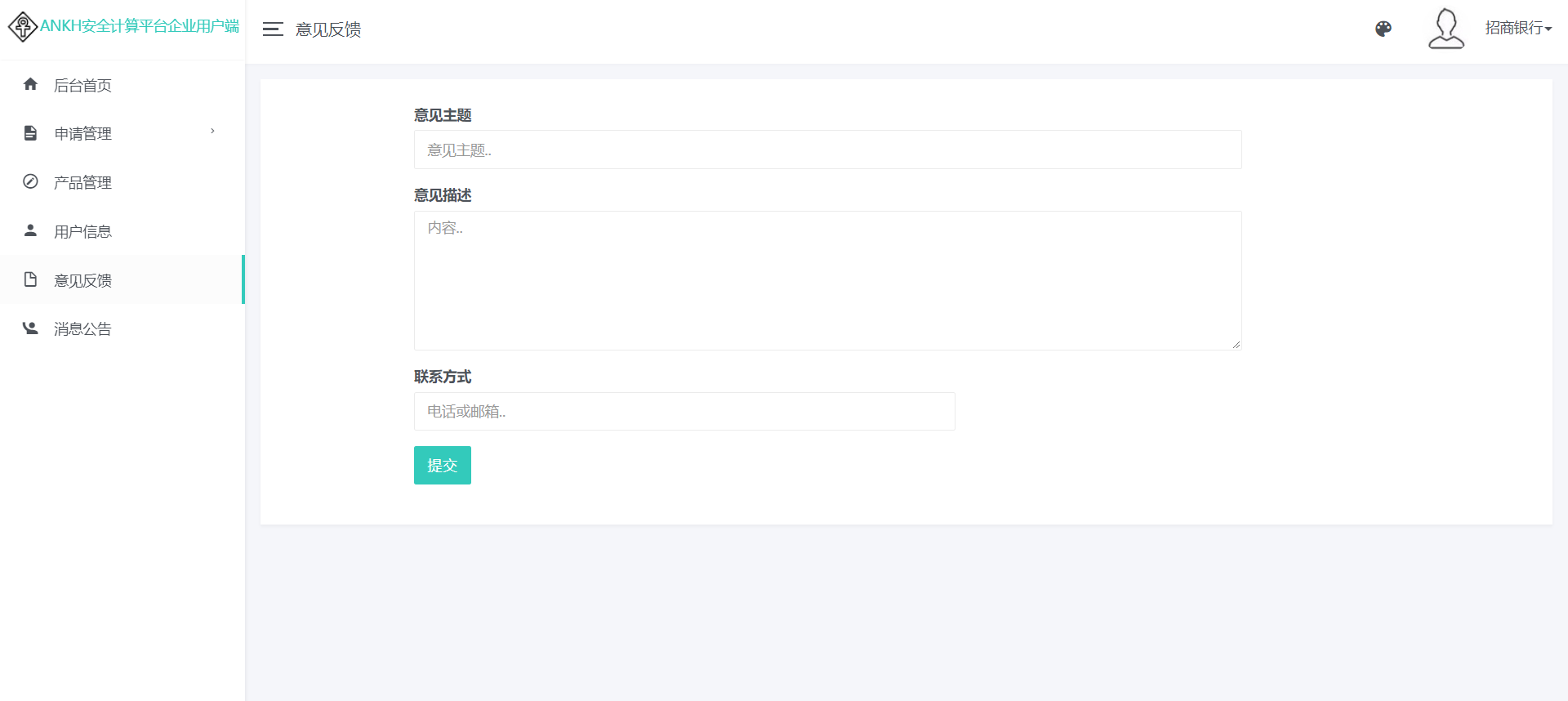


图4-15反馈页面

4）贷款申请用户

贷款申请流程：选择产品🡪输入贷款金额、提交材料🡪确认申请信息，如图4-16、图4-17、图4-18所示

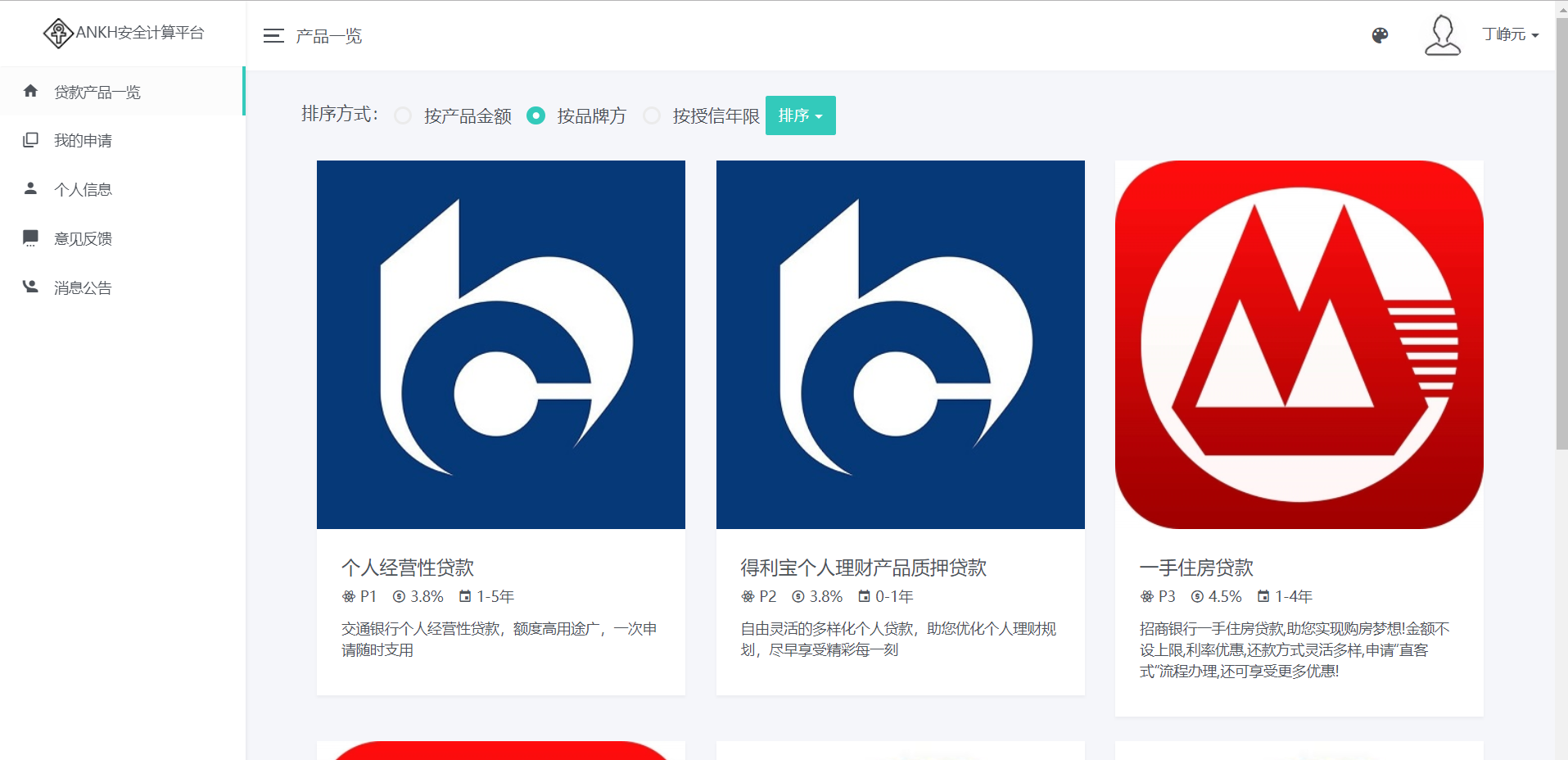


图4-16 贷款产品总览页面



图4-17 产品详情页面

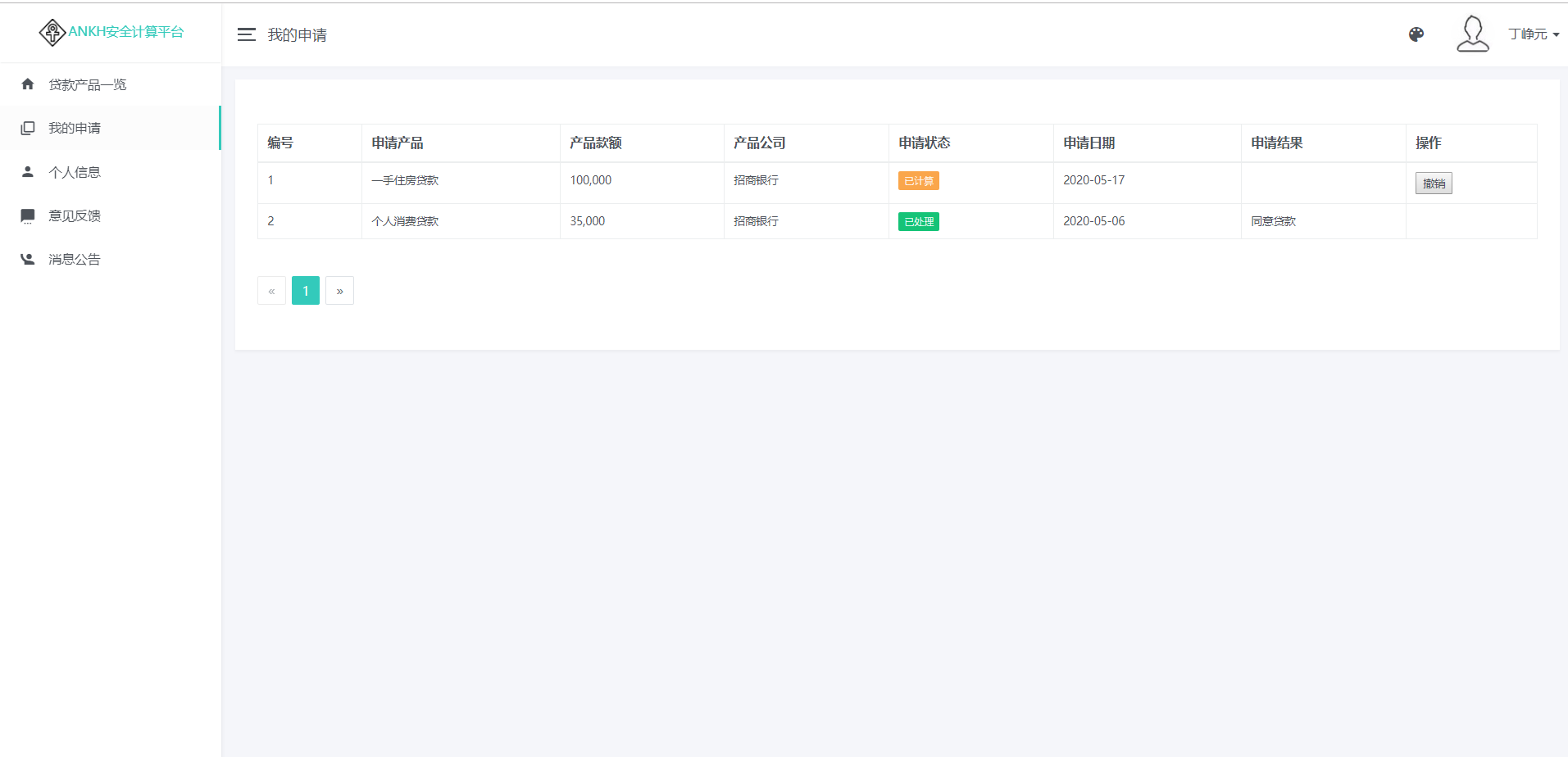


图4-18 申请总览页面

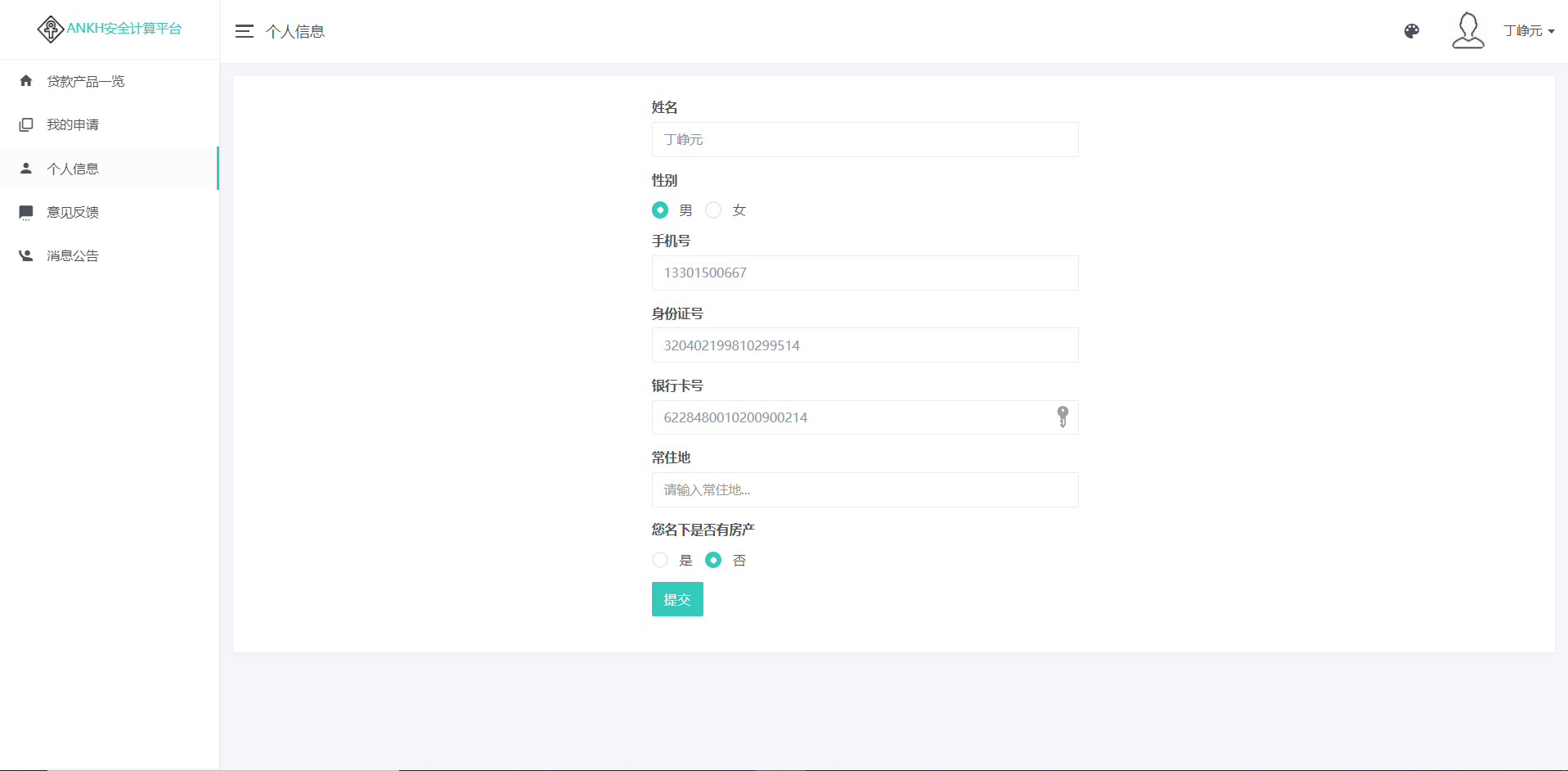


图4-19 个人信息修改

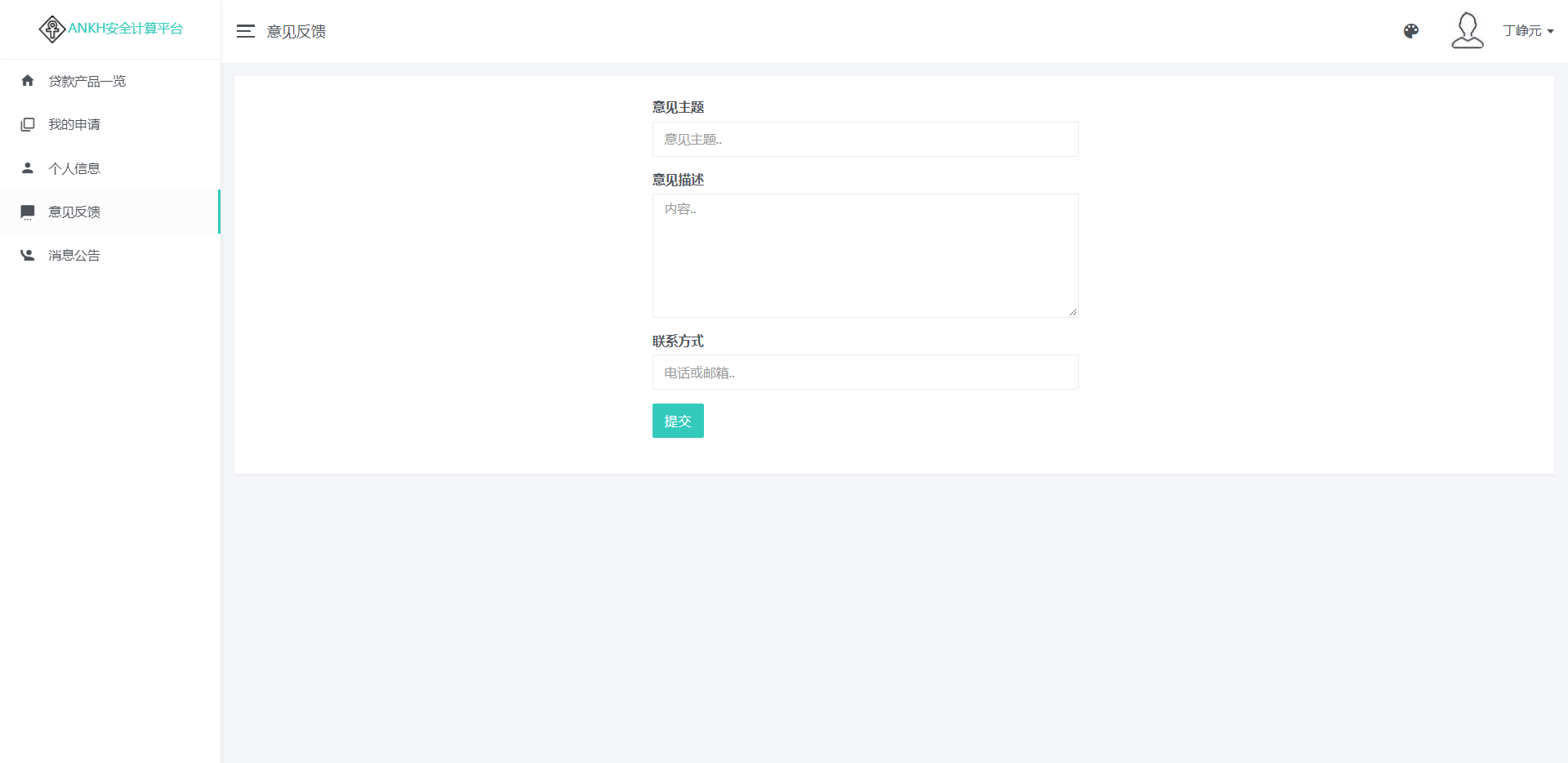


图4-20 意见反馈页面

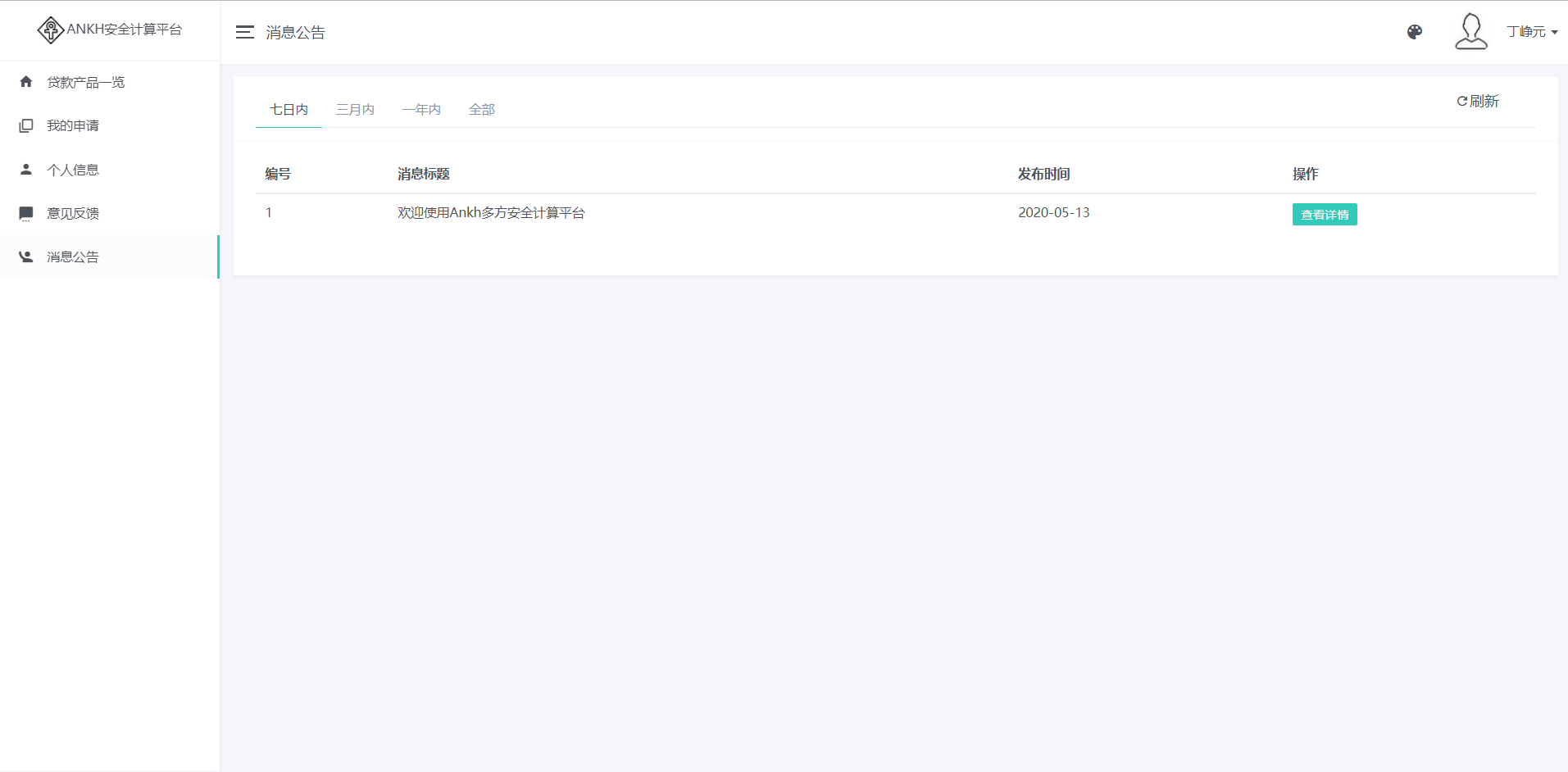


图4-21消息公告页面

5）平台管理员

主要对计算平台使用情况进行总览和可视化显示以及对反馈信息的处理



图4-22 平台使用情况页面

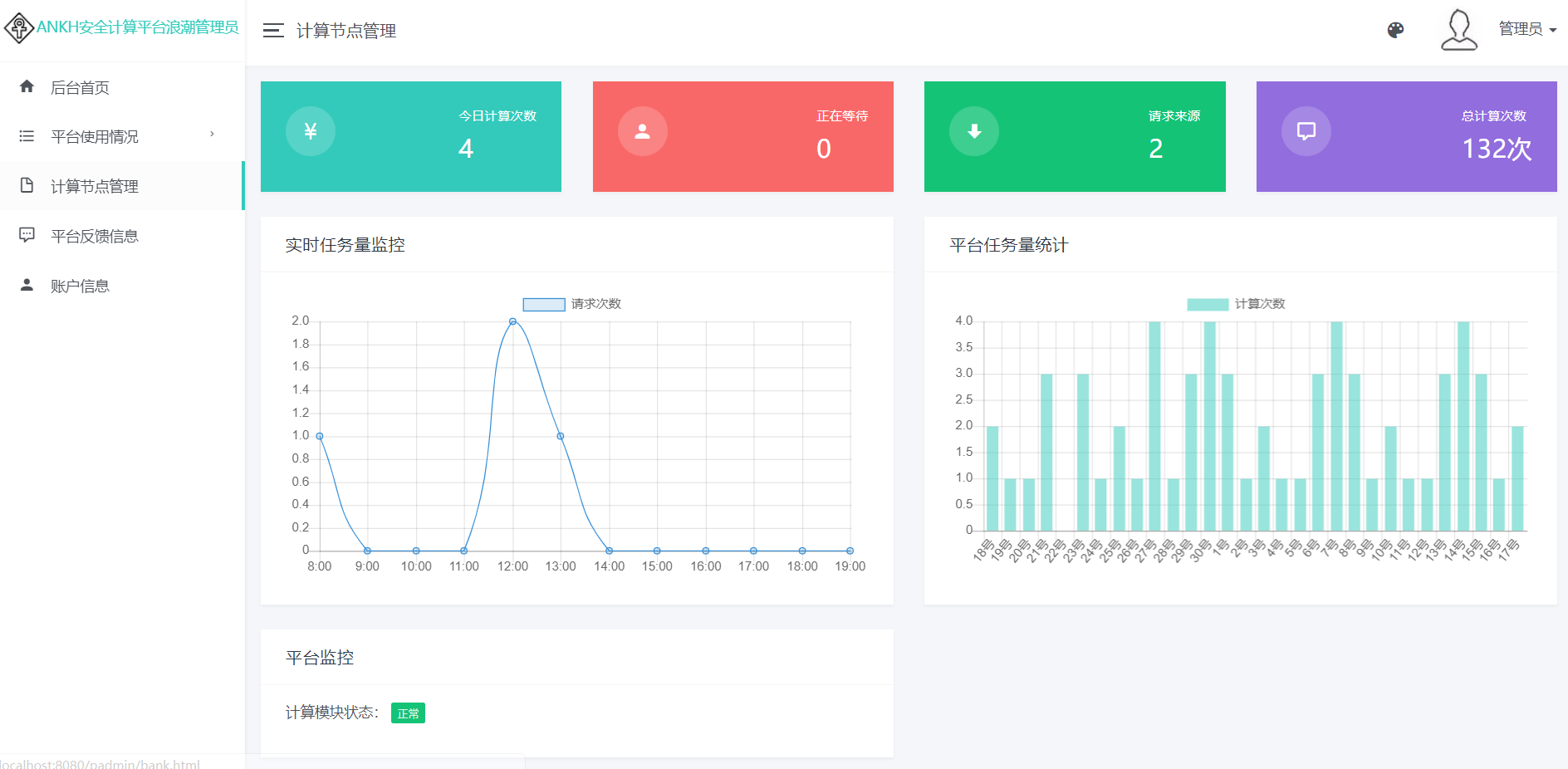


图4-23 计算节点管理页面

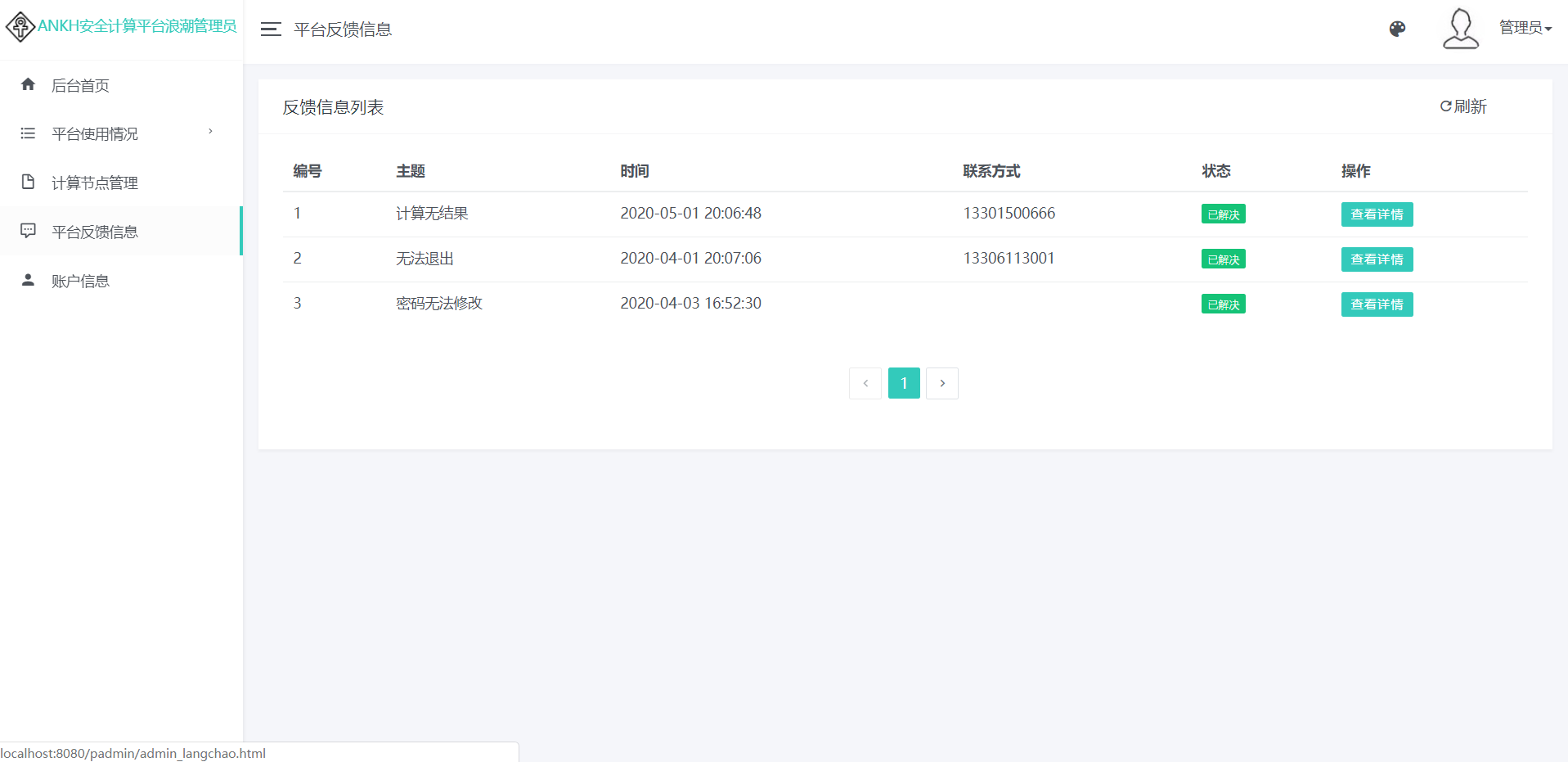


图4-24 平台反馈处理页面

6）政府管理员

侧重对政府数据使用的监控、对风控模型的管理以及消息发布



图4-25 使用情况总览页面

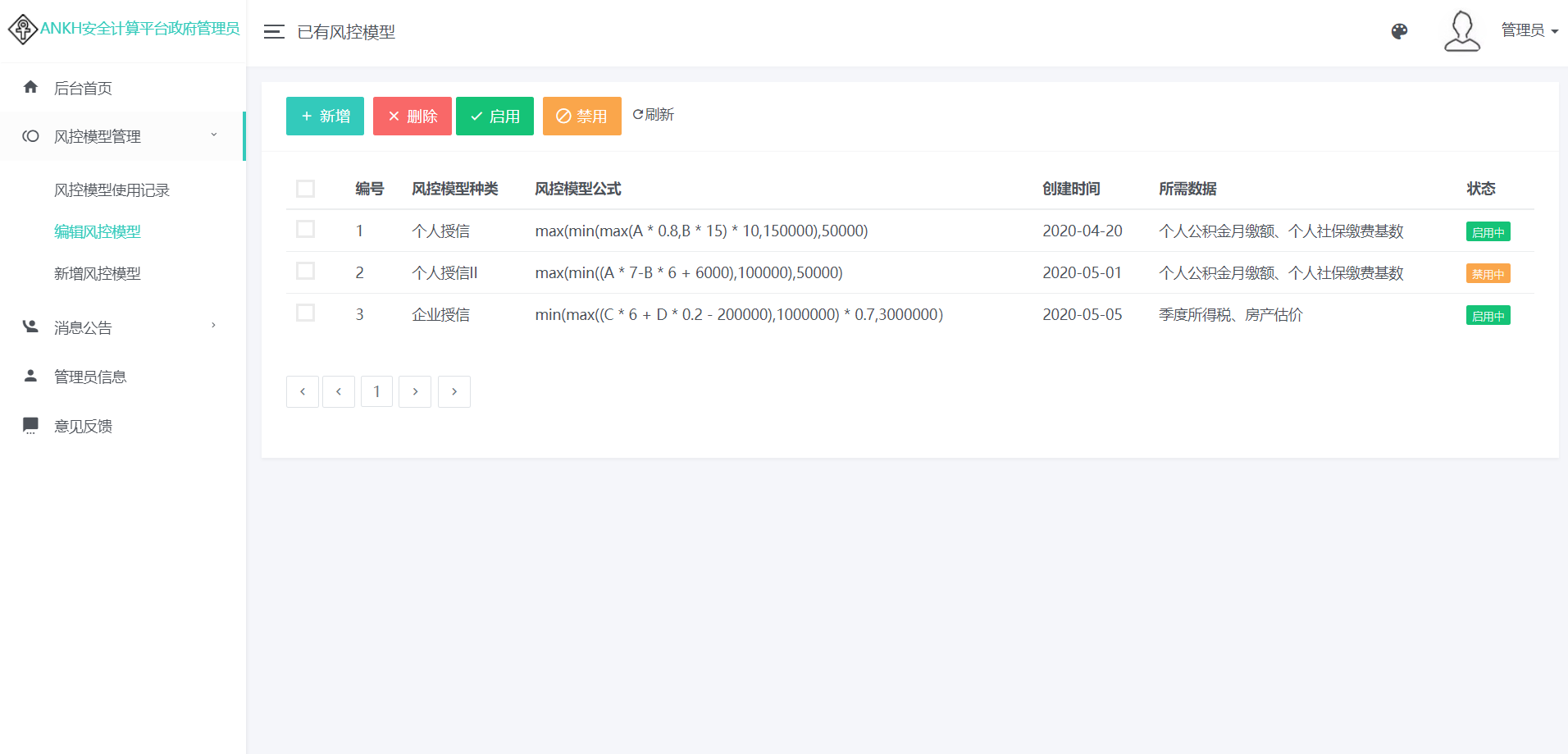


图4-26已有风控模型管理页面



图4-27 添加风控模型页面

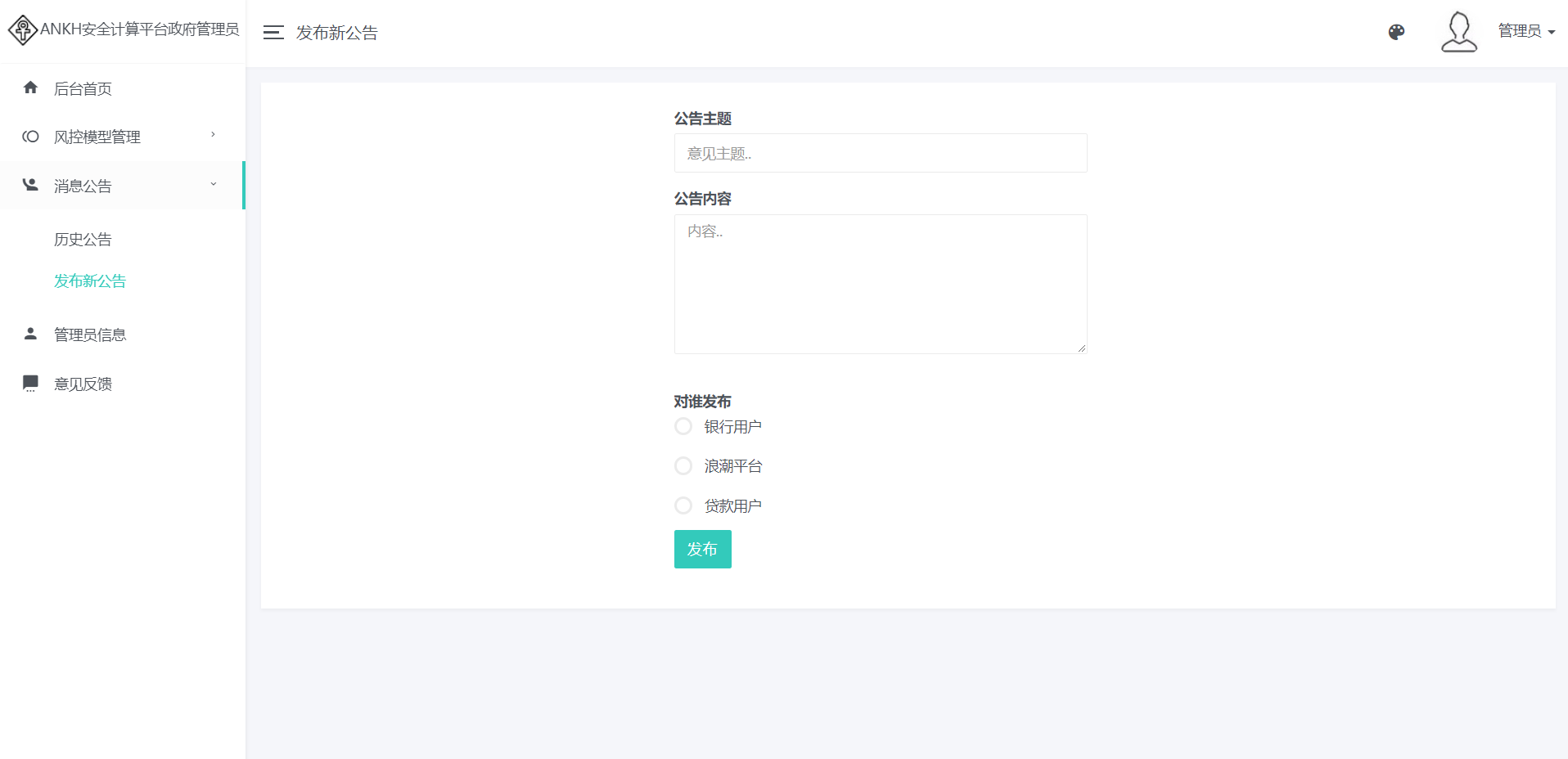


图4-28 消息发布页面

**第五章 组织管理**

**5.1 组织结构**

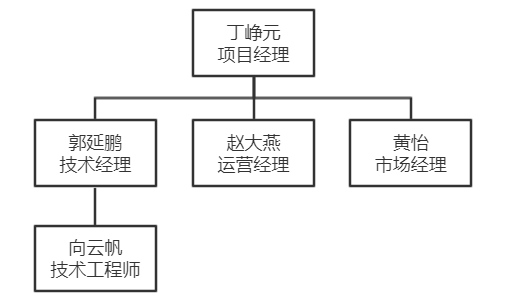


图5-1 项目组织机构

**5.2 角色与职责**

表5-1 团队分工表

|  |  |  |
| --- | --- | --- |
| 成员 | 岗位 | 职责介绍 |
| 丁峥元 | 项目经理 | 1、组织和协调团队，进行资源配置；  2、确定项目整体设计方案、商业计划，统筹各项计划；  3、监督各部门落实公司各项计划；  4、项目质量控制，风险监控，成本控制，项目最终评估；  5、对技术经理、客户关系经理和运营经理进行绩效考核。 |
| 郭延鹏 | 技术经理 | 1、制定并实施公司技术发展规划，制定技术标准和规范；  2、负责设计项目整体方案，技术可行性评估和技术决策；  3、负责系统开发，开发任务的分配，监督落实技术方案 并解决技术难题；  4、对程序员进行指导、培训，并进行绩效考核。 |
| 黄怡 | 市场经理 | 1、负责与客户沟通，引导、整理、发掘客户的业务需求；  2、构建公司良好的文化氛围和积极向上的精神面貌；  3、负责产品的商业运作，制定落实商业方案和商业决策；  4、对商业运作参与人员进行绩效考核。 |
| 赵大燕 | 运营经理 | 1、负责公司资金运作管理、日常财务管理与分析、资本运作、筹资方略、对外合作谈判等；  2、负责公司财务管理及内部控制，根据公司业务发展的计划完成年度财务预算，并跟踪其执行情况；  3、制定、维护、改进公司财务管理程序和政策，以满足 控制风险的要求，如：改进应收账款、应付账款、成本 费用、现金、银行存款的业务程序等；  4、负责编制及组织实施财务预算报告、月/季/年度财务 报告，完成上级交给的其他日常事务性工作。 |
| 向云帆 | 项目工程师 | 1、对技术经理负责，软件项目的详细设计、编码和内部 测试的组织实施，系统分析工作，完成分配项目的实施 和技术支持工作。  2、参与需求调研、技术可行性分析和需求分析；  3、编写系统开发过程中的技术文档和《用户手册》；  4、参与软件首次安装调试、数据割接和项目测试；  5、负责项目的质量保证工作；  6、向技术经理及时反馈系统开发问题并提出改进建议。 |

**5.3 协作与沟通**

1） 项目团队内部协作

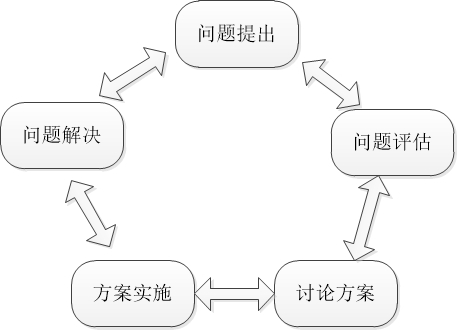


图5-2 团队协作图

2） 项目接口人员

表5-2 项目接口人员

|  |  |  |
| --- | --- | --- |
| 接口名称 | 人员 | 责任 |
| 项目总接口 | 丁峥元 | 负责项目总体计划、实施 |
| 客户接口 | 黄怡 | 负责与客户沟通，记录反映客户提出的需求 |
| 技术总接口 | 郭延鹏、向云帆 | 负责处理技术相关问题 |
| 质量接口 | 黄怡、赵大燕 | 负责系统测试，质量检查、监控 |
| 商务接口 | 丁峥元 | 负责系统推广、成本控制 |

**5.4 项目日程**

表5-3 项目日程表

|  |  |
| --- | --- |
| 时间 | 任务描述 |
| 2019.12.1-12.10 | 需求调研、市场分析、任务计划制定 |
| 2019.12.11-12.30 | 系统方案设计、完成方案概要 |
| 2020.1.1-1.20 | 系统构建、数据库设计、完成项目计划 |
| 2020.1.22-3.4 | 系统基本功能编码，完成基本功能模块 |
| 2020.3.6-3.23 | 系统拓展功能编码，完成系统拓展功能 |
| 2020.3.24-4.15 | 系统优化，完成整套系统，完成最终界面设计 |
| 2020.4.15-5.4 | 系统集成、测试 |
| 2020.5.5-5.20 | 文档完善、ppt、视频制作及完善 |

**5.5 开发模型**

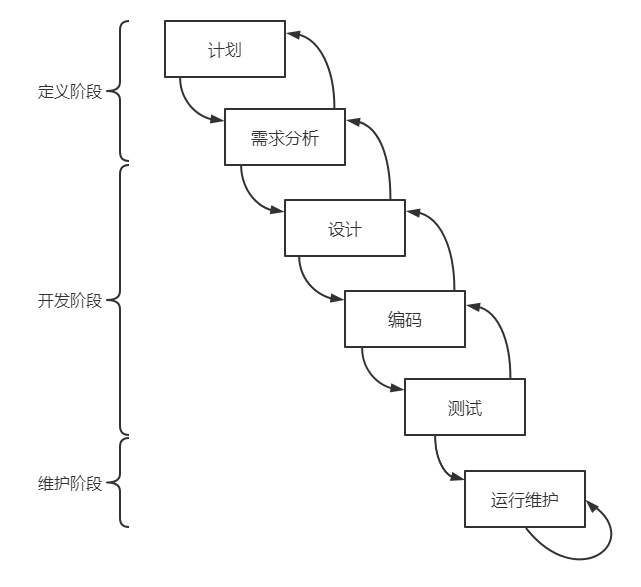


图5-3 瀑布开发模型

**第六章 测试计划**

**6.1简介**

1）目的

为了确保项目的可用性以及可靠性，使得项目能够按质按量地完成，保证项目成品在后期使用以及维护过程中不会出现极其严重的错误，我们编写了此测试计划。本文档对多方数据安全计算平台系统做了总体规划，用于指导多方数据安全计算平台系统的测试工作展开，适用于本项目的所有参与者。

2）背景

项目名称：Ankh多方安全计算平台

分为以下模块：政府数据平台、核心计算端、用户平台、平台数据仓库、管理员平台

开发者：本文档撰写团队

3）范围

表6-1

|  |  |  |  |
| --- | --- | --- | --- |
| 模块 | 子模块 | 是否计划测试[Y/N] | 备注 |
| 政府数据平台 | 加密模块、数据库 | Y |  |
| 核心计算端 | 风控模型，数据交互 | Y |  |
| 用户平台 | 登录、注册、申请 | Y |  |
| 平台数据仓库 | 数据库 | Y |  |
| 管理员平台 | 登录，查看信息 | Y |  |

**6.2 参考资料**

表6-2 参考资料表

|  |  |  |  |
| --- | --- | --- | --- |
| 文档(版本/日期) | 是否创建[Y/N] | 是否评审[Y/N] | 备注 |
| 软件概要设计 | Y | Y |  |
| 软件详细设计 | Y | Y |  |

**6.3 测试安排**

1）测试进度安排

表6-3 进度安排表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试活动 | 计划开始日期 | 计划结束日期 | 测试人员 | 备注 |
| 制定测试计划 | 2020.4.12 | 2020.4.14 | 丁峥元 |  |
| 设计测试用例 | 2020.4.15 | 2020.4.19 | 赵大燕 |  |
| 集成测试 | 2020.4.20 | 2020.4.24 | 黄怡 |  |
| 系统测试 | 2020.4.25 | 2020.4.30 | 郭延鹏 |  |
| 用户验收测试 | 2020.5.1 | 2020.5.5 | 向云帆 |  |

2）测试目标

表6-4 测试目标表

|  |  |  |
| --- | --- | --- |
| 测试目标项 | 通过标准 | 备注 |
| 需求覆盖率 | 100% |  |
| 测试用例执行率 | 100% |  |
| 测试用例通过率 | 100% |  |
| 缺陷修复率 | 95% | 个别遗留问题可等待下个版本跟踪修复 |

**6.4测试资源**

1）人力

表6-5 人力资源表

|  |  |  |
| --- | --- | --- |
| 角色 | 姓名 | 具体职责 |
| 测试管理人员 | 丁峥元 | 测试策划：   1. 测试策略：用多组数据测试计算结果的准确度；用多个不同的账户注册登录进行测试； 2. 测试进度：一周之内完成所有测试； 3. 资源准备：主机、路由器、客户终端； 4. 测试设计：根据需求规格说明书的内容对系统功能进行检验测试。 |
| 主要测试人员 | 郭延鹏 | 测试执行：利用多组数据测试计算结果的准确度和效率。 |
| 参与测试人员 | 赵大燕 | 测试执行：注册登录多个账户，反复测试系统。 |

2）测试环境

CPU: Itel(R) Core(TM) i5-4200M CPU @2.50GHz 2.50GHz

内存：4GB 硬盘：1T

操作系统:Windows 10

应用软件：MySQL IDEA

3）测试工具

禅道测试管理工具。

**6.5测试策略**

1）测试类型

表6-6 测试类型表

|  |  |  |
| --- | --- | --- |
| 测试类型 | 说明 | 备注 |
| 数据和数据库完整测试 | 检查数据库中所有的数据是否均正确 |  |
| 接口测试 | 检查系统与外部系统的接口是否正常 |  |
| 集成测试 | 检查模块组装成系统后是否能正常工作 |  |
| 功能测试 | 根据需求文档、设计文档等检查产品是否正确实现功能 |  |
| 用户界面测试 | 检查界面是否符合规范，是否合理美观 |  |
| 性能测试 | 提取系统性能数据，检查系统是否满足需求中所规定要达到的性能 |  |
| 负载测试 | 检查系统在超出最大预期工作量的情况下是否能正常运行 |  |
| 安全性和访问控制测试 | 检查系统是否达到安全需求，是否存在安全隐患；测试系统控制运行的有效性 |  |
| 安装测试 | 检查系统是否能正确安装，配置等基础数据是否正确 |  |
| 兼容性测试 | 考虑用户端浏览器版本，测试各浏览器版本的兼情况 | IE浏览器8.0以下版本不考虑 |

2）测试阶段

单元测试

单元测试集中检测模块的测试工作，通过模块接口、局部数据结构、重要的执行通路、出错处理通路、便捷条件五个方面对模块进行测试。通常，单元测试主要使用白盒测试技术，而且对多个模块的测试可以并行的执行，主要测试代码语句的正确性，如所有的代码是否都可以跑到，是否有冗余的代码等等。

集成测试

接口测试，主要测试代码块之间的接口，看看数据的传输是否有问题。用集成策略组装程序模块，对系统的接口及集成后的功能进行正确性检测。检查软件单位之间的接口是否正确。

系统测试

黑盒测试，不接触代码，只对整个系统做功能的测试和性能的测试。系统测试主要包括功能测试、界面测试、可靠性测试、易用性测试、性能测试。功能测试主要针对包括功能可用性、功能实现程度（功能流程&业务流程、数据处理&业务数据处理）方面测试。

确认测试

确认测试也称作验收测试，是用户做的测试，目标是验证软件的有效性，根据需求分析阶段产生的需求规格说明书作为软件有效性的标准，也是作为此项测试的基础。

**6.6测试风险和优先级**

表6-7

|  |  |  |
| --- | --- | --- |
| 优先级 | 测试风险描述 | 备注 |
| 1 | 软件需求风险，对需求特性理解有偏差 |  |
| 2 | 代码质量风险，扩展性不足，兼容性差 |  |
| 3 | 测试用例风险，用例设计不完整，用例覆盖率没有做到足够覆盖 |  |

注：数字小的优先级更高。

**6.7 测试标准**

1）测试通过标准

* + - * 版本发布不能遗留1级Bug。考虑特殊情况，容忍概率型1级Bug，可容忍数量为2，浮现率不大于5%。
      * 版本发布不能遗留2级Bug。考虑特殊情况，容忍第三方型2级Bug，可容忍数量为2。
      * 版本带Bug发布，遗留3、4级Bug数不能超过该系统Bug总数的5%。
      * 详细测试用例执行率：100%。
      * 详细测试用例通过率：不低于95%。

2）测试挂起标准及恢复条件

* 如果测试过程中发生致命问题，导致50%用例堵塞无法执行，需要将测试挂起，待导致堵塞的问题被修复后，恢复测试。
* 如果高优先级用例未能100%执行，需要将测试挂起，等导致堵塞的问题被修复并通过回归测试后，恢复侧四。
* 不断修改和版本变更引起部分结果失效，需要将测试挂起，待开发自检确定测试版本，且通过回归测试后，恢复测试。

3）测试验收标准

* + - * 完成所有类型测试
      * 没有影响到用户业务使用的bug
      * Bug数量少于一定数量
      * 功能业务、性能指标符合要求

4）产品上线标准

* + - * 已按照交互文档、需求文档完全实现需求
      * 符合交互文档的交互设计规范、符合视觉要求，已经通过设计评审
      * 允许遗留可能会对用户正常使用造成一定影响的normal级缺陷，但应在发布前告知项目组，并经风险评估一致同意发布后方可发布

**第七章 商业分析**

**7.1 市场背景**

安全多方计算问题由图灵奖得主姚期智于上世纪八十年代首先提出，现在已经成为密码学的一个重要研究方向。安全多方计算旨在解决一组互不信任的参与方之间保护隐私的协同计算问题，为数据需求方提供不泄露原始数据前提下的多方协同计算能力。而该问题模型之所以被广泛关注，是因为在如今大数据、云计算发展迅猛的背景下，能够直接基于密文进行运算、分析，这将在保证数据安全性的前提下极大的提升不同企业、组织之间数据共享合作的效率。传统的加密数据共享只能保证数据在两方间传输的保密性，而对数据的处理只能在对密文解密之后完成，这就导致无法借助云计算平台对数据进行计算，此外，像诸如百万富翁问题这样两方都拥有保密数据，但需要得出两方数据关系的实际问题更是难以解决。随着国内各大企业规模扩展，市场竞争加剧，而效率是企业在市场中制胜的必要。因此一个能拥有良好适应性、安全性、高效率的多方安全计算平台对企业的良好发展是至关重要的。

**7.2 市场分析**

1）多方安全计算平台行业现状

在调查中，我们发现国内多方安全计算平台大多只在理论层面，仅有矩阵元公司在2018年发布了安全计算服务平台JUGO，其使用加密电路和不经意传输作为加密手段实现两方计算。但是使用该平台需要使用其特定的Frutta语言进行布尔电路转化，因此开发人员需要重新学习编程语言。使得其通用性和适应性降低。而我们设计的平台可支持多种计算模型，同时使用常用编程语言Java及C++实现，能够很好的与现有数据库及软件相结合。

2）多方安全计算平台市场容量

如今企业在商业上合作相当频繁，企业之间仅存在互利关系也存在竞争关系，故数据及信息安全在合作中是至关重要的。而在安全利用数据前提下，能够高效使用云计算平台对双方数据进行运算处理将大大提升企业合作的效率，增进运营能力，进而提升营业额，获取更多的利润。因此，多方安全计算平台对于企业来说有着极大的意义

3）市场预测

随着机器学习、大数据以及云计算技术的进一步发展，企业间、政企间合作将愈发频繁，故多方安全计算平台将会成为企业软件体系中不可或缺的一环，特别是那些涉及诸多大数据分析的企业。

我们分析认为在未来，企业对该平台的需求将有大幅提升。由于如今该平台的市场空缺很大，故在对我们平台计算效率的进一步提升后，将有巨大的发展潜力。

**7.3 资源投入**

资源投入主要包括服务器等硬件设施租借预算，开发预算，销售预算以及市场推广预算，详细费用见表7-1

表7-1前期资源投入

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 项目 | 描述 | 费用 |
| 1 | 服务器费用 | 企业级服务器，满足快速处理计算任务。 | 25000元/台 |
| 2 | 服务端开发 | Java工程师开发后端项目。 | 16,000元/月 |
| 3 | UI设计及web开发 | 团队内专业设计师设计网页界面以及公司logo等。 | 12,000元/月 |
| 4 | 多方安全计算算法研究 | 算法工程师研发多方安全计算算法以及同态加密算法。 | 20,000元/月 |
| 5 | 产品销售 | 销售人员月薪 | 7000元/月 |
| 6 | 公司注册资金 |  | 10,000元 |
| 7 | 百度广告 | 打一年广告，出价1元钱，每天有100点击量（“多方安全计算”关键字最低报价是0.6元） | 42,000元/年 |
| 8 | 接待来访客户 | 接待客户一年的总费用 | 15,000元/年 |
| 9 | 产品推广视频 | 与视频制作外包公司合作，交由外包公司做后期处理。 | 5000元 |

由于本项目涉及数据加密，不宜租借阿里云等云端服务器，直接使用公司服务器，能够保证数据保密，计算处理速度更快。本项目至少包括两台服务器，一台用于搭建服务器后端，一台用于处理多方安全计算任务，所以设备预算共50000元。

服务器端开发，web及UI设计师，算法研究开销均为工程师月薪，当前团队规模较小，团队主要成员包括，一名java工程师，两名web兼UI设计师，两名算法工程师，合计80000元/月。暂定产品开发周期为2个月时间，那么开发人员预算为160,000元。

产品上线之后，销售人员开始负责推销产品与接待客户，暂定两名销售人员，销售人员预算为14000元/月，假声接待来访客户预算15000月/年，第一个销售期为10个月，则销售预算共计155000元。

百度广告与推广视频做为公司的广告预算共计52000元。

以上预算共计417000元。

**7.4 SWOT分析**

S（Strength）优势

1） 人员优势

我们的组员都是三年级本科学生，具备一定的专业知识，有较强的学习能力，并且具有极大的创新、创业热情。我们在大学学习中，已经接触到计算机领域前沿领域，并且对创新创业有一定的学习实践经验，具备一定的风险意识，市场意识。此外，组员之间专业相近，文化素质整齐，易于分工合作。

2） 产品优势

我们的平台汲取众长，并有独特的创新之处。系统具有易于操作、安全稳定、扩展和调整灵活的特点。同时针对多方安全计算平台的市场空缺，我们的产品将能够有效填补这些空缺，激发企业活力，也可以促进技术人员对该领域的进一步探索，从而研发出更加高效的多方计算平台。

W（Weakness）劣势

1）创业管理缺乏经验

由于仍是在校学生，故将产品向市场推广以及对公司的管理缺乏相关锻炼，故将产品由校园模式向商业模式转变仍需一定时间

2）产品安全性的实际论证困难

本产品的安全性可由理论进行证明，但是由于专业方向和技术原因，难以对产品进行攻防实验。

3）发展过程的资源及人力物力匮乏

本产品在将平台进一步升级以适应更大的计算量需要更多硬件以及人员支持。同时由于所使用的密码学知识都是近几年的最新技术，对产品的更新换代需要理论的支撑，但该方向技术人才较为缺少。

O（Opportunity）机会

1）市场需求量大，竞争小

由于多方计算平台的的实际应用技术还在起步阶段，且市场需求大而成熟的企业平台少，故竞争较小，拥有良好的发展环境。产品基于当今密码学最新成果，拥有巨大发展前景。

2）多方支持

目前国家积极鼓励大学生创业，颁布了诸多政策对大学生企业进行扶持；同时，基于我们产品的创新点，可能可以得到学校、企业的资助。这些支持将大大激发我们的创业热情。

T（Threat）威胁

1）技术缺陷

由于当前多方安全计算技术还并不成熟，致使不能实现项目更深一层的需求；由于算法的局限性会出现对于使用特定复杂运算的风控模型不适用的情况，面对特定运算增加会导致开发周期增长

2）能否抵御新型量子攻击是未知数

如今密码学已经步入后量子时代，新型的量子攻击可能将能够攻破本产品的密码体系。

**7.5 竞争策略**

1）提升服务质量

在保证技术支持可靠外，同时注重对客户提供个性化服务，可以针对客户需求，对产品部分内容进行修改，从而尽最大所能方便用户

2）提升客户使用体验

本产品面向用户类型较多，故要根据不同用户制定不同的软件形式。针对政府数据平台，着重对其数据库和加密/解密计算进行优化，结合身份认证、数据库备份恢复、容灾设计等多种安全方案保障系统安全；针对企业数据平台，则更加注重API的适应性，为计算端提供更加可靠的服务；针对个人用户，将以微信小程序或者安卓客户端，提供简洁的计算查询服务。

3）降低企业成本

由于是自主研发产品，成本较低，故在推广初期具有较大优势。

4）不断创新，融合最新理论成果

信息技术产业发展迅速，密码学领域亦是如此。我们的团队将时刻关注密码学最新研究成果，并将这些成果结合至我们的产品中去，使之安全性、运算效率得到提升。大学生是时代最活跃的元素，是最具创造力，学习力的群体。我们团队也将在密码学领域进行探索研究，以期提升我们产品质量。

**7.6 风险分析**

1）环境风险

正值国家大力发展大数据和人工智能等高精尖科技领域的时期，国家注重产学研的结合，大力推动最新理论成果的工业化和产业化发展，并对相关企业有利好性政策。我们所开发的多方安全计算平台，是现有云计算平台上加上了强力的安全保证，是大数据处理，机器学习算法运作的基础保证。可以说，在这方面国家扶持，政策利好，风险较低。

2）市场风险

如今，深度学习的算法与大数据挖掘的结合使得数据成为了各大企业的宝贵资源。企业在商业上合作相当频繁，但合作的同时想要保证自家数据的私密性。因此，数据及信息安全在合作中是至关重要的。

此外，政府作为公众的服务方，保证公众信息的安全性是义不容辞的。因此，政府对于外包项目的数据安全保证方面有着足够大的刚性需求。这正是与我们平台提供的服务紧密链接的。

在安全利用数据前提下，能够高效使用云计算平台对双方数据进行运算处理将大大提升企业合作的效率，增进运营能力，进而提升营业额，获取更多的利润。对于政府方面，减轻数据处理的负担同时保证了公众数据的私密性，进而保证了政府的公信力。因此，多方安全计算平台对于政府和企业来说都有着巨大的需求，市场方面风险较低。

3）竞争风险

在调查中，我们发现国内多方安全计算平台大多只在理论层面，仅有矩阵元公司在2018年发布了安全计算服务平台JUGO，但由于其进行不同场景得加密操作需要自行设计，要求技术操作水平过高，使得其通用性和适应性降低。

而我们设计的平台可支持多种类型的计算模型，有着较高的并发访问负载能力，同时有着较快的处理速度。无需任何技术，用户可通过傻瓜式操作完成需要，用户体验极佳。最重要的一点是，我们采用了最新型的全同态加密技术，并与安全比较协议相结合，其安全性得到了广泛的论证，可归约到环-LWE困难问题之上，在半诚实模型下可以称得上绝对安全可靠。安全性在如今的多方安全计算平台上无可比拟。

我们的平台加密上有着强有力的保证，提供了友善的人机交互界面，使我们平台用户体验极佳，有着出色的竞争力，竞争风险较低。

**7.7 推广方案**

1）宣传推广

1、线上推广

随着网络的普及，网络成为一种快速、直接、广泛、有效的宣传方式，所以线上推广是我们团队推广的中心。根据以上结论，我们做出如下推广策略：

A.产品网站的建设——Ankh多方安全计算平台建设

在所有的宣传工具中，产品网站是最基本、最重要的一个。没有产品网站，许多营销方案也将无用武之地，产品的网络推广总体效果也将大打折扣。我们将网站建设得更加完善，有吸引力。网站的风格设计成简约、清新的风格，给人一种耳目一新的感觉，从而吸引客户，设计出一个独特的Logo和标语以便于更好的推广产品。

然后，对产品全面详细地介绍是客户是否与我们合作的关键所在。因此，在每一项业务的介绍里，都要详细地描述。介绍应用的场景以及业务的流程，便于客户理解。

最后，还要介绍我们产品的一系列特点，操作简洁的一体化平台是我们产品的关键，保障数据安全是我们的核心，要注重突出介绍。

B.与其他银行或放贷网站合作

中国目前市面上的知名银行以及放贷机构较多，也有各自的网站门户，我们可以和其他的贷款机构及银行的网站合作，通过网站交换链接、交换广告、内容合作、用户资源合作等方式，在具有类似目标网站之间实现互相推广的目的，利用合作伙伴之间网站访问量资源合作互为推广，实现资源共享，共同扩大收益。

C.充分利用网络通讯手段加大宣传力度

利用QQ、邮件等方式对Ankh多方安全计算平台的产品和理念进行宣传，同时对我们的团队信息以及创新创业大赛进行阐述，以一种真诚、努力的态度来获取客户对我们的信任，对Ankh多方安全计算平台的信任。

D.网络广告

网络广告是一种潜移默化的信息沟通和传播手段，我们可以在热点网站中放入广告，另外论坛、博客、微博还有贴吧等也是传播信息的门户，我们可以在这些站点中对产品进行宣传和推广。

2、线下推广

我们可以主动与各类贷款机构，银行及涉及企业进行洽谈；并与政府人员进行联系，介绍我们的产品。制作宣传彩页和海报在指定地发投放，以达到更好的宣传效果。

2）客户来源

客户主要为三类对象：a、政府 b、借贷用户 c、放贷机构。

来源：1、客户通过产品的网站联系我们；

2、我们主动与各类贷款机构，银行或政府进行洽谈；

**7.7 盈利模式**

Ankh多方安全计算平台（以下简称为安可）致力于打造一个集政府、银行、贷款用户三位一体的一站式贷款服务平台。与政府、各大银行及房贷金融公司合作，面向广大需要贷款的用户，提供安全、可靠、便捷的贷款服务。

安可将采用组合的、动态的、进化的盈利模式，在安可项目初期，主要业务是为广大需要贷款的个人或企业用户提供一站式贷款平台，与各大银行或公司合作，为其提供投放产品的平台。因此，在项目初期，为了拓宽市场，将采取让利甚至是免费的模式，待公司发展到一定程度，将会对银行及放贷公司收取一定的手续费及广告费，以及在贷款中抽取一定比例的利息。

等到公司拓宽了足够的市场，将拓展除贷款以外的其他功能，在发展中期，公司凭借初期的可靠服务在众多中小微企业中获得了较高的知名度以及广阔的信息资源。安可将反过来利用整合这些信息资源，打造一个专为中小微企业服务的信息平台，而到此时，安可则通过提供信息服务来收取费用。

到公司后期，在中小微企业市场稳定后，会慢慢将业务拓宽到中大型企业。

通过这样的业务模式，在获得足够的市场份额之后，公司将获得稳定的收入来源。