（“大白话版”思路：怎么让别人都知道“我就是张宇”，最直接的方法，就是”公开“，即我通过所有媒体告诉全世界的人“我是张宇”。这样每个人都“知道我就是张宇”，但却很难做到。例如，不能直接将”公开“用在DNS上，因为所有人要通过根“谁是张宇”。如果根作恶怎么办？我们的思路，基于”互信“，即张宇和甲认识，甲和乙“互信”，甲就可以告诉乙“谁是张宇”，乙就知道了。大家相互转告，这样就不依赖于单个根了。但是如果又有一个人丙告诉乙，另外一个人是张宇，乙相信甲还是丙？这就是BGP里的问题，一个路由器收到了不一致的前缀声明，该怎么办？我们的思路是“共识”，即乙要把这件事告诉其他人，大家一起商量，看看到底“谁是张宇”。最后，如果去掉DNS和BGP上的束缚，让我们设计一个未来网，我们该怎么办？最直接的方案就是把前面的”互信“和”共识“融合在一起，即”互信+共识  公开“。）  
  
题目：互联网关键基础设施资源多方安全共治框架机制研究  
英文：Multi-Party Secure Cooperation Governance Framework Mechanisms for Internet Critical Infrastructure Resources  
  
摘要：互联网关键基础设施资源治理正面临政策和技术双重挑战， 本项目针对多方共治中拜占庭式安全威胁，提出一套基于”互信+共识=公开”的多方安全共治框架机制：首先，名字空间基础理论 （康，夏）；其次，针对域名系统DNS，基于互信的互联根（刘）；接着，针对域间路由BGP，基于共识的RPKI增强（秦）；最后，针对未来网NDN，基于公开（区块链技术？）（余）。  
英文：  
  
关键词：互联网关键基础设施资源安全，互联网治理，域名系统安全，域间路由安全，未来网体系结构  
英文：  
  
  
研究背景、意义：  
互联网起初在一个可信环境下运行，目前受到系统内威胁(ICANN独裁、BGP错误配置等)，根源在于域名系统和域际路由治理存在问题。问题很大程度上涉及政策，但技术对政策也有较大影响。研究治理机制现实意义和理论意义都很大。  
  
相关研究：  
1、DNS，DNSSEC，若IANA作恶怎么办，各种根替代方案，P2P，比特币  
2、RPKI研究，若一个AS出错怎么办  
3、NDN研究， 关于资源治理还是空白  
4、名字空间基础理论，zooko三角，扁平名字与层次化名字争论，发现理论很重要，所以我们要研究理论  
  
总结，关键基础设施资源治理问题很大，相关研究很多，但尚未解决这些问题。 这些问题似乎具有一定共性，但以往研究都没有充分认识到 。  
  
  
  
科学问题：  
我们认识到这些问题是具有共性的，即都是关于如何”公开信息”，多方治理（分配、绑定、解析）一个资源所对应的名字空间，威胁在于系统内部成员的不当行为对相关资源所依赖服务造成伤害，同时也是有差异的（信任锚，信源，信道）。本项目研究令资源治理更安全的共性理论。  
  
研究内容：  
  
1、研究单信任锚问题，具体案例DNS  
2、研究多来源不一致问题，具体案例RPKI  
3、研究多锚多源，具体案例NDN  
  
研究目标：  
  
1、在单信任锚下，实现互信  
2、在多信任锚下，实现共识  
3、 实现公开。。。  
  
关键问题：  
  
1、如何保证zooko三角猜想前提下，实现去中心化？  
2、如何保证。。。。，BGP？  
3、如何公开。。。。？  
  
研究方案：  
1、针对DNS单信任锚，互信：互信根间交换信息，就像BGP（但不同来源信息不同怎么办），实现名字分配与名字公开的分离  
2、针对BGP多信源冲突，共识：从多个AS获得信息来综合（但信息源不足怎么办），实现。。。。  
3、针对NDN名字空间治理机制空白，公开：把自己的信息尽量公开，让所有人都知道，公开=互信+共识，类似比特币的区块链方案 （终极方案）， 通过融合两套方案一起满足在zooko三角猜想的三个属性（但没有违背）。  
  
可行性分析：  
1、互信，DNS， 满足了zooko三角  
2、共识，BGP，，。。。。。  
3、公开，NDN，因为前两个可行，而且因为没有限制  
  
特色与创新之处：  
发现了资源治理问题的一个”共性“（公开）和两点”差异“（DNS缺乏互信，BGP缺乏共识），提出 公开=互信+共识 的思路，并设计了对应共治框架机制。