**密 级： 公开**

**XXXXX**

**总体技术方案**

|  |  |
| --- | --- |
| **课题名称：** | **XXXX** |
| **起止时间：** | **2022年10月1日-2023年6月31日** |
| **组长：** | **吴飞宇** |
| **联系电话：** | **13351504524** |
| **编制日期：** | **2022年10月** |
|  |  |

**目 录**

[一、文档介绍 1](#_Toc103464492)

[1.1 文档目的 1](#_Toc103464493)

[1.2 文档范围 1](#_Toc103464494)

[1.3 读者对象 1](#_Toc103464495)

[1.4 术语与解释 1](#_Toc103464496)

[1.5 参考资料 1](#_Toc103464497)

[1.6 文档概览 1](#_Toc103464498)

[二、需求背景及国内外发展状况 1](#_Toc103464499)

[2.1 课题概述 1](#_Toc103464500)

[2.2 课题背景 1](#_Toc103464501)

[2.3 国内发展现状 1](#_Toc103464502)

[2.3.1 无人机通信模块 1](#_Toc103464503)

[2.3.2 通信认证 1](#_Toc103464504)

[2.3.3 组网协调/抗毁 2](#_Toc103464505)

[2.4 国外发展现状 2](#_Toc103464506)

[2.4.1 无人机通讯模块 2](#_Toc103464507)

[2.4.2 通信认证 3](#_Toc103464508)

[2.4.3 组网协调/抗毁 3](#_Toc103464509)

[2.5 预计今后发展趋势 4](#_Toc103464510)

[2.5.1 无人机通讯模块 4](#_Toc103464511)

[2.5.2 通信认证 4](#_Toc103464512)

[2.5.3 组网协调/抗毁 4](#_Toc103464513)

[三、课题目标及考核指标、测评方法等 4](#_Toc103464514)

[3.1 课题目标 4](#_Toc103464515)

[3.2 课题考核指标及测评方法 5](#_Toc103464516)

[3.2.1 终端统一认证模块 5](#_Toc103464517)

[3.2.2 用户认证 5](#_Toc103464518)

[3.2.3 生物认证 5](#_Toc103464519)

[3.2.4 推广示范性应用 6](#_Toc103464520)

[3.3 课题成果的呈现形式及描述 6](#_Toc103464521)

[3.3.1 硬件设备 6](#_Toc103464522)

[3.3.2 软件系统 6](#_Toc103464523)

[3.3.3 应用示范 7](#_Toc103464524)

[3.3.4 知识产权 7](#_Toc103464525)

[3.4 预期经济社会效益 7](#_Toc103464526)

[3.4.1 科学价值 7](#_Toc103464527)

[3.4.2 技术价值 7](#_Toc103464528)

[3.4.3 社会和产业效益 7](#_Toc103464529)

[四、技术方案及技术路线 7](#_Toc103464530)

[4.1 移动互联网大规模身份管理与认证体系框架 8](#_Toc103464531)

[4.2 终端统一接入认证机制 8](#_Toc103464532)

[4.2.1 研究内容 8](#_Toc103464533)

[4.2.2 技术方案 8](#_Toc103464534)

[4.3 群组接入认证方法 10](#_Toc103464535)

[4.3.1 研究内容 10](#_Toc103464536)

[4.3.2 技术方案 10](#_Toc103464537)

[4.4 用户认证 11](#_Toc103464538)

[4.4.1 研究内容 11](#_Toc103464539)

[4.4.2 技术方案 11](#_Toc103464540)

[4.5 生物认证 12](#_Toc103464541)

[4.5.1 研究内容 12](#_Toc103464542)

[4.5.2 技术方案 13](#_Toc103464543)

[4.6 系统部署 15](#_Toc103464544)

[五、需要突破的关键技术及其突破途径和方法 15](#_Toc103464545)

[5.1 自适应终端统一接入认证机制 15](#_Toc103464546)

[5.1.1 问题描述 15](#_Toc103464547)

[5.1.2 突破途径和方法 16](#_Toc103464548)

[5.2 用户认证 18](#_Toc103464549)

[5.2.1 问题描述 18](#_Toc103464550)

[5.2.2 突破途径和方法 18](#_Toc103464551)

[5.3 软生物特征融合的隐私数据保护方法 20](#_Toc103464552)

[5.3.1 问题描述 20](#_Toc103464553)

[5.3.2 突破途径和方法 20](#_Toc103464554)

[六、已有研究基础 23](#_Toc103464555)

[6.1 关键技术 23](#_Toc103464556)

[6.2 产品研制 23](#_Toc103464557)

[七、进度安排与组织保障 23](#_Toc103464558)

[7.1 进度安排 23](#_Toc103464559)

[7.2 组织保障 25](#_Toc103464560)

[7.2.1 课题的内部组织管理方式、协调机制 25](#_Toc103464561)

**一、文档介绍**

1.1 文档目的

1.2 文档范围

1.3 读者对象

1.4 术语与解释

1.5 参考资料

1.6 文档概览

**二、需求背景及国内外发展状况**

2.1 课题概述

2.2 课题背景

2.3 国内发展现状

2.3.1 4/5G自适应设备认证

2.3.2 用户认证

2.3.3 （软）生物认证

（1）人脸识别

我国在人脸识别领域的研究虽然起步相对较晚，但是进展迅速，很多研究机构、高等院校及多家IT公司都成立了人脸识别技术的研究小组，如华中科技大学、国防科学技术大学、武汉大学、北京交通大学，上海银晨智能识别科技有限公司等等，都取得了一定的成果。由中科院自动化所的科研人员历时近一年研发的人脸识别信息比对系统，开创性地将国际先进的人脸识别技术引入奥运安保，实现了奥运会开闭幕式对门票持有者进行实名制查验和人员身份识别的功能，为奥运安保大系统提供了决策支持依据。863计划、国家科技支撑计划、自然科学基金都拨出专款资助人脸识别的相关研究。我国的人脸识别技术正处在高速发展时期。

（2）声纹识别

国内对声纹识别技术的研究起步稍晚于国外，但经过国内研究人员的共同努力，声纹识别技术在国内已经得到了较好的发展与应用。2011年中国建设银行与北京得意公司合作，构建了基于说话人识别技术的声纹电话银行系统。2013年 11月，厦门天聪公司与厦门公安局指挥中心合作，搭建厦门“110”报警声纹采集与辅警系统。2013年12月，北京得意公司与中大信通合作的社区矫正项目，利用声纹识别技术为深圳司法局提供服务。

（3）软生物特征

杨文明等人介绍了一种通过使用手指背纹理作为软生物特征并结合手指静脉信息来提高个人身份识别鲁棒性的方法。杨璐等人将从手指静脉图像中获得的指骨关节宽度作为一种新的软生物特征来使用，可增加鲁棒性并辅助手指静脉识别。等人提出了一种多标签卷积神经网络来识别行人的软生物特征如性别、年龄和服装等。康文雄等人提出使用由手指组织在背景中形成的强度分布作为一种新颖的软生物特征来实现更好的手指静脉识别性能，融合主要生物特征和软生物特征可以产生更低的EER。

2.4 国外发展现状

2.4.1 4/5G自适应设备认证

2.4.2 用户认证

2.4.3 （软）生物认证

（1）人脸识别

当前很多国家展开了有关人脸识别的研究，主要有美国，欧洲国家，日本等，著名的研究机构有美国麻省理工大学（MIT）媒体实验室和人工智能实验室、美国卡耐基梅隆大学（CMU）的机器人研究所、法国INRIA研究院、美国伊利诺斯大学Beckman研究所和Microsoft ResearehAsia Face Group。美国国家标准技术局举办的FRVT2006（Face Recognition Vendor Test 2006）通过大规模的人脸数据测试表明，当今世界上人脸识别的一些方法的识别精度已经超过人类的平均水平。而对于高清晰、高质量人脸图像识别，机器的识别精度几乎达到百分之百。现在研究的方法主要有模板匹配、示例学习、神经网络、基于隐马尔可夫模型的方法等。

（2）声纹识别

声纹识别技术早已在西方许多国家开始应用，如：1998年欧洲电信联盟应用声纹识别技术在电信与金融结合领域，完成了cAvE计划；2004年美国最大的银行自动出纳机制造商NCR分部，开始试验自动出纳机的声纹核实效果。同年 5 月美国加利福尼亚州Beepcard公司发明了一种带有特殊安全功能的信用卡，这种信用卡只有在识别出主人的声音后确认身份后才能正常操作。2006年，荷兰的ABN AMRO银行率先使用了美国Voice Vault的声纹识别系统，借助预先录制的个人私密问题进行身份验证。目前在国外，声纹识别技术已经广泛应用到军事、国防、政府、金融等多个领域。

（3）软生物特征

Wayman明确提出了一种使用软生物特征（包括性别和年龄）过滤大型生物特征数据库的方法，可以缩短识别时间。Jain、Dantcheva等人分别对软生物特征进行了定义。Malhotra等人在监控场景中无法识别面部的情况下提出了以头部图像作为软生物识别对人员身份进行认证，并且通过实验证明了这种方法在10%的FAR下有超过90%的准确率。Lyle等人从眼周区域图像中提取性别和种族特征，以提高眼周识别的准确性和性能。Tome等人对软生物识别标签作为辅助信息的优点进行了实验研究，基于Southampton多生物特征隧道数据库的实验结果表明，利用软生物特征可以通过自适应融合规则在真实场景和理想场景中提高基于稀疏表示的人脸识别性能。

2.5 预计今后发展趋势

2.5.1 4/5G自适应设备认证

2.5.2 用户认证

2.5.3 （软）生物认证

如何确定个体身份并赋予对应权限是身份认证的基础和目标，而生物特征作为一种快捷有效的生物标识，已逐渐被安全认证系统所认可和采用。但是由于生物特征的隐私性问题，基于生物特征的认证技术还普遍局限于具有安全隔离能力的封闭系统中，且对设备的性能具有较高的要求。由于设备厂商、设备性能以及模型能力等诸多差异，基于生物特征的认证系统往往都是专门设计，无法实现网络化的统一认证需求。因此，针对 5G 网络下生物特征认证的特点，研究基于生物特征且具有隐私保护能力的身份鉴别方法是实现本课题最终目标的又一重要问题。在本项目中，我们所提出的方法利用 5G 云雾混构模式为生物认证提供计算能力，并采用软生物特征密钥生成和加密机制来保护用户隐私，可实现在5G云雾混构环境下对个体生物特征的隐私保护和快速鉴权。

**三、课题目标及考核指标、测评方法等**

3.1 课题目标

3.2 课题考核指标及测评方法

3.2.1 终端统一认证模块

#### 3.2.1.1 数量指标

完成时需提供一种支持终端统一认证模块的认证系统并通过现场数量查验。

#### 3.2.1.2 技术指标

立项时在终端接入认证方面有可供借鉴的技术积累。完成时需要提出支持具有动态可重构、自适应的终端统一接入认证机制。通过科技查新、专家鉴定或授权专利的方式进行测评。

3.2.2 用户认证

#### 3.2.2.1 数量指标

完成时需发布一种海量用户实体认证系统并通过现场数量查验。

#### 3.2.2.2 技术指标

立项时在用户实体认证安全协议设计方面有可借鉴的技术积累。完成时需发布具备一种海量用户实体认证服务虚拟化、用户的注册/注销等功能，支持5G云雾混构环境下海量实体认证系统支持10万用户并发下认证响应≤1s，高速实体认证系统认证处理时间≤500ms。

3.2.3 生物认证

#### 3.2.3.1 数量指标

完成时需发布一种实体认证系统并通过现场数量查验。

#### 3.2.3.2 技术指标

立项时在身份认证方面有可借鉴的技术积累。完成时需发布支持2种以上生物特征身份鉴别方式的实体认证系统并通过功能性能第三方或专家测试；在完成时需发布活体检测率达到98%的活体检测系统并通过功能性能第三方或专家测试。

3.2.4 推广示范性应用

#### 3.2.4.1 数量指标

完成时需发布一项以上推广示范性应用并通过现场数量查验。

#### 3.2.4.2 技术指标

无。

3.3 课题成果的呈现形式及描述

3.3.1 硬件设备

1、海量实体认证服务系统：用于对登录系统的用户进行快速身份认证，支持对采用不同鉴别方式的用户进行身份认证。面向海量用户身份认证需求，支持密码、短信验证码、TOTP、密码和验证码、TOTP和密码、TOTP和验证码等6种鉴别方式，认证处理时间≤500ms，支持10万用户并发下认证响应≤1s。

2、生物特征认证用户终端设备：对采用不同鉴别方式的用户采集所需的生物特征信息，并进行认证请求、获取认证结果。支持人脸和声纹生物特征的采集和传输。

3.3.2 软件系统

1、终端统一认证系统：用于终端设备的统一接入认证，支持对采用不同接入认证协议的终端进行设备认证。对现有认证协议进行改进，采用国密算法，实现接入网络自适应的、面向终端接入方案动态可重构的终端统一接入认证系统。

2、海量实体认证服务系统：用于实体身份管理、认证请求调度、认证策略管理，支持对采用不同鉴别方式的用户进行身份认证，具备实体认证服务系统配置管理、认证服务虚拟化、用户注册、认证和注销等功能，能够抵御重放、篡改、伪造等攻击。

3、生物特征认证系统：分别部署在雾计算节点、统一认证云和认证中心。具备用户特征信息注册、人脸识别、声纹识别等功能，其中软生物特征融合生成加解密密钥以保证安全传输。

3.3.3 应用示范

3.3.4 知识产权

标准、专利与论文：申请发明专利6项，发表SCI/EI检索源的学术论文10篇。专利以受理通知书或授权为准，论文以SCI/EI检索源期刊或EI检索源会议的论文录用通知或检索号为准。提交至全国信息技术标准化技术委员会或全国信息安全标准化技术委员会。

3.4 预期经济社会效益

3.4.1 科学价值

3.4.2 技术价值

3.4.3 社会和产业效益

**四、技术方案及技术路线**

4.1 移动互联网大规模身份管理与认证体系框架



图4-1 移动互联网大规模身份管理与认证体系框架

4.2 终端统一接入认证机制

4.2.1 研究内容

针对异构网络下终端漫游切换频繁、接入认证多模混合、降级攻击防御困难等问题，对现有认证协议进行改进，采用国密算法，提出适合于5G异构网络的统一接入认证协议；研究5G异构网络下多种接入认证机制的统一表述模型，并基于表述模型建立语义规约和等价判定方法，提出基于接入网络自适应的、面向终端接入方案动态可重构的统一接入认证机制。

4.2.2 技术方案

现有的多种安全接入标准都自立门户，分别在不同的领域被使用，从而导致没有保障网络安全的统一机制。在异构网络中，进行安全管理配置较繁琐，用户使用不方便，因此支持多种移动接入技术的多模接入终端成为未来网络发展的必然趋势。在融合了不同接入技术的异构网络中提供自适应的统一接入认证机制，保障设备安全接入成为了促进5G移动互联网络广泛应用的关键。需研究异构网络统一认证方法，使得终端能够自适应的接入不同网络。终端在自适应选择接入网络时可主要考虑三个方面的内容，当前终端所在的接入网络种类，当前终端所支持的接入网络类型以及从所支持的接入网络的类型中根据安全等级或网络信号质量等选取最佳的服务网络。本项目在分析现有多种异构无线网络接入机制安全性的基础上，针对未来5G网络中多种接入技术及安全机制并存的现状，提出适合于异构无线网络的动态可重构的、自适应的终端统一接入认证机制。具体思路如下：

首先，设计一种新的适合于5G异构网络环境下的统一接入认证协议。在5G网络中，用户可采用EAP-AKA'认证机制或5GAKA认证机制通过3GPP或非3GPP接入5G核心网络。在WLAN、2G、3G、4G等网络中，所采用的接入认证机制均是基于EAP-AKA协议设计。这些协议均是在EAP协议体系下设计和实现的。因此，本项目可通过对当前EAP协议进行适当修改，克服协议中存在的安全问题，设计适合于5G异构网络环境下的统一接入认证机制，屏蔽不同无线接入网的差异，实现5G网络在不同异构接入网络间的统一认证。

另一方面，由于当前5G网络中多种接入技术及安全机制并存的问题将存在很长一段时间，多模终端将在2G、3G、4G、5G网络下频繁的切换，接入认证机制无法忽视前向兼容的特性。因此，需要提出动态可重构、自适应的统一接入认证机制。如图4-2所示，通过分析异构网络现有接入认证方案，建立形式化异构网络认证协议统一模型并研究该模型下的语义一致性规约和语义等价关系，从而确定不同认证协议的语义一致性部分和模块，并对语义不一致部分使用变量进行表示，最终形成异构网络安全协议统一动态可表模型。当基于该模型的网络终端进行接入认证时，首先通过网络自适应模块确定统一模型中的变量部分和组合方式，从而动态生成对应网络的接入认证方案。同时，在接入认证服务器端，通过使用该方法，可以将不同认证协议中语义相同的部分统一实现，并在终端接入时确定不一致部分，充分利用动态可组合性提高认证的适配性和安全性，保证5G异构网络的接入认证安全。



图4-2 自适应终端统一接入认证机制

4.3 群组接入认证方法

4.3.1 研究内容

针对5G移动互联网络中终端类型多样、连接设备个数海量、高并发接入、时延和性能要求严格等特点，结合国密算法、群组机制以及聚合消息验证码等技术，提出适合于海量设备的轻量级群组安全接入认证机制，保证海量轻量级设备无差别的并发安全接入网络。

4.3.2 技术方案

选取国家标识密码SM3、SM4算法为核心加密算法，并采用接入点聚合的思想来实现大量无线认证信令的聚合和批量验证。具体地，在此研究方案中，根据群成员的不同类型，我们主要考虑下列两种研究思路。

一种是固定群组思路，例如同属于一个用户的设备。在该方案中，群成员之间一般会共享一个组密钥，群成员的添加和删除都需相应的动态密钥管理机制。

另一种是临时群组思路，例如，当大量的终端进入车站、体育场、大商场等密集区域时，这些同一区域的大量设备，临时被同时激活或者是并发接入，我们就可将这些设备构成一个临时群组。

这两种思路的认证流程大致相同，对于固定群组，可选择群组一个性能最佳的节点作为群主。对于临时群组可以将覆盖范围的雾节点作为临时群主。当群组需要同时接入到5G核心网络时，每个群成员生成认证消息并且将认证消息发送给群主。群主汇聚所有认证消息并采用聚合消息验证码AMAC方式将所有设备的认证消息聚合为一个消息，并转发给接入网络。接入网络将认证消息转发给5G核心网络中的认证服务器。5G认证服务器直接通过验证聚合消息验证码的合法性认证这群设备并产生相应的响应信息。同时，每一个设备也通过验证5G认证服务器生成的响应信息来确保其合法性。通过该方案可以有效减少终端发送给服务网络的请求认证的信令消息，因此可以很大程度地缓解接入网络的信令拥塞。

在这两种思路中，由于临时群组中的群成员之间无需在初始阶段生成群组密钥，因此无需一个群密钥的动态管理过程。但是，需要每一个设备均发送一条接入认证请求信息到雾节点，由雾节点来实施聚合。而固定群组认证机制则需要实施一个动态群组密钥管理过程，但是无需发送大量的接入认证请求信息到雾节点，直接由群主聚合生成一条聚合的接入认证请求信息到雾节点。

4.4 用户认证

4.4.1 研究内容

针对云雾混构场景下应用业务多元、实体海量等特点，提出海量实体身份认证系统。制定适用于云雾混构场景下实体身份注册安全接口与规范；解决高并发和支持多种鉴别方式的用户认证问题，设计面向多场景不同安全等级需求的安全协议族，实现多因子按需组合与统一认证方法，为接入应用服务系统的用户提供不同安全等级的认证服务，是应用系统服务建立安全连接的第一步。

4.4.2 技术方案

用户认证服务主要分为处理层和支撑层，整体逻辑框架如图4-3所示：



图4-3认证服务设备整体框架

1、处理层

处理层主要结合加密服务和TOTP服务，处理层模块的设计要满足以下几个目标：

（1）通过调度与认证服务中间件组件建立通信；

（2）根据本项目支持的（6种）认证协议处理认证信息，与客户端（用户）完成双向认证，生成token，协商会话密钥。

基于上述目标，在处理层模块中设计了以下子模块：PwAuth、MsgAuth和TotpAuth等。

2、支撑层

支撑层利用哈希算法实现数据存储的安全服务，支撑层模块的设计要满足以下几个目标：

（1）基于线性哈希算法的用户名快速检索结构

（2）定时与数据库中数据进行同步。

基于上述目标，在支撑层模块中设计了以下子模块：主查找树Hash\_Table、邮箱辅助查找树Mail\_Tree和手机号辅助查找树Phone\_Table。

4.5 生物认证

4.5.1 研究内容

我们主要研究基于软生物特征的融合鉴权和加解密技术，充分利用软生物特征的非隐私性和部分机密性，设计并实现在5G云雾混构环境下对个体生物特征的隐私保护和快速鉴权方案，并开发了一个生物特征认证系统，主要功能包括支持基于人脸和声纹的身份鉴别。

4.5.2 技术方案

1、组成模块



图4-4 生物特征认证系统组成模块

用户终端子模块（UE）：用于发起注册、认证请求；根据指示采集用户的软生物特征、生物特征信息并上传。

雾计算节点子模块（FCC）：用于转发认证请求、响应信息等；利用用户上传的软生物特征融合生成密钥、加密生物特征数据。

统一认证云子模块（Cloud）：用于使用软生物特征来过滤数据库和生成软生物特征密钥对生物特征尝试解密，将解密成功的用户子集发送到认证中心子模块。

认证中心子模块（AUC）：用于用户信息注册和生物特征识别。

2、处理流程



图4-5 注册和认证流程

整个流程可分为注册流程和认证流程，如图4-5所示：

1、注册阶段：

用户在可信认证中心AUC处进行注册。用户向AUC发送自己命名的唯一的身份标识（如用户名）。AUC指示用户采集生物特征和软生物特征并上传，并将用户的生物特征、软生物特征和身份标识等所有信息保存在自己的本地数据库中。

2、认证阶段：

UE将认证请求（包括支持的软生物特征列表、生物特征列表和会话标识）经由雾计算节点FCC转发到统一认证云Cloud。Cloud在中随机选择用于Cloud过滤、筛选数据库的软生物特征序列，剩余软生物特征序列用于生成软生物特征密钥加密生物特征，在中随机选择生物特征序列用于生物识别，并发送认证请求给认证中心AUC。AUC将数据库中所有用户的软生物特征数据返回给Cloud。最后Cloud将与序列经雾计算节点FCC转发到UE；

UE接收认证响应，采集和对应的特征，在采集到的特征数据中，将对应的软生物特征标记为，剩余的软生物特征标记为，采集到的生物特征标记为。将所述消息<，，，>发送给雾计算节点FCC；

雾计算节点FCC接收特征数据，使用K（雾计算节点FCC和统一认证云Cloud共享，此K为设备认证完成后得到的K）、和密钥派生算法生成软生物特征密钥，使用和加密算法加密生成生物特征密文；使用K、和SM3算法派生生成会话密钥，使用和SM4算法加密会话消息生成传输消息密文，并将和会话标识发送给统一认证云Cloud；

统一认证云Cloud接收密文后，使用K、和SM3算法派生生成会话密钥解密传输消息密文，得到；使用在保存的用户信息中进行过滤和筛选，生成集合={|符合的对应的身份标识的哈希}；对中的每个UE均利用和SM3算法派生生成密钥尝试解密生物特征密文；若解密成功，则可能是同一个用户；最后将解密成功得到的集合和生物特征发送给认证中心AUC；AUC收到认证消息，进行生物识别，将认证结果经Cloud、FCC转发给UE，认证结束。

4.6 系统部署

**五、需要突破的关键技术及其突破途径和方法**

5.1 自适应终端统一接入认证机制

5.1.1 问题描述

不同的接入网络采用了不同的接入认证机制，且现存的接入认证机制都存在安全和效率方面的问题。针对5G网络下多种无线网络技术接入体制并存、网络结构复杂、安全接入机制不统一等特点，需要研究可自适应所有不同异构接入机制的统一认证机制，保证终端能够透明地经多种无线网络安全接入网络。

5.1.2 突破途径和方法

针对异构网络下终端漫游切换频繁、接入认证多模混合、降维攻击防御困难等问题，对现有认证协议进行改进，采用国密算法，提出适合于5G异构网络的统一接入认证协议；研究5G异构网络下多种接入认证机制的统一表述模型，并基于表述模型建立语义规约和等价判定方法，提出基于接入网络自适应的、面向终端接入方案动态可重构的统一接入认证机制。

本项目在分析现有多种异构无线网络接入机制安全性的基础上，针对未来5G网络中多种接入技术及安全机制并存的现状，提出适合于异构无线网络的动态可重构的、自适应的终端统一接入认证机制。具体思路如下：

首先，设计一种新的适合于5G异构网络环境下的统一接入认证协议。在5G网络中，用户可采用EAP-AKA'认证机制或5GAKA认证机制通过3GPP或非3GPP接入5G核心网络。在WLAN、2G、3G、4G等网络中，所采用的接入认证机制均是基于EAP-AKA协议设计。这些协议均是在EAP协议体系下设计和实现的。因此，本项目可通过对当前EAP协议进行适当修改，克服协议中存在的安全问题，设计适合于5G异构网络环境下的统一接入认证机制，屏蔽不同无线接入网的差异，实现5G网络在不同异构接入网络间的统一认证。

另一方面，由于当前5G网络中多种接入技术及安全机制并存的问题将存在很长一段时间，多模终端将在2G、3G、4G、5G网络下频繁的切换，接入认证机制无法忽视前向兼容的特性。因此，需要提出动态可重构、自适应的统一接入认证机制。通过分析异构网络现有接入认证方案，建立形式化异构网络认证协议统一模型并研究该模型下的语义一致性规约和语义等价关系，从而确定不同认证协议的语义一致性部分和模块，并对语义不一致部分使用变量进行表示，最终形成异构网络安全协议统一动态可表模型。

要实现动态可重构、自适应的统一接入认证机制，具体包括如下步骤：

（1）使用规格和描述语言SDL形式化抽象建模，即从系统、功能块和进程三个层次进行分析，具体包括：

系统层次，即一种5G大规模终端的自适应组合认证方法所得的系统；

功能块层次，划分为统一处理模块，认证方式选择模块和认证处理模块；

进程层次，有解析标识符进程，认证方式选择进程，用户请求认证向量AV进程，用户认证网络和网络认证用户进程等；

（2）协议比较阶段，首先，分析多源终端的接入认证协议，对各个协议中涉及到的认证实体，认证结果确认和锚定密钥等方面进行分析和比较；然后，结合各个协议的具体接入认证流程，得到协议分析和对比结果；

（3）协议合并阶段，针对所得协议分析及对比结果，可以抽象出一个统一使用的认证框架，该认证框架可以处理异构网络的一些认证请求；

（4）协议功能模块划分，按照统一认证框架和各个协议的认证步骤进行功能模块的抽离，统一认证框架的内容分为公共部分和协议特有部分；公共部分是每一个接入认证流程都必须执行的部分，根据具体的认证协议，功能相同的部分，即公共部分，抽取成公共模块，功能不同部分，即协议特有部分，抽取成为功能模块，作为可以载入的子模块进行调用。

将统一认证框架的内容分为公共部分和协议特有部分。对协议的功能模块进行划分，该框架主要包括以下功能模块：公共模块、计算模块、鉴权模块、群组模块、检验模块和保存模块等。其中，

公共模块：主要包括计算随机数RAND，计算认证向量时使用的f1-f5函数并生成AUTN；计算认证响应RES等部分。

计算模块：主要包含除公共模块外，协议特有的计算部分，例如：5GAKA在计算哈希期望响应HXRES\*；生成各个协议的锚定密钥等过程。

鉴权模块：主要是各个协议在生成认证向量的一些计算过程。由于在公共模块中已经包含f1-f5和AUTN计算的过程，因此鉴权模块主要包含生成各自认证向量的后续步骤，并生成认证向量。

检验模块：主要包含一些参数的检验，包括消息序列号是否在合理的范围内和用户检验AUTN的新鲜性；网络对比两个参数是否一致等。

存储功能模块：保存模块主要负责在认证流程中的某个实体对一些参数进行保存。主要包括：对接收到的AV中的内容进行保存，以便完成后续的检验和认证流程。

综上所述，自适应终端统一认证结构图，如图5-1所示。



图5-1 自适应终端统一认证结构图

当基于该模型的网络终端进行接入认证时，首先通过网络自适应模块确定统一模型中的变量部分和组合方式，从而动态生成对应网络的接入认证方案。同时，在接入认证服务器端，通过使用该方法，可以将不同认证协议中语义相同的部分统一实现，并在终端接入时确定不一致部分，充分利用动态可组合性提高认证的适配性和安全性，保证5G异构网络的接入认证安全。

5.2 用户认证

5.2.1 问题描述

一方面，考虑到海量用户获取服务具有突发性，在某些时间段会出现大类的服务请求。然而，服务请求之前，用户都需要实体身份认证系统进行身份鉴别。另一方面，考虑到云雾混构场景下用户认证的丰富应用场景与长期稳健性，所以实体认证系统在对多角色差异化的用户进行统一认证时，应支持多种适应服务场景的身份鉴别方式，以实现用户在不同场景、不同角色登录系统时可以按需组合灵活地完成登录。因此，需要实现高并发的实体身份鉴别模型，同时适应多场景不同鉴别方式的需求。

5.2.2 突破途径和方法

**问题1：高并发的支持**

解决途径：利用大内存的服务器实现I/O多路复用，然后结合Event通知技术进行事件响应。

步骤1：突破TCP协议对连接的限制。TCP协议本身存在限制，在Linux中，标识一个TCP链接使用的是文本描述符fd，每个fd是根据客户端IP，客户端Port，服务器Port，服务器IP的四元组定义，往往在CS架构中，服务器port、服务器IP、客户端IP是固定的，导致一个Client到Server最大的链接数是客户端本地能拥有的port的数量。linux内核对一个进程可以使用的port的范围一般是1024-65534个，因此在协议层面，单个客户端链接一个服务器最多是64510个。如果让服务器端采用epoll机制，实现I/O多路复用，可突破fd的个数限制，进行连接检测从用户态拷贝到内核态只需要一次，使用事件通知机制来触发。通过epoll\_ctl注册fd，一旦fd就绪就会通过callback回调机制来激活对应fd，从而触发相关的I/O操作。

步骤2：突破linux对fd的限制。由linux定义可以知道，linux中对于套接字是按照文件来定义，对于一个套接字，在内核层面认为是一个可以进行网络读写的文件。打开一个文件会创建一个文本标识符。linux中对于单个进程会限制其打开文件的最大数量即fd的数量上限，通过ulimit -n可以查看和修改这个限制，通过修改这个上限为1024000，可以实现单线程支持100万个连接。

步骤3：增大系统内存以支持足够多的fd。linux对于套接字占用的内存，也会有所限制，假设每个fd消耗内存为16K字节（即读buffer、写buffer、逻辑读缓冲器、逻辑写缓冲器都取最低值4KBytes），那么4GB/16KB=26.2万,即4GB的空闲内存可以支持操作系统建立26.2万左右个套接字描述符fd。如果要增加并发数的上限，需要增加内存。为了让每一个fd都能正常处理大量的数据，需要增加其预计分配内存，因此还是需要增加内存。每个fd的预计分配内存可以通过在sysctl.conf修改值的形式来进行修改。

步骤4：增加等待时间让服务器能接受大量并发的接入客户端。对于服务器端的程序，其侦听函数int listen( int sockfd, int backlog)的第二个参数是指定当前sockefd上等待accept的链接的最大长度，因为accept会存在延时，为防止过多链接涌入，导致因为默认队列长度过短而丢弃，可以修改队列最大长度。为了减少因为等待超时而丢失的fd，可以修改等待时间来保证高并发环境下每次链接的成功率增加。

步骤5：利用主从式多线程突破单线程连接限制。经调研可发现通过u limit-n可以将该值增加到上限1024000，该值定义了单线程最大可以打开文件描述符的限制。为绕过该限制，服务可采用多进程的思想，即启用主从服务模型，由主进程进行调度。将数客户端的链接分别重定向到不同子进程中，又由于linux中限制同一个端口同一时间只能由一个程序监听0.0.0.0，因此服务可采用多端口监听。

**问题2：多种适应性身份鉴别方案**

解决方案：设置多因子按需组合的鉴别方案，即密码、短信、TOTP等认证因子三种认证因子一种或多种组合认证方式，实现用户与服务系统双向可信认证，抵御仿冒、重放等各类协议攻击，具体包括：

密码为通过键盘等外设输入提取为标准认证数据格式，与注册密码数据比对。验证码通过短信认证辅助服务器，在接收认证请求后，推送验证码短信至认证用户预留手机号，通过键盘等外设设备输入提取为标准认证数据格式。TOTP为一种一次一密的认证方式，为内置密钥及计算方法，用户在通过密码或验证码认证为所属用户后，选择进行TOTP申请后，在特定的软件上获取TOTP码，认证服务器通过相同的方式计算数据是否是正确的。

5.3 软生物特征融合的隐私数据保护方法

5.3.1 问题描述

生物特征识别是指利用人体独一无二的特征进行身份识别的一种便捷高效的身份认证技术，当前普遍采用的生物特征主要有指纹、人脸、虹膜和声纹等等。与传统的认证办法相比，生物特征具有唯一性，可唯一标识一个人的身份，已广泛被安全认证系统认可和采用，应用于各个行业。但另一方面，生物识别技术的隐私问题也同样存在，用户的生物特征数据一旦遭到泄露，将对用户的个人信息安全、生命财产安全造成极大威胁。

5.3.2 突破途径和方法

我们提出基于生物特征和软生物特征的融合鉴权和加解密技术方案，利用雾计算节点的计算能力将非隐私性的软生物特征融合生成密钥来加密生物特征，从而保证传输过程中生物特征的安全性和隐私性；统一认证云利用软生物特征尝试解密生物特征，但不知道该用户是谁；可信的认证中心进行生物识别并返回认证结果。通过部署在不同的节点、供不同的用户使用，可实现云雾混构场景下对个体生物特征的隐私保护。但是在不同时间、不同地点采集到的软生物特征不是完全相同的，存在一定的偏差，因此如何在雾计算节点和统一认证云生成相同的软生物特征密钥是一个问题，提出的方案也解决了这个问题。



图5-2 密钥派生流程



图5-3 加解密流程

密钥派生和加解密方法，如图5-2、图5-3所示，包括以下步骤：

1、将雾计算节点FCC和统一认证云Cloud共有的K（密钥长度为256bits）分为SK（前128bits）和BK（后128bits），分别用于派生会话密钥和软生物特征融合密钥。FCC和Cloud共享会话标识和软生物特征融合参数，在每次不同认证请求中均将变化，因此可分别辅助用于不同的密钥派生；

2、雾计算节点FCC接收特征数据，首先根据计算软生物特征融合参数：

（为用户的第j个软生物特征，为对应的权重，为软生物特征的加权和），

（此处<…>代表向下取整），

然后使用SM3算法和不同的参数通过密钥派生生成软生物特征密钥和会话密钥：

，

，

之后使用和SM4算法加密生物特征数据生成生物特征密文：

，

使用和SM4算法加密传输消息生成传输消息密文：

，

最后FCC将和会话标识发送给统一认证云Cloud；

3、统一认证云Cloud接收密文后，首先使用SM3算法密钥派生生成会话密钥：

，

使用和SM4算法解密传输消息密文得到：

，

然后使用在保存的用户信息中进行过滤和筛选，找出所有可能是同一个待认证用户的用户组，生成集合={|符合的对应的身份标识的哈希}。对中的每个UE均计算：

（为第i个UE的第j个软生物特征，为对应的权重，为第i个UE的软生物特征的加权和），

（此处<…>代表向下取整），

,

,

,

使用生成的三个密钥、、尝试解密生物特征密文，若解密成功则可得到生物特征明文：

。

**六、已有研究基础**

6.1 关键技术

6.2 产品研制

**七、进度安排与组织保障**

7.1 进度安排

年度制定完成课题的计划进度，将课题的考核指标分解落实到年度计划中。

|  |  |  |  |
| --- | --- | --- | --- |
| 年度 | 任务 | 考核指标 | 成果形式 |
| 2017年 7月  |  2017年 12月 | (1)课题总体技术方案设计  (2)课题总体技术方案评审  (3)完成电子凭据安全服务体系框架、电子凭据服务监管与核准、大规模实体统一接入与鉴权、安全电子凭据服务及其监管标准等关键技术研究方案编制 | (1)课题总体技术方案1 份 | (1)课题总体技术方案报告 |
| 2018年 1月  |  2018年 12月 | (1)课题实施方案编制  (2)完成电子凭据安全服务体系框架、电子凭据服务监管与核准、大规模实体统一接入与鉴权、安全电子凭据服务及其监管标准等技术研究方案论证 | (1)电子凭据安全服务体系框架及服务监管系统关键技术研究报告1 份  (2)年度报告1 份  (3)发明专利2 项  (4)论文4 篇 | (1)研究报告  (2)年度报告  (3)发明专利  (4)论文 |
| 2019年 1月  |  2019年 12月 | (1)完成核准业务监管服务中间件、电子凭据核准服务管理系统、统一身份管理系统、电子凭据服务监管平台管理系统、电子凭据服务监管平台存储系统、电子凭据服务监管平台运维系统、电子凭据标准符合性评测系统的方案论证，开展研发  (2)完成高性能监管业务调度设备、电子凭据高速核准服务设备、统一认证服务设备、身份鉴别终端的方案论证，开展研制  (3)初步完成电子凭据服务监管的接口规范，具备初步用户身份管理、核准业务管理、存储资源管理、权限管理、平台运行监控等功能  (4)完成电子凭据密码应用安全方案的初步设计 | (1)核准业务监管服务中间件原型系统1种  (2)电子凭据核准服务管理原型系统1 种  (3)统一身份管理原型系统1 种  (4)电子凭据服务监管平台管理原型系统1 种  (5)电子凭据服务监管平台存储原型系统1 种  (6)电子凭据服务监管平台运维原型系统1 种  (7)电子凭据标准符合性评测原型系统1种  (8)高性能监管业务调度设备原理样机1种  (9)电子凭据高速核准服务设备原理样机  1 种  (10)统一认证服务设备原理样机1 种  (11)身份鉴别终端原理样机1 种  (12)中期检查报告1 份  (13)年度报告1 份  (14)发明专利2 项  (15)论文5 篇  (16)标准建议稿2 项 | (1)原理样机与原型系统  (2)中期检查报告  (3)年度报告  (4)发明专利  (5)论文  (6)标准建议稿 |
| 2020年 1月  |  2020年 12月 | (1)完成核准业务监管服务中间件、电子凭据核准服务管理系统、统一身份管理系统、电子凭据服务监管平台管理系统、电子凭据服务监管平台存储系统、电子凭据服务监管平台运维系统、电子凭据标准符合性评测系统的研发  (2)完成高性能监管业务调度设备、电子凭据高速核准服务设备、统一认证服务设备、身份鉴别终端的研制  (3)完成电子凭据密码应用安全方案  (4)课题验收 | (1)核准业务监管服务中间件1 种  (2)电子凭据核准服务管理系统1 种  (3)统一身份管理系统1 种  (4)电子凭据服务监管平台管理系统1 种  (5)电子凭据服务监管平台存储系统1 种  (6)电子凭据服务监管平台运维系统1 种  (7)电子凭据标准符合性评测系统1 种  (8)高性能监管业务调度设备1 种  (9)电子凭据高速核准服务设备1 种  (10)统一认证服务设备1 种  (11)身份鉴别终端1 种  (12)测试报告1 份  (13)发明专利2 项  (14)论文4 篇  (15)标准建议稿2 项 | (1)设备与系统  (2)测试报告  (3)验收报告  (4)发明专利  (5)论文  (6)标准建议稿 |

7.2 组织保障

7.2.1 课题的内部组织管理方式、协调机制

7.2.2 课题实施的相关政策，已有的组织、技术基础，支撑保障条件。

7.2.3 对实现项目目标的支撑作用及与项目内其他课题的协同机制