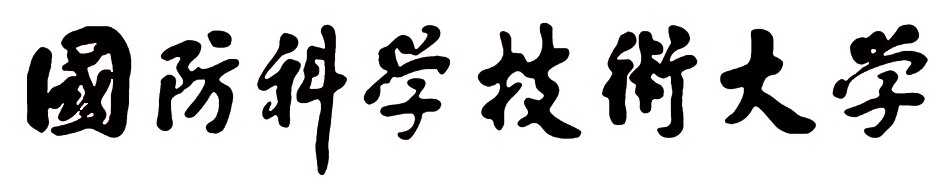
密级： 公 开

编号：



**博士研究生学位论文**

**开题报告**

|  |
| --- |
| **论文题目：** 基于新型信任体系的域间路由安全关键技术研究 |
| **学 号：** 15069036 **姓名：** 邢倩倩 |
| **一级学科：** 计算机科学与技术 |
| **研究方向：** 网络与信息安全 |
| **指导教师：** 王宝生 **职称：** 研究员 |
| **学 院：** 计算机学院 |
| **开题时间：** 2017 **年** 3 **月** 26 **日** |

国防科学技术大学研究生院制

二〇一四年十二月

说 明

1. 开题报告应按下述要求打印后装订成册：

1.使用A4白纸，双面打印；

2.封面中填写内容使用小3号仿宋字体；

3.表中填写内容使用5号楷体字体。

1. 封面中的编号由学院填写，采用八位数编码，前四位为审批日期，精确到年月即可，第五位为院别，后三位为审批流水号（按年）。如15016100，为6院15年审批的第100位开题申请者，审批时间为15年1月份。院别代码与编制序列一致，海洋科学与工程研究院代码为0。
2. 开题报告表中学员填写的内容包括学位论文选题的立论依据、文献综述、研究内容、研究条件、学位论文工作计划、主要参考文献等，指导教师认可学员开题报告内容后，对学员学位论文选题价值、对国内/外研究现状的了解情况、研究内容、研究方案等方面予以评价。
3. 开题报告评议小组一般由3-5名具有正高级专业技术职务的专家（包括导师）组成，其中一名为跨一级学科的专家。
4. 博士生开题报告会应面向全校公开举行，评议小组听取研究生的口头报告，并对报告内容进行评议审查。
5. 若开题报告获得通过，应根据评议小组意见对开题报告进行修改，并在开题报告会后两周内，将评议表和修订后开题报告纸质版原件交学院备案；若开题报告未获得通过，则填报延期开题申请，由原开题报告评议小组重新组织开题报告会。

1.学位论文选题的立论依据

|  |
| --- |
| （课题来源、选题依据和研究意义）   1. **课题来源**   “全自主可控XXXX网络”——XX预研  “可信柔韧XX结构和协议体系” ——XX预研   1. **选题依据**   路由是互联网的神经系统和重要基础设施,是互联网能够支撑运行并提供服务的关键。所谓路由是指通过相互连接的网络把信息从源地点移动到目的地点的活动，而路由协议又是整个路由体系的核心。路由协议就是在路由指导数据包发送过程中事先约定好的规定和标准，主要用来进行路径选择，其工作性能的好坏以及安全与否直接影响到联网工作和服务的质量。路由协议分为域内路由协议和域间路由协议，针对沟通不同自治域的域间路由协议而言,目前的事实标准是制定于1995年的第四版本边界网关协议（Border Gateway Protocol version 4，BGPv4）。历史上，BGP 对于互联网的商业化和全球化立下了汗马功劳。然而，BGP 协议的设计在安全方面留有巨大的缺陷。BGP路由器默认接受并无条件信任邻居路由器通告的任何路由，导致BGP路由协议容易受到前缀地址劫持和路由篡改攻击，其结果轻可造成路由黑洞(black hole)和中间人攻击(man-in-the-middle attack,简称 MITM),重则容易导致互联网的大规模瘫痪。前缀劫持(network layer reachability information (NLRI) falsification attack)是指一个恶意的自治系统宣告并不属于它的地址前缀，从而非法获取流量，并使得地址前缀的真正拥有者收不到本应属于它的数据，路径篡改(AS\_PATH falsification attack)是指恶意自治系统篡改更新报文中的路径属性，如在AS\_PATH属性中插入或删除自治系统，或者更改自治系统的序列，从而产生路由延迟或允许恶意的自治系统改变网络的流量模式。  随着网络环境的日益复杂，当前网络的安全情况已经与原先协议设计时所处的安全可信的环境大相径庭。近年来，发生了多起由BGP的脆弱性引起的互联网安全事故，造成巨大的损失如2008年，巴基斯坦电信根据政府授意，对YouTube视频网站的前缀进行了劫持，造成2/3的互联网用户不能访问被劫持的网站，又如2010年4月，中国电信向外宣告了170多个国家的前缀，地址范围涉及互联网的1/7（15%的地址空间）[22]，该事件被美国政府高度重视。2014年，俄国黑客有针对性地对网络流量进行重定向，以盗取比特币[23]。2017年年初伊朗对其监管屏蔽的256个网址通告了更短的虚假路由路径[24]，造成访问流量的重定向，影响包括了印度、俄罗斯和香港的主要网络服务供应商对这些网址的正常访问。    图1.1 全球BGP安全事件  这一类全球BGP劫持事件虽然易察觉修补快，持续时间短，但依然给被攻击者造成了大量的经济损失。更加严重的是，全球著名安全公司赛门铁克 [76]披露互联网长期存在大量BGP隐蔽劫持的严重攻击，期间所发现的约有2,655个隐蔽劫持均未被实时BGP 监测系统Argus[77]检测到。进一步，BGP劫持可以作为其他高级网络攻击的有效手段，其威胁巨大。2015年黑帽大会[25]指出BGP安全缺陷可帮助攻击者隐蔽发动BGP本地劫持，实现Certificate Authority Hijacking窃取CA证书，之后任意发动中间人攻击。BGP劫持还可有效窃听、延迟比特币交易流量[26]，只要劫持全网不到15%的（900个）前缀，即可造成51%攻击。综合历史攻击事件和潜在严重威胁可以看出，BGP安全威胁仍然是个十分严峻的问题。   1. **研究意义**   BGP安全对于整个互联网的意义十分重大，安全问题也成为了研究的热点，主要分为两大研究方向，一类是被动防御型的BGP安全监测，一类是主动设计的BGP安全机制。BGP安全监测一般[77,78]针对前缀劫持和路由泄露进行监测，其报警往往不够即时，并且无法发现精心设计的本地BGP劫持[25]和未通告前缀，对路由路径篡改攻击也缺乏监测效力。BGP安全机制则为了弥补BGP路由协议固有的脆弱性，解决BGP的三个安全问题：(i)BGP协议本身没有机制来保证对等体之间通信消息的完整性、新鲜性以及对等实体的真实性; (ii) BGP协议中没有提供机制来确认一个AS宣告网络前缀的所有权; (iii)在BGP协议没有提供机制来保证所接收到的路径属性的真实性。为此，学术界和工业界提出过多个路由协议安全机制，通过采用各种路由认证技术来修补BGP协议缺乏路由认证机制的缺陷，具体机制包括S-BGP、soBGP、RPKI和BGPSEC等，我们统称为S\*BGP协议。目前所提出的方法都存在诸多局限与不足。  **（1）S\*BGP方案可部署性弱，应用普及率低**  S-BGP[41,42]的安全机制主要建立在三个安全实施模块之上：PKI、路由属性证明和IPsec。S-BGP使用的PKI基于X.509 (v3)的扩展证书，以此来验证AS号码和IP地址前缀的持有者的身份和授权。路由属性证明模块完成对路由信息的数字化签名授权，主要包括地址证明和路由证明。地址证明来授权它管辖范围内的AS可以发起到该地址前缀的路由，而路由证明用来授权其邻居可以通告发布给它的路由。IPsec模块确保路由器之间点到点传输的BGP流量的安全。由于需要依赖第三方基于X.509证书的PKI系统进行网络基本元素和基本行为的绑定，目前的路由协议安全机制的执行需要各层级互联网注册机构以及路由器厂商的共同参与，部署难度非常大。因此自2000年提出至今，S-BGP一直未能实现部署。  BGPsec[48]采用相似的认证思想实现路由路径认证，同样需要依赖第三方基于X.509证书的PKI系统进行网络基本元素和基本行为的绑定，虽然IETF工作组指定其为路由路径安全认证协议，并正在制定协议标准，但由于其证书管理复杂、签名验证耗时，只有部分部署情况下安全效力大打折扣，因此部署动力仍然不足[60]。  **（2）已有S\*BGP方案存在安全缺陷**  针对部署难的问题，soBGP[43]提出不依赖层次结构信任模型的简洁的安全机制。其采用web of trust信任网的信任，任何主体都可以通过对系统中的其他主体拥有的密钥证书进行签名而成为CA。由于缺乏信任锚，soBGP的安全性相对S-BGP等其他机制显著降低。  2010年IETF的安全域间路由工作组面向问题(ii)，发布RPKI(Resource Public Key Infrastructure)协议标准[18,21]，用于指导建立域间路由源安全认证。RPKI也依赖于独立的公钥基础设施，为了降低部署难度，该机制只针对前缀劫持攻击中篡改路由更新中源地址的问题，使用路由源证明和实体证书，实现BGP的源路由认证。但是RPKI无法进行路由更新的路径认证，使得部署了RPKI的BGP路由机制依然存在前缀劫持的威胁。BGPSEC在RPKI的基础上，利用RPKI构建的资源公钥基础体系，实现BGP协议的路径认证。但是，与S-BGP类似，依赖于公钥基础设施导致RPKI和BGPSEC在具体部署时也遭遇了一定的困难。并且研究表明，在部分部署域间路由安全机制的情况下，其安全状况可能会变得更加糟糕。针对RPKI机制的攻击模型也被证实对BGP的破坏是行之有效的。  为解决现有域间路由协议问题，设计一个具有低性能开销，满足增量部署的可行安全路由方案具有重大的意义。本课题针对传统公钥基础设施构建复杂，部署难度大的问题，提出基于区块链的去中心化信任基础设施构建高效可信的路由源安全通告，并能够增量部署，进一步基于身份基密码体制构建轻量级的安全域间路由协议，实现路由路径的低开销认证，解决BGP协议缺乏路由认证机制的缺陷。 |
|  |

2.文献综述

|  |
| --- |
| （该领域在国内/外的研究现状及发展动态；阅读文献的范围以及查阅手段等。博士不得少于2000字，硕士不少于1000字。可附页）   1. **基于证书认证的信任基础设施**   在一般的开放通信系统中，通信双方可能事先并不认识，并且在大多数情况下，双方只通信一次，简单的密钥管理方法要求每个主体都要管理不现实的巨大数量的公钥。由一个可信的主体提供密钥管理服务可以有效处理通信主体自身管理密钥的繁琐工作。在公钥管理服务中，使用证书机构（Certification Authority, CA）作为可信服务器，完成用户证书统一管理工作。公钥证书是一个包含多项数据的结构化数据记录，它包括持有者唯一可识别的身份、公钥参数以及CA的签名。CA对证书的签名提供了持有者的身份与其公钥的密码绑定。如果一个主体信任CA，那么当它验证了另一个实体的证书有效后，它就应该信任这种绑定的有效性，这是因为只有当CA正确地识别了持有者以后，才发放证书。Kohnfelder首先使用公钥证书这个概念[15]。  目前被广泛使用的基于证书的公钥认证框架实例主要有X.509公钥证书框架[16]和PGP公司推出的完美隐私（Pretty Good Privacy）信任网[17]。标准的公钥证书框架称为X.509公钥证书基础设施，其规模呈树状层次结构。在此层次结构中，根节点代表根CA，作为整个系统中的信任锚；除根节点外的每个节点代表一个主体，其公钥证书由它相邻的父节点颁发。在X.509信任树中，叶子节点表示端用户主体，所有非叶子节点代表不同层级的CA。由于用户对根节点CA的绝对信任，X.509建立了完整的行之有效的层次化信任体系。与X.509不同，PGP信任网是一种非层次结构的信任模型，而且不拥有全局统一的信任锚。在PGP信任网中，任何主体都可以通过对系统中的其他主体拥有的密钥证书进行签名而成为CA。显然，作为CA的主体并不是完全可信赖的。因此，PGP信任网为用户生成密钥对之后，由用户寻找足够多的主体为其密钥对签名以获得多个对应的证书。基于非所有签名者都是坏人的假设，PGP信任网的主体可通过验证系统中另一主体足够多的证书以判断该主体的公钥的真实性。  2011 年, IETF 开始由 SIDR 工作组来进行 Resource PKI(RPKI)的标准化工作[21]. RPKI 使用 X.509 PKI来保护 BGP 路由协议通信安全; IANA(Internet Assigned Numbers Authority)执行根 CA 功能, 与RIR(Regional Internet Registry)、 LIR(Local Internet Registry)形成 3 层 CA 结构, 为用户签发证书. 在 RPKI证书中, 以证书扩展的方式表示了 IP 地址资源的分配. 目前 RPKI 的部署仍未全面开展, 文献[27 50]给出了RPKI 的现实部署情况。  PKI面临许多问题，一方面证书管理系统较为复杂，在性能开销要求高的场景下应用受限，另一方面被攻击或恶意 CA 可导致重大安全隐患。如果依赖方信任的 CA被攻击或执行恶意操作、签发包含虚假信息但可验证成功的服务器证书, 则中间人攻击就很容易成功(即使客户端执行了正确的证书验证和域名检查步骤). TurkTrust CA 公司的虚假信息证书、 DigiNotar CA 公司被攻击、 Comodo CA 公司安全事件等等, 都显示此类攻击完全可能发生。虽然Certificate Transparency [28]、ARPKI[29]、Accountable Key Infrastructure[30]等给出了PKI基础设施安全增强方案，但其相当于对原本复杂的PKI系统增添了更为复杂的管理机制，实现部署的激励不够，可行性并不高。   1. **基于身份自认证的新型信任体制**   传统公钥基础设施(PKI)实质上是一组被信任的第三方提供证书目录，去证明服务与钥匙之间的联系。而基于身份基公钥密码体制构建基于非目录的公钥认证框架。由于身份基密码体制中主体身份标识与主体公钥的天然绑定，基于此密码体制构建的公钥认证框架无需使用可信第三方建立证书机构，极大降低认证框架的复杂性，提高主体间的认证效率。但是，由于身份基密码体制需要可信的密钥生成机构PKG为用户主体生成私钥，不排除PKG伪造用户签名的可能性。因此，基于传统身份基密码体制构建的公钥认证框架不适于开放系统环境中的应用。另一个有待解决的问题是不依赖与撤销列表的非交互密钥吊销方案的设计。目前，基于非目录的公钥认证框架的研究还较少，IKI[31]给出一种有效可行的身份注册管理框架，其基础设施包括互不串谋的PKG和第三方注册机构RA，解决了密钥托管的问题。美国的Voltage公司[19]基于身份基密码体制，设计出安全可扩展的数据中心加密、凭证化以及密钥管理方案，并为用户提供邮件加密等安全产品，是身份基密码体制在公钥认证的应用的重要示例。Tariq[20]等人将身份基密码体制应用于无中介的发布/订阅系统，解决由于松耦合特性带来的认证以及内容加解密困难问题。但是，该研究仅局限于密码体制的在发布/订阅系统的具体应用，并没有进一步构建完整的公钥认证框架。   1. **基于区块链的新型信任基础设施**   传统公钥基础设施(PKI)实质上是一组被信任的第三方提供证书，去证明服务与钥匙之间的联系。不过这些证书机构已经被证明有可能出问题的；当这些机构被攻克（无论是来自外部的还是内部的），都有可能悄悄地发出无效的证书。这就是集中式信任的滥用问题。  Google 的“透明证书”（CT）系统[28]使用分布式账本技术来实现CA证书发布行为的透明审计。所有的证书会被附加到一个分布式账本上，任何用户或服务都可以检查他们将要使用的证书就是账本里存放的证书。相应地，伪造的证书会被快速地发现——这会让那些寻求攻克或滥用 PKI 系统的人失去动力。  CONIKS[32]为了解决中心化方案不能解决当用户想保护个人信息和通讯记录时，在钥匙和实体机构间建立权威的联系中存在脆弱的安全问题，使用特别构造的分布式账本，去存储和调取用户的公钥，这些公钥可用于加密或者对邮件进行签名。与透明证书技术不同的是，透明证书技术依赖于第三方构成的网络去维护和审查分布式账本的完整性，而 CONIKS 使用通讯服务提供商和他们已有的用户数据库去建立一个具有高度完整性的账本。  以上都是分布式账本的雏形，用于实现全局统一的可审计信任数据库。2008年中本聪提出了点对点的比特币系统[33]，其中所利用的Blockchain技术给了分布式账本以新的实现范式。区块链算法让比特币的交易可以在“区块”里集中起来，并通过密码学签名添加到现有区块组成的“链”里面。比特币账本是用分布式及“无需许可”的方式构建的，任何人都可以通过解决生成新区块所需的密码学难题从而添加一个包含交易的区块。    图2.1 基于哈希链的blockchain区块结构示意图  由此建立的信任是去中心化的：区块链上记录交易状态信息，其数据的验证、记账、存储、维护和传输等过程均是基于分布式系统结构, 采用纯数学方法而不是中心机构来建立分布式节点间的信任关系, 从而形成去中心化的信任基础设施。因此，区块链能够通过运用数据加密、时间戳、分布式共识和经济激励等手段，在节点无需互相信任的分布式系统中实现基于去中心化信用的点对点交易、协调与协作，从而解决中心化机构普遍存在的高成本、低效率和数据存储不安全等问题。    图2.2 区块链交易格式  （1）代币  2014年，比特币官方客户端（Bitcoin Core），引进了一种可以添加任意元数据（metadata）的官方机制。这一机制很快被Proof of Existence[34]和BlockSign[35]这样的机构使用，他们通过将文档的数字签名嵌入到比特币的交易中，用来作为文档存在性的证据。其他还有php--OP\_RETURN[36]这样的工具，可以对区块链网络存储或读取更大的数据，把它变成了一个通用目的的、永久性、分布式的数据存储设备。比特币的元数据(metadata)功能被其他几个协议使用，比如CoinSpark[36], Counterparty[37], Omni Layer[38]，Open Assets[39]等，使得比特币网络开始支持第三方资产交易。  代币[40]的应用可以实现比特币与现实资产的链上交换。首先，一个资产发行实体，在比特币网络发送一个交易，附带一个“资产创始”的元数据，实际相当于创建了一个代币（tokens），用来代表某一项资产。当然，资产发行人必须承担合同业务，任何时候、任何人用这些代币都可以换取现实世界中的等价值资产。这些代币的所有权在比特网络上，不需要资产发行人的授权，就可以自由交易流通。  （2）区块链脚本  比特币采用一种简单的、基于堆栈的、从左向右处理的脚本语言, 而一个脚本本质上是附着在比特币交易上的一组指令的列表。    图2.3 面向智能合约的区块链交易示意图  比特币交易依赖于两类脚本来加以验证, 即锁定脚本和解锁脚本, 二者的不同组合可在比特币交易中衍生出无限数量的控制条件. 其中, 锁定脚本是附着在交易输出值上的\障碍", 规定以后花费这笔交易输出的条件; 解锁脚本则是满足被锁定脚本在一个输出上设定的花费条件的脚本, 同时它将允许输出被消费. 举例来说,大多数比特币交易均是采用接受者的公钥加密和私钥解密, 因而其对应的 P2PKH (Pay to public keyhash) 标准交易脚本中的锁定脚本即是使用接受者的公钥实现阻止输出功能, 而使用私钥对应的数字签名来加以解锁[53].    图2.4 P2PKH标准脚本模板    图2.5 Pay-to-ScriptHash (P2SH) 标准脚本模板    图2.6 m-n多重签名交易脚本模板  比特币脚本系统可以实现灵活的交易控制. 例如, 通过规定某个时间段 (如一周) 作为解锁条件,可以实现延时支付; 通过规定接受者和担保人必须共同私钥签名才能支配一笔比特币, 可以实现担保交易; 通过设计一种可根据外部信息源核查某概率事件是否发生的规则并作为解锁脚本附着在一定数量的比特币交易上, 即可实现博彩和预测市场等类型的应用; 通过设定N个私钥集合中至少提供M个私钥才可解锁, 可实现M-N型多重签名, 即 N个潜在接受者中至少有M个同意签名才可实现支付。多重签名可广泛应用于公司决策、 财务监督、中介担保甚至遗产分配等场景。  （3）基于区块链的网络信任基础设施  代币和脚本功能可以帮助区块链应用于分布式PKI[54]、去中心化的安全域名系统[55,56]、分布式安全存储系统[56]等去中心化的新型信任体制的网络信任基础设施。域名币（Namecoin）[55]是利用代币实现的第一个基于区块链的网络基础设施应用。它试图通过使用类似比特币的区块里来提供名称注册体系，用户可以把他们的名称与其它信息注册进这个公共数据库。其域名资产与比特币的交易示例如下图。    图2.7 域名转让交易  域名币独立于比特币建立公有区块链，在原有比特币脚本系统中增添了域名预定(NAME\_NEW)、域名注册(NAME\_FIRSTUPDATE)、域名更新(NAME\_UPDATE)三大脚本操作。当用户申请新域名，首先将相应额度的比特币转化为代币，NAME\_NEW将声称相应的域名哈希，存入代币脚本中，实现域名预定。之后，用户使用NAME\_FIRSTUPDATE，将域名及绑定的键值写入代币。后续使用NAME\_UPDATE实现域名键值的更新，以转移域名资产拥有权。域名币通过这样序列化状态操作，设定了域名注册管理策略，利用脚本实现域名的全周期管理。    图2.8 域名币系统的三大交易类型  域名币最大的用途被认为可以用来做 DNS 系统，把诸如“ bitcoin.org”的域名（在域名币体系里可能会是 bitcoin.bit）映射成 IP 地址。别的用途包括Onename[57]在线身份绑定服务，Certcoin[54]将PKI的操作放在记录单中，包括注册、更新、查找、撤销，另外如电子邮件认证和潜在的进阶信誉体系[58]。由于其独立于比特币建立新链，并使用替代币来实现交易，由于规模并不大，导致挖矿的安全性较低，该项目最终未能够获得足够的重大交易。  Blockstack[55]在比特币主链再次尝试利用区块链技术，来实现更为复杂和安全的去中心化域名管理系统，并且可以实现域名的交易。区块链也是包含内部所有信息的分布式数据库，因此是可信任的数据库（任何问题都可以选择多个用户进行验证）。所以区块链可以完美的保存域名服务器信息。Blockstack通过它的网络节点把基础设施建立在区块链上。区块链可以提供正式的账本用来存储公共信息，以及用来编辑信息的可编辑私钥路径。这些节点处理域名交易（每个节点包含各自域名的账本），域名所有人密钥对，以及记录解析后的域名（如IP地址）。网络上的域名交易包括登记、转移和数据升级。这些域名操作通过交易加密存储到底层区块链上（比特币的情况下，被转移的就是比特币）。  Blockstack利用虚拟链从比特币主链上提取域名交易，验证对<Name, Value>的相应操作是否合规，进而对数据库中的相应域名信息实现更新。Blockstack还可以利用键值作为索引，来存储更多的域名信息，有效解决了区块链数据存储能力不足的问题。   1. **域间路由安全机制**   作为域间路由的事实协议，边界网关协议（Border Gateway Protocol）设计之初是面向一个相对封闭、可控的网络范围，没有考虑安全可信的问题。但是随着计算技术、通信技术与应用模式不断进步，互联网已发展成为一个开放、不可控的复杂系统，网络层固有的脆弱性使得互联网的安全可信问题越来越严重。在BGP的控制平面，网络自治域之间对相互通告的路由信息缺乏认证和保护，因此BGP前缀地址劫持和路由篡改攻击可能造成网络瘫痪，使得有网不能通，用户无法正常链接网络。在数据平面，IP协议在分组转发过程中，缺乏对报文的认证、加密和完整性保护机制，因此报文嗅探、篡改、源地址欺骗以及DDoS等攻击可能造成网络混乱，使得有网不能用，用户无法正常使用网络。为了解决网络层控制平面的安全可信问题，学术界和工业界提出过多个路由协议安全机制，例如S-BGP[41,42]、So-BGP[43]、IRV[44]、OA[45]、SPV[46]、psBGP[47]、RPKI[18]、BGPSEC[48]和ROVER[49]。    图2.10 路由协议安全机制列举   1. 路由源认证   RPKI（Resource PKI）是由IANA（The Internet Assigned Number Authority）推行并已经实验性部署的用于构建一个支撑域间路由安全的互联网基础资源管理系统[44]，用于证书的发布以及对路由通告合法性的验证。该管理系统利用X.509公钥证书框架，为互联网的号码资源（包括IP地址和AS号码）颁发CA证书，将号码资源与其公钥绑定起来。然后，利用CA证书为终端实体颁发EE证书。当某个IP地址资源持有者(RPKI体系中的CA证书持有者)需要授权某个AS为其特定的IP地址前缀通告路由可达信息时，该IP地址资源持有者使用其持有CA证书对应的私钥签发一个EE证书，然后再用EE证书对应的私钥产生路由源声明（Route Origin Attestation，ROA）签名项。RPKI验证者通过验证ROA来判断一个AS是否被IP地址资源的持有者授权通告对应IP地址前缀的路由信息。  ROVER（Route Origin VERification）是由美国的Secure64公司[45]提出的利用反向域名解析服务以及DNSSEC提供的密码机制实现路由源认证的技术。ROVER通过计算IP前缀的反向域名，将一种称为安全路由源（SRO）的资源记录存储至该前缀域名指定的空间，并用DNSSEC对SRO记录进行签名，保证SRO的真实性。SRO记录包含一个存储AS号码的强制字段，该AS号码指示被授权发布SRO记录对应地址前缀的自治域。此外，ROVER还使用RLOCK记录路由源认证技术是否被此AS使用。ROVER路由源认证大致过程如下：当路由宣告者向邻居路由器宣告一段地址前缀时，邻居路由器首先通过反向域名解析服务查找地址前缀对应的域名，找到存储于域名服务器的对应SRO记录。如果RLOCK指示宣告源路由的AS使用了ROVER技术，并且找不到SRO记录或者SRO记录与宣告的路由前缀不一致，则说明发生前缀劫持攻击。因此ROVER具有RPKI所不具备的多个故障保护特性[46]。  针对RPKI的分析表明，使用RPKI进行网络号码资源保护，由于中央授权中心可以单方面收回IP前缀的授权，可能导致这一权利被政府滥用[48, 49]。Cooper等人通过理论分析，部署RPKI存在7个不同方面的缺陷，包括RPKI存在单方面回收的权利滥用，一个RPKI的authority可重写、删除自己发布的RC、ROA，因此可对自己的子节点资源实现秘密撤销等，必须引入辅助机制增加系统决策及信息的透明性。但是，由此带来的另外一个后果是RPKI也将变得复杂。另外，由于RPKI要求用户从服务器下载ROA和BGP路由表，可能会出现针对下载操作的DDoS攻击的发生[50]。  ROVER虽然缓解了RPKI设计缺陷造成的故障问题，但仍然需要集中式的DNSSEC作为公钥基础设施来实现证书存储和安全路由源记录，DNSSEC的安全性直接影响了ROVER实现路由源认证的安全性。  由此可见，依赖公钥基础设施实现证书下载验证令这些路由源认证机制复杂且存在安全缺陷，那么，考虑新型信任体系是否能实现非集中式的信任基础设施，来存放和通告可信的路由源记录，是打破现有集中式管理，更加高效安全地实现IP地址资源的分配与通告的未来方向。   1. 路由路径认证   S-BGP使用 PKI 技术来增强 BGP 安全性的最早的文献之一.通过建立一套用于证书发布和路由验证的 PKI,以及引入一种新的可选传递(optional transitive)路径属性,S\_BGP 构建了一个完整的解决 BGP 路由认证问题的架构。其安全机制主要建立在三个安全实施模块之上：PKI、路由属性证明和IPsec。S-BGP使用的PKI基于X.509 (v3)的扩展证书，以此来验证AS号码和IP地址前缀的持有者的身份和授权。路由属性证明模块完成对路由信息的数字化签名授权，主要包括地址证明和路由证明。地址证明来授权它管辖范围内的AS可以发起到该地址前缀的路由，而路由证明用来授权其邻居可以通告发布给它的路由。IPsec模块确保路由器之间点到点传输的BGP流量的安全。整体上S-BGP利用4种证书和两种证明成功地解决了路由认证问题，不过也相应地带来计算开销大、路径收敛时间延长的问题[47]，更加上建立PKI需要IANA、RIR、ISP以及路由器厂商的共同参与,致使 S-BGP 始终未能实际部署。  不同于S-BGP采用PKI证书来完成网络前缀、自治域号、路由器等与路由属性的绑定，So-BGP基于网状信任模型，可以依赖于VeriSign这样的知名认证服务提供商的公钥来认证。So-BGP设计了3类证书来实现路由认证：EntityCert，AuthCert (authorization certificate)和ASPolicyCert。其中，EntityCert 证书用于鉴定AS实体身份，AuthCert证书用于给AS提供通告一个IP地址块的授权，ASPolicyCert证书用于描述AS之间的拓扑连接关系。但是在So-BGP机制下，由ASPolicyCert证书建立的AS拓扑图，路由宣告者仅可以判断路由更新中的AS\_PATH路径是否存在，而无法确定该路径是否为真正宣告的路由路径。同时soBGP由于缺乏信任锚的地址授权认证体系，安全性显著地降低[59]。  虽然以上多个技术都在一定程度上对BGP协议提供保护，但都无法在增强安全与降低开销及部署难度方面取得平衡。虽然RPKI & BGPsec 作为 IETF 着力推广的 BGP 安全标准,其安全性如何还有待深入研究。目前已经有研究发现，RPKI 本身操作的不当会给路由安全带来不利的影响[61]。此外,有关 RPKI & BGPsec 标准本身可能存在的安全漏洞也正在讨论[79,80]。再者,该标准的增量部署将会导致 BGP 路由交换环境变得混杂，部署了 RPKI &BGPsec的 AS 与未部署该标准的 AS 同时存在于互联网,这极可能给攻击者以可乘之机，从而给 BGP 安全带来新的未知安全威胁。Lychev[60]等人通过安全分析以及实验证明，无论是S-BGP、So-BGP还是RPKI，在部分部署的情况下，存在由于部署了安全机制的路由器可能选择较高安全性的路由机制，即丢弃未部署相应安全机制的路由器宣告的路由更新的情况，可能导致路由黑洞的产生；即使已部署安全机制的路由器选择较为宽松的策略，接受未部署安全机制的路由器宣告的路由更新，也存在相应的攻击模型。研究表明部分部署域间路由安全机制可能反而导致路由安全性整体下降。此外，一个不容忽视的问题是安全机制的部署可能带来路由效率降低，Wahlisch等学者通过对Alexa选取1M个域名进行分析，指出部署了RPKI机制导致网站的服务质量严重恶化[64]。  从增强安全与降低开销间的平衡角度考虑，将无需证书的身份基密码应用于域间路由路径保护机制是一个行之有效的解决方案。国内信息工程大学[81]基于身份域间路由协议提出基于身份聚合签名体制的AS\_PATH真实性验证机制IDAPV。IDAPV采用与S-BGP相同的验证思路，不同之处是，IDAPV采用基于身份的聚合签名体制聚合AS\_PATH中所有AS的路由证明成一个路由聚合证明。聚合签名体制是指聚合n个不同用户分别对n个不同消息的签名成一个聚合签名，验证者只需验证这个聚合签名的正确性就能保证n个初始签名的正确性。但是聚合签名无法验证聚合签名的顺序，即只能验证签名是AS\_Path上的所有AS集合签出的，并不能验证AS\_Path本身的正确性，无法避免路径乱序攻击。  现有域间路由路径安全认证研究都不能实现增强安全与降低开销兼得，如何设计一种摆脱证书管理与复杂验证，又能保证安全性的路由路径认证方法，将能大大提升路由安全机制的可部署性。   1. **身份基公钥密码体制**   身份基密码体制的思想最早由Shamir于1984年提出[1]，其核心目标是将一个主体的公钥与他的身份消息结合起来。在主体的公钥本身显然与该主体的身份信息如名字、电子邮件等附属信息相联系的前提下，公钥基础设施的复杂度和建立与维护公钥密码认证框架的代价将大幅度减小。由于在提出之后，一直无法找到相应的数学工具为其提供支持，在将近20年的时间里，基于身份的公钥密码学仅停留在设想阶段。直到2001年，Boneh和Franklin[2]应用椭圆曲线上的双线性对技术，才建立了第一个实用的基于身份的公钥密码体制BF-IBE，该体制完全满足Shamir所声称的身份基公钥密码系统。BF-IBE利用椭圆曲线构造一个加法群，并将用户的身份标识，即一个任意长度的字符串，经过通用的算法映射到该椭圆曲线群上的某一点，选取该点作为此用户的公钥。身份基密码体制需要专门的密钥生成机构(PKG)为用户生成私钥。在BF-IBE中，PKG选择一秘密值作为系统主密钥，通过将主密钥与用户公钥相乘即得到用户的私钥。用户结合PKG发布的公共参数，利用双线性映射，完成信息的加密和解密。Boneh和Franklin给出了该方案的安全性的形式化证明：在随机预言机模型下，BF-IBE可抵抗可抵抗不可区分自适应选择密文攻击。此后，Sakai和Kasahara[3]同样基于椭圆曲线群上的双线性映射，提出了另一种IBE方案，简称为SK-IBE方案。该方案针对双线性对映射计算开销大的问题，实现具有较少双线性对映射计算量的签名/验证机制，有效地提高了身份基密码体制的签名/验证效率，但是在某些场景，比如层次式IBE的应用上，SK-IBE的性能和安全性并不如BF-IBE。McCullagh[4]则提出了另外一种私钥生成方案（MC-IBE方案）。该方案中，PKG将用户的身份，即某一个任意长度的字符串，通过一个公开的哈希算法映射为某一数值，与PKG的主私钥相加之后求逆，再与该PKG所选椭圆曲线群的生成元相乘，所得结果即为该用户的私钥。但是该方案的目的主要是为了密钥协商时更加简便，没有设计成熟的加密/解密机制以及签名/验证机制，应用的范围不广。虽然此后的研究还提出许多可抵御不同形式化攻击的基于双线性对[5, 6]以及基于双系统加密的身份基密码体制[7, 8]，目前比较完整的身份基密码体制还是基于BF-IBE建立。围绕BF-IBE方案，有关学者设计了高效的签名和认证方案[9, 10]，形成了一套较为完整的身份公钥密码体系。经过长期的研究和实践，2009年国际标准化组织将该方案标准化为RFC5408[11]。最近，国内学者曹珍富[12]又提出BF-IBE的改进方案M-IBE，增强原方案的可扩展性，使其应用范围更广。在身份基密码体制的基础上，Horwitz[13]提出层次化的IBE(HIBE)方案，通过高层级用户为低等级子孙用户生成私钥，有效解决IBE中私钥生成器负载过重、规模扩展受限等问题。但是，该HL-HIBE机制无法抵御子PKG串谋获取根PKG主密钥的攻击，无法直接应用于具体场景。Gentry和Silverberg提出的GS-HIBE方案[14]，通过根PKG选取主密钥，域PKG选取子密钥，共同参与生成用户私钥的方式，实现随机预言机模型下形式化证明安全的层次化身份基密码机制，包含有效的加密/解密、签名/验证算法。  身份基密码体制大规模使用面临一个主要问题是如何解决密钥撤销问题。由于身份即公钥的设计特性，身份基密码不能像PKI体制中通过剥夺公钥的合法性来作废非法用户的使用权，通过公钥撤销列表来标记和公示已撤销的密钥。为解决密钥撤销和更新问题，文献[2]提出消息的发送者在进行加密时可将当前的有效时间添加到身份信息中，并且消息的接收者周期性地获得新密钥, 要撤销某个用户，私钥生成中心停止为其发布更新密钥，只为其他用户产生更新密钥。这使得私钥生成中心工作量和用户数量成线性关系，并且可信中心需要与每一位非撤销用户建立安全信道来发送更新后的密钥。Boldyreva等人[72]给出了一个选择性安全的可撤销的基于身份的加密(Revocable Identity BasedEncryption, RIBE)方案，使得可信中心执行非撤销用户的对数级别的工作量，这有效地减轻了可信中心的负担，并且首次获得非交互的密钥撤销，发送者和接收者的效率也得以有效提高。然而，安全性证明仅在选择身份模型下实现的。在Boldyreva等的基础上，Libert和Vergnaud[73]提出了完全身份下的解决方案。锁琰等[74]提出一种基于密钥隔离的分布式群签名方案，但是需要分布式协助器帮助群成员完成密钥更新。另外，TsaiT．T等[75]提出一个安全的具有可撤销功能的基于身份签名方案，并在标准模型下给出安全证明。  可撤销的基于层次身份加密 (RHIBE)由于其层次性的密钥生成和有效的用户撤销，能够实现高效的动态用户安全管理。在可撤销的IBE方案中，利用完全子树方法(Complete Subtree, CS method) [66]，KGC生成更新密钥的负载大小仅与用户数量呈对数上升。但是这种方法如果直接引入RHIBE 并不有效，它将使得用户密钥大小与其所在层次深度成指数上升。在RHIBE方案中，每个周期更新密钥的大小以及用户私钥大小共同决定了用户撤销的效率。Seo 和Emura 提出了一个可撤销的 HIBE 方案[67]，虽然私钥大小已经与系统最大层次深度成多项式关系，其密钥更新很复杂。他的基于历史信息的更新方法使得更新密钥中携带过长的历史更新信息，并且需要递归式地生成私钥和更新密钥。这类密更新方法效率低，是不可取的。Lee的RIBE方案[68]用到了另一种撤销方法称作子集区分(subset difference, SD method)，同样也被用来构造RHIBE [69]. 虽然这种方法相比CS方法在通信开销上有更高效率，但会使得私钥更大。  现有的大多数RHIBEs 都受限于其系统管理层次，它们都必须在初始化阶段设定系统所能承载的最大层次用户身份的深度,也就是说他们需要在初始化阶段在系统公钥中声明系统所能承载的用户最大层次深度。一般来说正确设定合适的最大层次深度极其不易，用于用户的动态性递增性，在实际应用中很容易出现设定的过小不足以容纳足够多的用户，过大又造成身份空间不必要的浪费和生成密钥时不必要的计算量。因此层次受限的 RHIBE 不具有可拓展性。Ryu[70]提出一个层次不受限(unbounded)的 RHIBE 方案，但是它只具有选择性安全(selective-ID security)。所幸Lewko and Waters [71]提出过一个层次不受限的 HIBE 并且具有完全安全性，他们的方法可以借鉴来构造一个完全安全的层次不受限RHIBE。 |

3.研究内容

|  |
| --- |
| **3.1研究目标**  本课题将系统地研究新型信任体系下的路由安全机制以及相关关键技术，主要研究目标包括（1）避免集中式信任的地址资源安全通告，提出一种去中心化的网络地址资源分配与安全通告方法，能够做到避免现有方案存在通告地址段重叠的缺陷，实现地址资源灵活安全的分配与通告，并解决现有方案部署难的问题，实现一个可实际部署的网络资源安全分配通告的区块链应用；（2）提出一种基于层次身份基密码的路由路径通告授权机制，同时面向密码可撤销的应用需求，设计出可撤销的层次IBC加密及签名方案，最终实现只需一个HIBS签名的低存储低开销的BGP安全通告方案，从计算效率和存储效率上提升BGP安全机制部署的可行性。（3）面向BGP报文安全认证，提出可撤销的高效IBC加密及签名方案，提高签名运算和密钥更新的性能，以满足实际网络计算效率需求。 |
| **3.2主要研究内容及拟解决的关键科学问题和技术问题**    **3.2.1 基于区块链的路由源安全通告研究**  依赖集中式信任机构的路由源安全通告方案往往存在不透明，缺乏审计，易滥用的缺陷，且基础设施易遭受攻击的不足，因此，课题拟借鉴比特币的去中心化信任和不可更改交易记录的优势特点，开展基于区块链的地址资源分配与路由源安全通告研究。   1. **基于区块链的网络地址资源分配及安全通告方法**   利用区块链去中心化的可信数据存储机制，建立地址资源交易的公有链，实现AS级地址资源的分配与审计，实现地址资源归属的去中心化安全通告。具体内容包括：  （1）研究基于区块链交易的网络资源分配方式，包括地址分级管理机构的交易角色及交易类型等基本定义，实现地址分配机构、AS自治域等角色与交易钱包地址的映射和信息发布，实现分配交易提交和审计；  （2）研究区块链分配资源的通告模式，解决域间路由如何获取可信的前缀通告信息的问题，实现路由源安全认证。  拟解决关键技术问题1：区块链如何实现地址资源的分级管理；  拟解决关键技术问题2：基于链上交易的地址资源分配如何要能够实现IP前缀灵活分割与聚合。   1. **基于链上交易的网络地址资源信任分配机制**   利用区块链交易实现地址资源分配，需能对应现实地址资源分配各类情况，提供完整语义记录。因此课题研究基于链上交易的资源分配实现机制，具体内容包括  （1）研究基于区块链的地址资源交易模型及实现方法。由于地址资源相当于链外资产，与货币链上流通存在不同的交易属性，包括 (a)交易对象不同：地址资源不同于货币，相同额度的比特币并无差别，而每个IP地址都是独一无二的；(b)交易语义不同：电子货币交易一旦完成不可撤回，属于买卖，而地址资源分配是有时效的，属于租赁。因此需要研究区块链资产交易功能的实现方式，构建网络地址资源交易模型和交易实现方法。  （2）研究地址资源回收机制。地址资源使用权的租赁式交易必然存在到期回收，另外在对突发大规模网络攻击采取防御措施时也需要实现地址资源使用权的即时撤销。因此需要研究如何利用区块链交易的输出脚本功能，定制地址资源分配的相关策略，实现地址资源的灵活的分配与撤销。  拟解决关键技术问题1：网络地址资源的链上交易模型定义  拟解决关键技术问题2：如何在区块链上实现已分配资源的到期回收和即时撤销。   1. **部署设计与评估**   开发区块链应用，设计选取包括挖矿激励、共识算法、挖矿难度等指标。从IRR数据库、RPKI证书库等获取公开的前缀通告数据，开展模拟实验。从可扩展性、安全性角度，评估区块链用于网络资源管理的可行性和可部署性。  拟解决关键技术问题1：如何解决区块链挖矿的可扩展性问题，以适应全网范围内IP前缀声明的变化速度；  拟解决关键技术问题2：如何实现增量部署，以提高方案可行性。  **3.2.2 基于自证明标识的路由路径安全认证研究**  目前研究提出的域间路由安全机制普遍存在的问题是机制复杂，需要构建庞大的安全认证机构，路由验证需要与认证机构进行交互。同时，在部分部署甚至是完全部署的情况下，各种路由安全机制都存在可被利用发动新形式攻击的机制副作用。针对域间路由协议BGP缺乏认证机制的设计缺陷，课题拟通过基于身份基信任体制下的自证明实体，实现路由更新中更新消息的合法性认证，主要为路由路径认证。自证明实体包括自证明地址以及自证明路由宣告者，实现安全的路由机制，主要研究路由更新的路径认证，提出一种既能避免安全缺陷又能提高计算效率的安全域间路由机制，进行基于自证明实体的路由路径认证机制设计，包括设计路由认证书，实现安全的路由授权和无交互的高效的路由认证。   1. **基于自表示层次标识的路由路径授权通告与安全认证机制**   路由通告授权是安全路由必不可少的机制，如果没有授权及验证机制，即使BGP安全机制能够保证BGP报文的完整性，部署有安全机制的单个恶意路由也可以通过截取监听到非邻接AS路由发布的BGP安全报文，并利用自己的密钥附加新签名并充当下一跳，实现路径篡改和虚假路径通告，即便它也是受完整性保护的。针对路由通告授权，以往的路由安全通告如BGPsec和S-BGP通过向签名报文中加入下一跳信息来实现，具体是通过不断附加各跳签名来实现后续节点对当前路径上每一跳的授权验证，同样也有身份基域间路由安全协议利用相似的嵌套签名或者聚合签名来实现授权与认证。这些方法虽然同时实现了授权和认证，但由于签名方法的低效性，其验证仍然是复杂的。  课题提出基于层次密钥分发的路由通告授权机制，我们以路径即层次身份即公钥为出发点，利用路径标识的密钥分发实现授权。不同于嵌套签名需要层层验证签名，也不同于聚合签名要利用多个公钥验证，这里只需一个密钥进行一个签名即可实现路由授权和路径安全通告，相应的只需对单个签名进行验证即实现路由路径的安全认证。  拟解决关键技术问题1：针对每个前缀通告，源AS作为根PKG实现层次密码系统，其系统公共参数如何发布，如何保证公共参数可信。  拟解决关键技术问题2：如何考虑两个恶意路由器串谋下的安全性。  拟解决关键技术问题3：如何选择合适的层次身份基签名，降低报文存储，提高计算效率。   1. **面向路径通告授权的可撤销层次IBC加密及签名**   针对路由通告授权，提出一种基于层次身份的可撤销加密及签名方法，要求身份层次不受限，以满足路径通告长度不受限的要求，能够防止路径乱序攻击，方案达到自适应安全。  拟解决关键技术问题1：层次不受限的身份基加密是一类特殊的函数加密应用，证明难度大。如何设计多个高度混合的挑战游戏的不可取分证明，来适应层次不受限HIBE中系统公钥参数信息熵源不足的问题。  拟解决关键技术问题2：在没有层次不受限的HIBS可参考下，如何设计出能够有效证明的层次不受限RHIBS。   1. **面向路由安全认证的可撤销的高效IBC加密及签名机制**   基于层次密钥分发的路由通告授权可能存在虚假授权的风险，为了避免不诚实地路由授权行为，需要AS利用自己密钥进行报文签名，向下一跳证明授权行为确实由我发起。课题拟利用身份基密码来实现AS的签名认证，AS持有基于ASN为身份的密钥进行签名，可实现无需证书的高效验证。考虑到身份基密码应用需要解决密钥撤销的实际需求，对全球不断变化的AS使用情况，AS分配机构需要实现灵活的密钥更新。因此，课题为实现路由报文的高效安全认证，提出一种可撤销身份基加密及签名方法，实现高效的密钥更新，实现高效的密钥生成与签名计算，方案达到自适应安全。  拟解决关键技术问题1：AS分配机构进行密钥更新的工作量如何能从线性降低到指数级？  拟解决关键技术问题2：课题拟使用指数逆结构来实现高效密钥生成，但其构造不易扩展，如何解决基于指数逆结构的IBC方案不易扩展的内在缺陷，将其拓展到可撤销的IBC方案？  拟解决关键技术问题3：指数逆IBC的安全性证明较复杂，达到自适应安全要求，需要寻求新的证明框架。 |
| **3.3 拟采取的研究方法、技术路线、实施方案及可行性分析**  **3.3.1 研究方法**  课题分为两大部分，第一部分属于应用创新，首先要学习现有区块链应用方法，针对区块链应用研究，密切跟踪国内外的研究形势，以全面了解国内外的最新发展动态；其次，针对自己要实现的区块链应用，广泛搜集资料以掌握要实现背景及功能语义，从形式化抽象的数学模型开始，对要实现的机制进行深入分析研究；最后在构建应用原型及开展实验验证时, 首先对可借鉴的区块链应用系统进行功能和代码分析，加深区块链应用底层实现的了解，然后开展原型设计与功能性验证，并利用收集到的测试数据，实现与现有方法的对比实验与分析。  第二部分属于方法创新，特别需要过硬的密码基础，因此平时注意多学习一些数学和计算机理论知识，努力扩大自己的知识面。深入分析研究中遇到的理论问题，通过对问题进行形式化抽象出数学模型，广泛学习和借鉴现有的证明方法，从理论上给出验证或证明。实验遵循由易到难，先简单后复杂的原则。首先快速搭建原型系统，对自己的算法进行验证和评测。如果想法可行且效果也不错，那就继续完善；否则，立刻改变思路，迅速尝试其他的方法。实验数据一定要做到真实有效。  另外，要有针对性地与国内外研究小组进行学术交流，并建立经常性的联系；积极参与国内外相关的学术会议，多发表学术论文，促进本课题研究的进展；多向课题组老师请教，保证研究方向上的正确。  **3.3.2 技术路线和实施方案**  **（1） 基于区块链的网络地址资源分配及安全通告方法**  （a）研究基于区块链交易的网络资源分配方式  互联网数字分配机构IANA(Internet Assigned Numbers Authority)作为全球地址资源管理中心负责IP地址段的分配，另有5个分支机构分别负责欧洲、亚太地区、美国与其他地区的IP地址资源分配与管理。这5个机构是： RIPE（即设在比利时的Reseaux IP Europens)，负责整个欧洲地区、中东和中亚的IP地址资源分配与管理； APNIC（即设在澳大利亚的Asia Pacific Network Information Center），负责亚洲与太平洋地区的IP地址资源分配与管理；ARIN（即设在美国的American Registry for Internet Numbers)，负责美国与其他地区的IP地址资源分配与管理，LACNIC(Lation American and Caribbean Internet Address Registry),负责拉丁美洲和一些加勒比群岛，AfriNIC负责非洲地区业务。另外，许多国家和地区都成立了自己的域名系统管理机构，负责从前述3个机构获取IP地址资源后在本国或本地区的分配与管理事务。  这样的层次地址资源管理可以通过区块链交易来记录完成，通过矿工的交易验证可实现分配操作的正确性和政策性审计，只要IP资源申请者出卖一定数额的奖励费用。根据各层地址分级管理机构的职能角色，我们给出如下管理结构。    图3.1全网地址资源的层次管理结构  进而定义交易角色及交易类型。课题拟通过设计五类交易类型及操作约束，来实现层次地址资源管理语义。每种交易操作有其特定的实施角色、作用对象和操作触发约束。例如IP\_ Distribute操作的地址资源必须首先有IANA通过IP\_Register实现链上资源注册，或者已分配该地址资源的上级管理机构发起，向低一级的地址管理机构分发。  表3.1 交易类型与功能定义   |  |  |  | | --- | --- | --- | | 交易操作 | 实施角色 | 功能 | | IP\_Register | IANA | 全球网络管理机构注册IP资源 | | IP\_ Distribute | IANA、xIR(RIR/NIR/LIR) | 将IP块资源分发给LIR/NIR国家或地区网络管理机构 | | IP\_Allocate | xIR、ISP/子ISP | 将IP块资源“分配”给自治域AS | | IP\_Update | xIR、ISP/子ISP | 地址通告权更新 | | IP\_Revoke | xIR、ISP/子ISP | 地址通告权撤销 |   进一步，基于链上交易的地址资源分配可以实现IP前缀灵活分割与聚合。域名币没有考虑域名类似的功能，它不支持域名的层次语义。但针对本课题应用，由于IP地址块代表一定数量IP地址的集合，可分为几个前缀更长的IP块，在地址资源分配中需要实现地址资源分割，以保证每一个IP都在链上属于唯一通告的有效IP块及拥有者，这是RPKI没有做到的。同时，当某个分配机构或者AS拥有可聚合的多个IP前缀，也可通过交易重新聚合，压缩有效通告的数量，提高通告效率。    图3.2 基于区块链交易的灵活地址资源分配  （b）研究区块链分配资源的通告模式  区块链作为全局统一的地址资源分配可信记录源，如何获取区块链上正确合法的通告信息是边界路由器实现非法前缀通告过滤的最后一步。考虑到路由器本身性能局限，下载区块链实现本地验证并不实际，课题考虑AS可向自治域内矿工申请同步全网实时前缀通告，并发布给边界路由器，以实现路由源安全认证。  **（2）基于链上交易的网络地址资源信任分配机制**  基于区块链的地址资源交易模型主要分为资源分发(对应IP\_ Distribute操作)和资源租赁(对应IP\_Allocate操作)两种，如下图。当全球(洲) 地址资源管理中心A向国家(地区) 地址资源管理机构B分发地址资源时，IP令牌的所有者变更，实现地址资源分发。当国家级地址资源管理机构NIR或网络供应商向自治域AS分配IP前缀通告权时，IP令牌的键值变化，令牌所有者不变。在链上交易中，AS自始至终没有拥有IP资源，而是上层管理者来声明AS的通告权。这样，地址资源的所有权保留在管理机构手中，通过更新资源键值，让渡地址资源使用权，有效实现基于区块链交易的地址资源租赁。   |  |  | | --- | --- | |  |  | | 1. 地址资源层级分发 | 1. 地址资源“分配” |   图3.3 地址资源链上交易模型  课题通过IP\_revoke来有效实现地址资源回收机制，管理机构有权更改资源通告声明，实现AS通告权的即时撤销。另外可参考域名币，规定若干区块后，如果没有针对某地址段的新的交易产生，该资源通告会自动过期，归入IANA保留的未分配资源中，若要启用，则需IANA重新注册。  表3.2 链上交易功能实现   |  |  |  |  | | --- | --- | --- | --- | | 交易操作 | 实现语义 | 代币交易内容 | | | IP\_Register | 将注册IP块写入等额比特币，实现链上代币转化 |  | | IP\_ Distribute | 链上代币交易，实现IP资源的分发 |  | | IP\_Allocate | 将AS号赋与IP资源键值，声明通告权 |  | | IP\_Update | IP资源键值更新，让渡通告权 |  | | IP\_Revoke | IP资源键值删除，收回AS通告权 |  |   依据区块链交易及验证原理，课题定义脚本操作功能的基本实现方法，如上表所示，给出了五类交易操作的实现内容。每个操作通过区块链脚本来实现分配语义，矿工在验证交易时验证相关的触发条件，若符合操作约束则接受交易，写入区块。以IP\_ Distribute为例，其交易scriptPubkey语句设计如下图所示。    图3.3 地址资源分发操作的scriptPubkey脚本  针对OP\_IP\_DISTRUBUTE操作，矿工验证工作包括：（1）检查当前钱包拥有者是否为IANA且上一交易操作是OP\_IP\_ REGISTER，（2）若否，则检查本交易的上一交易输出脚本是否为OP\_IP\_DISTRUBUTE，（3）若否，则拒绝交易，（4）若真，读取地址块<IPB>并对比上一交易的metedata，（5）若不一致则拒绝交易，若一致则接受交易，写入区块。  **（3）基于自表示层次标识的路由路径授权通告与安全认证机制**  不同于一般的S\*BGP思想采用每跳路由对AS\_PATH进行签名来实现路径授权和认证方法，课题从“路径即标识即公钥”的思想出发，任何一个时刻BGP通告报文中只需存一个以路径AS\_PATH为公钥的签名即可证明AS\_PATH本身的真实性。  令第n跳的AS\_PATH=，每个有效的IP前缀都有前缀主密钥MK，在分配前会全网公布前缀公钥参数PP用于验证前缀通告。当IP前缀分配给源路由时，会为其生成并发送一级密钥，此密钥为关于前缀主密钥MK和ASN号码的函数，密钥赋予了授权邻接AS继续通告该路由的权利。当要授权继续通告该路由，的操作就是利用自己的一级密钥和第二跳的ASN号码生成二级密钥并分发给。每一个被授权的AS都可利用自己分发得到的密钥来签名报文，任何人只要利用前缀公钥参数PP来验证签名是否为公钥所签的名，即可验证当前路径是否为合法通告。由此，该方案实现了路径授权与认证。    图3.4 具体安全通告流程  基于自表示路径标识的签名实现的路由认证，路由宣告者的对等路由器无需与框架中的认证中心进行交互，即可获得 IP 地址块以及路由宣告者的公钥，进行签名验证，与现有的路由安全机制相比，极大减小通信以及存储开销。  表3.3 初步性能分析   |  |  |  | | --- | --- | --- | | 工作量比较 | 本方案 | BGPsec方案 | | 证书下载 | 无 | O(k) | | 证书验证 | 无 | O(k) | | 签名验证 | O(1) | O(k) | | 密钥分发 | O(1) | - | | 加密传输 | √ | √ | | 签名 | O(1) | O(1) |   以上基于自表示层次标识的路由路径授权通告的实现与部署依赖于三个问题的解决：（1）如何利用层次身份基签名方案实现密钥分发和路由路径签名，（2）签名验证所需的IP前缀公钥参数如何全网公开获取，（3）基于层次密钥分发的授权是否可能出现新的安全问题并如何解决。  第一个问题需要考虑密钥和签名的时效性，以避免重放攻击和密钥非法重用，还要考虑到路由通告长度无法预测的现实情况，在签名方案设计时要求作为层次身份的路径不能预设长度限制。这些要求我们提出一个面向路径通告授权的层次不受限的可撤销层次IBC加密及签名，即下一部分的研究内容。  第二个问题要考虑到公钥参数必须真实可信，若利用原有证书方式来实现则需引入新的PKI系统，所以，课题考虑利用第一部分研究内容所提出的基于区块链的路由源通告基础信任设施，不仅完成IP前缀与AS的绑定信息的通告，还负责通告相应的前缀公钥参数。这样既无需增加新的证书系统，又能实现全网前缀公钥参数的可信通告，即拓展第一部分内容。  第三个问题针对可能出现的非法或虚假授权，需要细致考虑保护机制。第一种非法授权的实现方式为路径上某一恶意AS向非邻接AS发布路由通告，若此AS为诚实中继AS，则可直接根据通告策略发现来自非邻接AS的错误通告而过滤，若为串谋AS，则需要再下一跳AS通过验证串谋AS是否与恶意AS存在邻接关系来过滤通告，因此需要添加链路证明机制。第二种虚假授权指的是不诚实地路由授权行为，例如路径上的某恶意路由直接向某一目标AS伪造一条从其邻接AS发出的路由，由于此恶意路由可直接分发该虚假路径对应的身份基密钥，可绕过非法授权保护机制，那么我们采取路由认证方法，要求每个AS利用自己密钥进行报文签名，向下一跳证明授权行为确实由我发起，而非仿冒者发的虚假路由。课题拟利用身份基密码来实现AS的签名认证，AS持有基于ASN为身份的密钥进行签名，可实现无需证书的高效验证，即最后一部分研究内容。  需要注意的是，增加的路由认证签名只需保留一跳，也即每跳路由只需要多增加一个签名，多验一个签名，因此本方案的域间路由安全机制仍然保持每个路由O(1)量级的性能开销。  **（4）面向路径通告授权的可撤销层次IBC加密及签名**  路由通告授权机制需要层次身份基密码方案做支撑。为满足路径通告长度不受限的要求，课题提出一种身份层次不受限的层次身份基可撤销加密及签名方法，在一开始无需设定系统的最大层次深度，拓展更灵活，更重要的是，层次密钥签名可天然地防止路径乱序攻击。  课题拟参考并简化Lewko和Waters的层次不受限HIBE方案，使用无状态更新方法[4]衍生出一个可拓展的层次不受限的RHIBE。在这个方案中，用户私钥是直接生成，与父节点更新生成的解密密钥无关, 与系统主密钥也无关. 因此未被撤销的用户它的私钥大小与所在层次深度从多项式相关降为线性相关，同时系统公钥大小固定，不像已有可撤销层次方案那样随用户层次深度呈线性增长.  与传统的双系统加密以及嵌套双系统加密不同, 我们设计一个全新的嵌套双系统，不仅能够克服层次不受限(R)HIBE中固定长度的系统公钥提供信息量十分有限的难题, 同时也能够处理RHIBE中解密密钥有多种挑战方法的特殊情况，由此试图完成第一个面向层次不受限的RHIBE的嵌套双系统，并且证明不论解密密钥是由挑战所得私钥与更新秘钥计算得到还是直接由挑战获得，都没有信息泄露。  然后通过一系列挑战游戏的混合区分来证明U-RHIBE双系统加密的安全性. 由于在低信息量情况下通过嵌套双系统完成挑战游戏的无区分等价转化仍然是一个复杂的过程, 我们拟构造六个预言机通过混合步骤来最终实现不同挑战游戏间密文和三类密钥分布特性的改变。 通过复杂的挑战游戏的转化, 可证明U-RHIBE能够依据合数阶双线性群的安全假设获得标准模型下的自适应身份安全。  **（5）面向路由安全认证的可撤销的高效IBC加密及签名机制**  要实现BGP报文认证，需首先给AS分发以AS号为身份的密钥，由于AS分配是各洲平行分配（实际上AS分配由国家NIC如CNNIC自行分配，并在分配AS号前需在洲级NIC如APNIC的Whois 数据库中注册），因此在AS注册时，洲地址管理机构验核批准使用AS号的同时也分发合法密钥。此后定期向AS持有机构发送更新密钥以实现AS号的续用或撤销。当AS向外发布BGP通告时，AS的边界路由器利用密钥实现BGP报文签名，用于后一跳的报文认证。由于路由器处理报文的存储与计算能力有限，这对所用的RIBS方案有较高的要求，课题拟采用指数逆结构实现高效的可撤销身份基密码方案，以满足实际部署的性能要求。  方案拟利用模糊基于身份加密(Fuzzy IBE)的构造方法，私钥与更新密钥采用相同的构造形式，即私钥sk为，更新密钥uk为。进而计算身份与时间的拉格朗日系数，在解密时分别对身份密文与时间密文用拉格朗日系数作幂，解密计算时实现相消。  在证明方法上，方案基于合数阶(composite-order)群构造，采用标准子群判定问题，归约的安全性强于非标准q-SDH(strong Diffie-Hellman inversion)问题。然后利用Deja Q[51]框架实现问题归结，免去原始指数逆证明的复杂过程。实现基于混合挑战游戏(Hybrid Game Sequence)的安全证明。最终方案能够获得标准模型的自适应安全。    图3.5 基于混合挑战游戏的RIBE安全证明  **3.3.3 可行性分析**  当前基于区块链的资源管理应用已有成功部署的案例，可为课题方案的设计开发提供有效参考，基于身份基密码的域间路由安全增强机制也因其无需证书的优势引起了学术界的讨论研究，有助于课题方案的横向对比设计，而作为IETF标准的RPKI+BGPsec的域间路由增强方案的缺陷和部署问题在近年各大顶会均有讨论，有助于课题方案的纵向对比完善。  指导老师长期从事网络路由和信息安全方面的研究，在大方向上能给予有效的把握和指导。教研室的老师经验丰富，具有很高的从事跨学科研究水平和指导，本人具有相关的课题研究经验、理论基础和时间，这是本课题能按时完成的保障。总的来说，本课题的总体研究方向清晰，具有足够的理论、技术积累，是可行的。 |
| （4）预期创新点  本课题的预期创新点包括：   1. 提出一种基于区块链去中心化信任的网络地址资源可信管理方法，实现网络地址资源的可信租赁及撤销。 2. 提出一种基于层次标识密码的路由通告授权机制，实现一个签名的低存储低开销的BGP安全通告方案，从计算效率和存储效率上提升了BGP协议安全增强机制部署的可行性。 3. 提出一种具有自适应安全的基于不受限层次标识的可撤销加密及签名方法，用于路由通告授权。 4. 提出一种基于指数逆构造的高效可撤销身份基加密及签名方法，用于路由通告报文的安全认证。 |

4.研究条件

|  |
| --- |
| 开展研究应具备的条件及已具备的条件，可能遇到的困难与问题和解决措施。  本课题研究应具备的条件：   1. 充足的文献资料来源，包括上网查阅、调研、图书馆等途径； 2. 良好、可靠的试验设备和环境； 3. 良好的上网环境。   目前已具备的条件：   1. 由于长期从事计算机技术的学习和科研，对计算机网络、路由协议等相关知识具有较为扎实的基础； 2. 网络所设有高性能网络与通信技术实验室和网络攻防对抗实验室，拥有大量先进设备、完善的网络基础设施和良好的科研环境； 3. 最近收集并整理的国内外在相关领域的研究论文和资料，可以开拓思路，了解最新的研究成果； 4. 有项目小组经常内部讨论交流。   可能遇到的问题及解决措施：   1. 研究问题的深度不够。这个问题的解决措施是：深入研读领域论文，多向导师，教研室老师汇报自己工作，听取老师意见。 2. 关键技术问题难以攻克。这个问题的解决措施是：本着拿来主义精神和艰苦奋斗的作风，多方面寻求帮助，向领域专家咨询。保持充足的精力，用勤奋弥补自身条件和环境的不足。 3. 课题范围很广，设计计算机领域内的多个经典问题，每个研究内容都有不同背景，需要大量的前期积累，而研究时间有限。这个问题的解决措施是：认真分析课题的各个方面，抓住问题的主要矛盾，尽自己最大的努力在有限的时间内解决最核心的问题。 4. 论文遭拒，情绪低落。做好充分的心理准备，论文被拒是很正常的事情，要有屡败屡战的精神。论文被拒实际上是一次对自己水平提升的机会，论文被拒后，根据修改意见，认真分析原因，做到更好。 |

5.学位论文工作计划

|  |  |  |
| --- | --- | --- |
| 起讫日期 | 主要完成研究内容 | 预期成果 |
| 2016.5-2016.11 | 可撤销层次身份基密码研究 | 2篇论文 |
| 2016.12-2017.2 | 高效的可撤销身份基密码研究 | 1-2篇论文 |
| 2017.3-2017.8 | 域间路由安全机制研究 | 1-2篇论文 |
| 2017.9-2018.2 | 基于区块链的地址资源分配研究 | 2-3篇论文 |
| 2018.3-2018.9 | 撰写毕业论文 |  |
| 2018.10-2018.12 | 修改论文，答辩 |  |

注：每个子阶段不得超过3个月；预期成果中必须包含成果的形式、数量、质量等可考性指标该计划将作为论文研究进展检查的依据。

6.主要参考文献（博士不少于50篇、外文不少于25篇，硕士不少于30篇、外文不少于15篇，可附页）

| 序号 | 文献目录（作者、题目、刊物名、出版时间、页次） |
| --- | --- |
| [1] | A Samir. Identity-based cryptosystems and signature schemes [A]. Advances in Cryptology-Crypto 1984 [C]. LNCS 0196, Berlin: Springer-Verlag, 1984. 47-53. |
| [2] | D Boneh, M Franklin. Identity-based encryption from the Weil pairing [A]. Advances in Cryptology-Crypto 2001[C]. LNCS 2139, Berlin:Springer-Verlag, 2001. 213-229. |
| [3] | Sakai R, Kasahara M. ID based Cryptosystems with Pairing on Elliptic Curve. [J]. IACR Cryptology ePrint Archive. 2003, 2003: 54. |
| [4] | McCullagh N, Barreto P S. A new two-party identity-based authenticated key agreement [M] // McCullagh N, Barreto P S. Topics in Cryptology–CT-RSA 2005. Springer, 2005: 2005: 262–274. |
| [5] | Boneh D, Boyen X. Efficient selective-ID secure identity-based encryption without random oracles[C]//Advances in Cryptology-EUROCRYPT 2004. Springer Berlin Heidelberg, 2004: 223-238. |
| [6] | Boneh D, Boyen X. Efficient selective identity-based encryption without random oracles[J]. Journal of Cryptology, 2011, 24(4): 659-693. |
| [7] | Waters B. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions[M]//Advances in Cryptology-CRYPTO 2009. Springer Berlin Heidelberg, 2009: 619-636. |
| [8] | Lewko A, Waters B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts[M]//Theory of Cryptography. Springer Berlin Heidelberg, 2010: 455-479. |
| [9] | Paterson K G. ID-based signatures from pairingson elliptic curves [J]. Electronics Letters. 2002, 38 (18): 1025–1026. |
| [10] | Oh J, Lee K, Moon S. How to solve key escrow and identity revocation in identity-based encryption schemes [M] // Oh J, Lee K, Moon S. Information Systems Se- curity. Springer, 2005: 290–303. |
| [11] | Appenzeller G, Martin L, Schertler M. Identity-based encryption architecture and supporting data structures [J]. RFC5408. 2009. |
| [12] | Wang S, Cao Z, Xie Q, et al. Practical identity-based encryption in multiple private key generator (PKG) environments [J]. Security and Communication Networks. 2013. |
| [13] | Horwitz J, Lynn B. Toward hierarchical identity-based encryption [C]. In Advances in Cryptology - EUROCRYPT 2002. 2002: 466–481. |
| [14] | Gentry C, Silverberg A. Hierarchical ID-based cryptography[M]//Advances in cryptology - ASIACRYPT 2002. Springer Berlin Heidelberg, 2002: 548-566. |
| [15] | Kohnfelder L M. Towards a practical public-key cryptosystem[D]. Massachusetts Institute of Technology, 1978. |
| [16] | Rec I. X. 509 (revised), The directory-authentication framework[J]. International Telecommunication Union, 1993. |
| [17] | Zimmermann P R, Zimmermann P R. The official PGP user's guide[M]. Cambridge: MIT press, 1995. |
| [18] | Huston G, Michaelson G, Kent S. Resource Certification-A Public Key Infrastructure for IP Addresses and AS's[C]//GLOBECOM Workshops, 2009 IEEE. IEEE, 2009: 1-6. |
| [19] | Voltage Security. http://www.voltage.com. |
| [20] | Tariq M A, Koldehofe B, Rothermel K. Securing broker-less publish/subscribe systems using identity-based encryption[J]. Parallel and Distributed Systems, IEEE Transactions on, 2014, 25(2): 518-528. |
| [21] | The Resource Public Key Infrastructure (RPKI) to Router Protocol, RFC 6810 |
| [22] | <http://www.renesys.com/2010/11/chinas-18-minute-mystery/> |
| [23] | <https://www.wired.com/2014/08/isp-bitcoin-theft/> |
| [24] | <http://www.theverge.com/2017/1/7/14195118/iran-porn-block-censorship-overflow-bgp-hijack> |
| [25] | Breaking-HTTPS-With-BGP-Hijacking, http://www.blackhat.com/docs/us-15/materials/us-15-Gavrichenkov-Breaking-HTTPS-With-BGP-Hijacking.pdf |
| [26] | Apostolaki M, Zohar A, Vanbever L. Hijacking Bitcoin: Large-scale Network Attacks on Cryptocurrencies[J]. 2016. |
| [27] | Gilad Y, Cohen A, Herzberg A, et al. Are We There Yet? On RPKI's Deployment and Security[C]// NDSS. 2017. |
| [28] | Laurie B, Langley A, Kasper E. RFC 6962: Certificate transparency[S]. 2013. |
| [29] | Basin D, Cremers C, Kim H-J, et al. ARPKI: Attack resilient public-key infrastructure[C]. In: ACM Conference on Computer and Communications Security—CCS 2014. ACM, 2014: 382–393. |
| [30] | Perrig A, Jackson C, Gligor V. Accountable key infrastructure (AKI): A proposal for a public-key validation infrastructure[C]. In: International Conference on World Wide Web, 2013: 679–690. |
| [31] | Karatop A, e G, Erkay. An identity-based key infrastructure suitable for messaging and its application to e-mail[C]// International Conference on Security and Privacy in Communication Netowrks. ACM, 2008:10. |
| [32] | Melara M S, Blankstein A, Bonneau J, et al. CONIKS: bringing key transparency to end users[C]// Usenix Conference on Security Symposium. USENIX Association, 2015:383-398. |
| [33] | Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2009. |
| [34] | https://proofofexistence.com/ |
| [35] | http://www.coindesk.com/blocksign-utilises-block-chain-verify-signed-contracts/ |
| [36] | https://github.com/coinspark/ |
| [37] | https://counterparty.io/ |
| [38] | http://www.omnilayer.org/ |
| [39] | https://github.com/OpenAssets/openassets |
| [40] | https://en.wikipedia.org/wiki/Token |
| [41] | Kent S, Lynn C, Seo K. Secure border gateway protocol (S-BGP). IEEE Journal on Selected Areas in Communications, 2000,18(4): 582−592. |
| [42] | Kent S, Lynn C, Mikkelson J, Seo K. Secure border gateway protocol (S-BGP) real world performance and deployment issues. In: Proc. of the Annual Network & Distributed System Security Symp. San Diego: The Internet Society, 2000. |
| [43] | White R. Securing BGP through secure origin BGP. Internet Protocol Journal, 2003,6(3):15−22. |
| [44] | Goodell G, Aiello W, Griffin T, Ioannidis J, McDaniel P, Rubin A. Working around BGP: An incremental approach to improving security and accuracy of interdomain routing. In: Proc. of the 10th Annual Network & Distributed System Security Symp. San Diego: The Internet Society, 2003. |
| [45] | Le ZJ, Xiong NX, Yang B, Zhou YZ. SC-OA: A secure and efficient scheme for origin authentication of inter-domain routing in  cloud computing networks. In: Proc. of the 25th IEEE Int’l Symp. on Parallel and Distributed Processing. Anchorage: IEEE Computer Society, 2011. 243−254. |
| [46] | Hu YC, Perrig A, Sirbu M. SPV: Secure path vector routing for securing BGP. In: Proc. of the SIGCOMM 2004. Portland: ACM  Press, 2004. 179−192. |
| [47] | Wan T., Kranakis E., and van Oorschot, P. 2005. Pretty secure BGP (psBGP). In Proceedings of the 2005 ISOC Symposium on Network and Distributed Systems Security (NDSS'05). San Diego, CA. |
| [48] | Huston G, Bush R. Securing bgp with bgpsec[J]. FR o MTHEED i T o R The process of adding security to various components of Internet architecture reminds me a little bit of the extensive seismic retrofit-ting that has been going on in California for decades. The process is slow, expensive, and occasionally intensified by a strong earthquake, 2011: 2. |
| [49] | Gersch J, Massey D. Rover: Route origin verification using dns[C]//Computer Communications and Networks (ICCCN), 2013 22nd International Conference on. IEEE, 2013: 1-9. |
| [50] | The RPKI Deployment Monitor, [NIST](http://www.antd.nist.gov/) [Information Technology Laboratory](http://www.nist.gov/itl). http://rpki-monitor.antd.nist.gov. |
| [51] | M. Chase and S. Meiklejohn. Déjà Q: using dual systems to revisit q-type assumptions. In EUROCRYPT, pages 622–639, 2014. Cryptology ePrint Archive, Report 2014/570. |
| [52] | Malhotra A, Goldberg S. RPKI vs ROVER: comparing the risks of BGP security solutions[C]//Proceedings of the 2014 ACM conference on SIGCOMM. ACM, 2014: 113-114. |
| [53] | Antonopoulos A M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. USA: O0Reilly Media Inc., 2014. |
| [54] | CertCoin: A NameCoin Based Decentralized Authentication System, http://courses.csail.mit.edu/6.857/2014/files/19-fromknecht-velicann-yakoubov-certcoin.pdf |
| [55] | An empirical study of Namecoin and lessons for decentralized namespace design, http://weis2015.econinfosec.org/papers/WEIS\_2015\_kalodner.pdf |
| [56] | https://github.com/StorjOld/MetaDisk |
| [57] | https://onename.com/ |
| [58] | Dennis R, Owen G. Rep on the block: A next generation reputation system based on the blockchain[C]// International Conference for Internet Technology and Secured Transactions. 2015:131-138. |
| [59] | Huston G, Rossi M, Armitage G. Securing BGP—A literature survey. IEEE Communications Surveys & Tutorials, 2011,13(2): 199-222. [doi: 10.1109/SURV.2011.041010.00041]。 |
| [60] | Lychev R, Goldberg S, Schapira M. BGP security in partial deployment: is the juice worth the squeeze?[J]. ACM SIGCOMM Computer Communication Review, 2013, 43(4): 171-182. |
| [61] | Cooper D, Heilman E, Brogle K, et al. On the risk of misbehaving RPKI authorities[C]//Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks. ACM, 2013: 16. |
| [62] | Heilman E, Cooper D, Reyzin L, et al. From the consent of the routed: Improving the transparency of the rpki[C]//Proceedings of the ACM SIGCOMM 2014 Conference. 2014. |
| [63] | Wahlisch M, Maennel O, Schmidt T C. Towards detecting BGP route hijacking using the RPKI[J]. ACM SIGCOMM Computer Communication Review, 2012, 42(4): 103-104. |
| [64] | Wahlisch M, Schmidt R, Schmidt T C, et al. When BGP Security Meets Content Deployment: Measuring and Analysing RPKI-Protection of Websites[J]. arXiv preprint arXiv:1408.0391, 2014. |
| [65] | BGPSEC: Leaks and Leaks. http://packetpushers.net/bgpsec-leaks-leaks/. |
| [66] | Naor, D., Naor, M., Lotspiech, J.: Revocation and tracing schemes for stateless receivers. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 4162. Springer, Heidelberg (2001) |
| [67] | Seo, Jae Hong, and Keita Emura. "Efficient delegation of key generation and revocation functionalities in identity-based encryption." Topics in Cryptology–CT-RSA 2013. Springer Berlin Heidelberg, 2013. 343-358 |
| [68] | Lee, K., Lee, D.H., Park, J.H.: Efficient revocable identity-based encryption via subset difference methods. eprint.iacr.org/2014/132 (2014) |
| [69] | Seo, Jae Hong, and Keita Emura. "Revocable hierarchical identity-based encryption: History-free update, security against insiders, and short ciphertexts." Topics in Cryptology–CT-RSA 2015. Springer International Publishing, 2015. 106-123. |
| [70] | Ryu, Geumsook, et al. Unbounded Hierarchical Identity-Based Encryption with Efficient Revocation. Information Security Applications. Springer International Publishing, 2015 |
| [71] | Lewko, Allison, and Brent Waters. "Unbounded HIBE and attributebased encryption." Advances in Cryptology–EUROCRYPT 2011. Springer Berlin Heidelberg, 2011. 547-567 |
| [72] | Boldyreva A, Goyal V, and Kumar V. Identity-based encryption with efficient revocation[C]. Proceedings of the 15th ACM Conference on Computer and Communications Security, Alexandria, USA, 2008: 417-426. |
| [73] | Libert B and Vergnaud D. Adaptive-ID secure revocable identity-based encryption[C]. Proceedings of the Cryptographers’ Track at the RSA Conference, Lecture Notes in Computer Science, San Francisco, USA, 2009, 5473: 1-15 |
| [74] | 锁琰, 李晓辉, 徐小岩,等. 一种安全的分布式群签名方案[J]. 哈尔滨工程大学学报(英文版), 2011, 32(12):1594-1598. |
| [75] | Tsai, Tung‐Tso, Tseng, Yuh‐Min, Wu, Tsu‐Yang. Provably secure revocable ID‐based signature in the standard model[J]. Security & Communication Networks, 2013, 6(10):1250–1260. |
| [76] | Vervier P A, Thonnard O, Dacier M. Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks[C]// Network and Distributed System Security Symposium. 2015. |
| [77] | X. Shi, Y. Xiang, Z. Wang, X. Yin, and J. Wu, “Detecting prefix hijackings in the internet with argus,” in IMC. ACM, 2012, pp. 15–28 |
| [78] | Lad M, Massey D, Pei D, et al. PHAS: A Prefix Hijack Alert System[C]//Usenix Security. 2006. |
| [79] | Kent S, Chi A. Threat model for BGP path security. Internet Draft, 2012. https://datatracker.ietf.org/doc/draft-ietf-sidr-bgpsecthreats/ |
| [80] | SIDR. A hack for the next generation of rpki-based origin validation. 2012. http://www.ietf.org/mail-archive/web/sidr/current/msg03990.html |
| [81] | Wang N, Zhi Y J, Zhang J H, et al. Identity-Based Secure Inter-Domain Routing Protocol: Identity-Based Secure Inter-Domain Routing Protocol[J]. Journal of Software, 2009, 20(12):3223-3239. |

7、指导教师对开题报告的评语

|  |
| --- |
| 对1-6项逐项予以评价，并着重对国内/外研究现状的了解情况、研究内容的创新性等方面进行评价。  本课题针对当前域间路由存在的安全问题进行了深入的分析，阐述了基于新型信任体系域间路由安全增强技术的特点和优势，包括去中心化区块链用于网络地址资源分配和路由源通告，以及身份基密码用于路由路径通告授权认证，对于解决现有网络问题提供了很好的思路，有着重要的研究意义，立论依据充足。  报告对该领域中的研究现状有较为充分的了解，首先通过现有对域间路由安全问题解决问题方案的广泛了解，给出了其存在的缺陷和原因。然后详细说明了两种新型信任体制的研究现状，特别对基于区块链的去中心化信任体制的基本原理、实现机制和相关应用有深入的分析。另外对基于无证书的身份基信任体制下的身份基密码的研究现状进行了分析总结，特别是密钥撤销方面进行了阐述，分析了现有研究的欠缺，对课题研究有指导作用。由于当前对基于区块链的去中心化资源信任基础设施的应用相对还比较有限，需要进一步加强资料的查询力度，及时跟踪国内外的发展动态。  报告的研究内容拟从基于区块链的资源分配通告、基于自证明资源的路由路径安全认证、面向授权认证的身份基密码方案几个方面对域间路由安全进行研究，较好的涵盖了路由系统的各个方面，通过解决这些问题能够给出一套域间路由安全的关键技术和机制，有效解决当前网络面临的一系列问题，提高网络的安全性。研究内容论证充分，技术可行，有较好的创新性。  现有的研究条件较为充分，学位论文工作计划较为合理。  导师签字：      年 月 日 |