未来互联网体系结构中的内生安全研究

陈 钟[1,2,3], 孟宏伟[1,2,3], 关 志[1,2,4]

[1]高可信软件技术教育部重点实验室(北京大学) 北京 中国 100871
[2]网络和软件安全保障教育部重点实验室(北京大学) 北京 中国 100871
[3]北京大学信息科学技术学院 北京 中国 100871
[4]北京大学软件工程国家工程研究中心 北京 中国 100871

摘要 未来互联网体系结构试图通过其内生安全特性解决目前互联网中的安全问题。新型的未来互联网体系结构命名空间普遍使用了具备自认证能力的网络标识支持网络的内生安全, 但目前的方案不能将用户标识符、网络标识符、公钥三者在脱离 PKI 的情况下实现同时绑定。本文提出了基于组合公钥密码体制的自认证标识(SCI-CPK)命名方案, 可用于未来互联网体系结构命名空间中标识安全绑定, 并给出了在未来互联网体系结构 XIA、MobilityFirst 和 NDN 中支持实体鉴别的应用方法。分析表明, SCI-CPK 方案能够支持未来互联网中泛在互联和泛在移动场景下的大规模实体身份和地址鉴别。

关键词 未来互联网体系结构; 内生安全; 自认证; 组合公钥体制
中图法分类号 TP393 DOI 号 10.19363/j.cnki.cn10-1380/tn.2016.02.004

Research on Intrinsic Security in Future Internet Architecture

CHEN Zhong[1,2,3], MENG Hongwei[1,2,3], GUAN Zhi[1,2,4]

[1]Key Laboratory of High Confidence Software Technologies (Peking University) Ministry of Education, Beijing 100871, China
[2]Key Laboratory of Network and Software Security Assurance (Peking University) Ministry of Education, Beijing 100871, China
[3]School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China
[4]National Engineering Research Center of Software Engineering, Peking University, Beijing 100871, China

Abstract The characteristics of intrinsic security in the future Internet architecture have been used to conquer the security problems of current Internet. Self-certifying addresses are introduced in future Internet architecture (FIA) to enable the intrinsic security properties. However, without PKI, these approaches in FIA miss the intrinsic binding between user-level descriptor, network-level identifier and correspondent public key. To this end, a naming scheme of Self-Certifying Identifier in FIA based on Combined Public Key (CPK), named as SCI-CPK, is proposed in this paper. The use cases of identity authentication based on SCI-CPK in FIA designs are also given, including XIA, MobilityFirst and NDN. The analysis shows that the proposed method is benefit of ubiquitous access and vast mobility scenario in the future Internet.

Key words future Internet architecture; intrinsic security; self-certifying; combined public key

1 引言

一直以来, 以 TCP/IP 协议为核心的互联网得到了飞速发展, 实现了大多数计算机系统、移动设备的互联, 在经济发展、社会生活、军事等方面发挥着巨大作用, 已经成为世界范围不可或缺的信息基础设施。但与此同时, 由于现有互联网体系结构不具备地址真实性鉴别的内生机制[1,2], 不仅造成了源地址欺骗(Source Spoofing)、路由劫持(Hijacked Route)、拒绝服务(Denial-of-service)等大量攻击的发生, 而且导致攻击源头和攻击者身份难以追查, 严重扰乱了互联网秩序, 给互联网乃至越来越依托互联网运行的国家经济、社会和军事系统的安全带来了极大危害。例如, 路由设备基于目的地址转发分组, 对数据包的来源不做验证, 无法验证数据包的来源是否可信, 大量基于地址伪造的攻击行为无法跟踪。但是到目前为止, 针对以上问题并没有周全、彻底的解决办法。现有的安全技术都是以修修补补的形式增加进

通讯作者: 陈钟, 博士, 教授, Email: zhongchen@pku.edu.cn。
本课题得到国家自然科学基金项目(Nos.61170263、61421091)资助。
收稿日期: 2016-04-07; 修改日期: 2016-04-21; 定稿日期: 2016-05-01

来的, 系统性不强, 基本处于被动应对状态[3,4]。例如, 为了防止拒绝服务攻击需要网络管理员设置复杂的包过滤策略[5], 为了解决边界路由安全问题的S-BGP协议(Secure Border Gateway Protocol)需要引入第三方可信证书和繁杂的认证过程[6]。David[7]等人认为, 造成这一问题的根本原因在于IP网络不具备审计能力, 即发生问题后无法进行追责。因此, 包括地址真实性鉴别在内的命名安全体系是互联网可信的基础和前提, 对互联网安全具有关键意义, 成为未来互联网体系结构亟待解决的重要问题之一。

事实上, 从互联网体系结构上系统地解决互联网安全问题, 已经成为未来互联网体系结构(Future Internet Architecture)研究的一项重要课题[8,9]。2005年开始, 以美国NSF为代表的未来互联网体系结构研究项目启动, 开始了从全新角度设计未来互联网的大胆尝试[9,10]。例如NDN(Named Data Networking)、MobilityFirst、XIA(eXpressive Internet Architecture)研究项目等已经形成了较为成熟的体系结构、网络协议和原型试验系统等研究成果[10-12]。虽然这些研究项目侧重点以及具体的技术方案有所差别, 但总体目标与研究思路基本一致: 在设计之初就充分考虑未来互联网发展趋势中的内容获取、按需服务、移动性等方面, 且都把内生安全特性作为解决互联网安全问题的重要手段[29]。由于地址(或标识)和路由系统是当前互联网体系结构的核心, 而地址(或标识)又是路由系统的基础。因此, 互联网地址(或标识)是实现其内生安全的基本载体之一, 未来互联网体系结构都不约而同地针对命名空间中地址/标识本身的构造方式、结构特征以及路由寻址协议进行创新性改造。

本文分为两个部分: 第一部分首先回顾了未来互联网体系结构研究中地址安全的研究历史和现状, 分析了其面临的主要问题。第二部分介绍了基于我国组合公钥[30]的命名方式, 提出了将用户标识符、网络标识符和公钥三者天然绑定的方案(SCI-CPK), 并给出了该方案在标识和地址分离的未来互联网体系结构(如XIA和MobilityFirst)和命名数据网络(如NDN)中的应用方式。

2 研究现状

2.1 互联网命名空间安全

互联网命名空间是网络实体标识集合, 包括了身份标识、位置标识、以及结构、可扩展等多重属性。命名空间安全主要是指身份标识和位置标识的可信可控。即每个网络终端都使用真实的身份或地址访问网络, 网络基础设施能够识别伪造源身份或地址的分组, 禁止不真实分组在网络上传输, 并能够通过身份/地址鉴别机制实现对用户网络行为追查。身份或地址鉴别是保证互联网真实性(Authenticity)和可审计性(Accountability)的重要手段。真实性是指用户身份、信息来源、信息内容的真实性; 可审计性是指网络实体发起的任何行为都可追踪到实体本身; 保证真实性是实现可审计的前提。

在IP网络中, 命名空间安全主要是指IP地址安全。但IP地址兼具身份和定位的语义过载特性带来了源地址和路由前缀两个方面的安全威胁[2]。IP网络通过源地址鉴别保证IP的真实性。源地址鉴别是指对数据包中的源地址字段进行检查, 以保证其发送者IP地址的真实性和有效性, 达到验证数据源的身份并丢弃假冒数据包的目的。源地址鉴别本质上属于实体鉴别, 即验证信息的发送者是真实的, 而不是冒充的, 此为信息源鉴别; 在此基础上, 可以进一步实现消息鉴别, 即证实收到的消息来自声称的源点且未被篡改。

为了实现互联网命名空间(地址)安全, 基于密码学的地址安全机制受到越来越多研究者的关注, 包括基于证书的公钥密码机制和自认证(self-certifying)机制。在公钥密码体制下, 用户A先用私钥对信息数字签名。如果其他用户收到用户A的签名信息, 并且可以用A的公钥验证签名的正确性的话, 他就可以相信消息的确来自A, 因为只有A拥有能产生正确签名的私钥, 并且信息在传输中没有被篡改。公钥数字签名技术需依赖公钥基础设施(PKI)颁发的CA证书绑定实体身份和公钥, 以保证对方实体公钥的真实性。但CA证书管理复杂、可扩展性差。于是研究人员提出了具备自认证特性的地址方案。

2.2 具备自认证特性的地址方案

(1) Cryptographically Generated Addresses (CGA)

CGA[13]是一种用公钥的哈希值生成部分IPv6地址的方法。节点生成一个公私钥对, 使用公钥的哈希值作为其IP地址的后64位。该方法的优点是可以通过自身携带的公钥来验证自己的身份, 节点的公钥验证不需要任何网络基础设施的支持。当节点发送数据包时, 首先用私钥对数据包进行签名, 然后和公钥一起发送到通信对端, 当通信对端接收到该数据包时, 首先用公钥的哈希值来验证数据包的源地址(IP地址的后64位)是否正确。当验证通过后, 再用公钥来验证数据包的数字签名, 只有这两次验证通过, 通信对端才对此数据包进行下一步处理。

基于标识/位置(ID/locator)分离的网络协议如 LISP[14]和 ILNP[15], 可以利用 CAG 的方式实现主机鉴别, 保证源地址安全。在 LISP 或 ILNP 中, IPv6 地址分成两个独立的区域, 其中高 64bit 作为位置标识, 用于表示节点在网络中的位置, 故也称之为路由前缀, 低 64bit 作为主机标识。主机标识可以利用自身公钥的哈希值生成, 用于主机身份鉴别。但由于 IPv6 地址中的高 64 位是网络地址部分, 本身的结构性特性使其无法通过公钥哈希后得到的随机字符串表示, 因此使用 CGA 的方式不能实现子网地址鉴别, 无法保证路由前缀安全。

(2) Host Identity Protocol(HIP)

由于 IP 网路将主机标识和网络地址标识耦合在一个 IP 地址中, 主机发生移动后, IP 地址发生了变化, 这样也就存在其他主机也可能伪造移动主机身份发送数据包的安全隐患。为了解决这个隐患, IETF 提出了 HIP[16]协议。HIP 在网络层和传输层之间插入主机标识层, IP 地址只作为网络层所使用的定位标识符, 实现数据报的路由转发, 主机标识符 HI(Host Identity)提供主机身份标识功能, 由传输层使用。双方在通信时, IP 地址的变化对传输层透明, 从而保证在发生移动或地址变化时, 通信不中断可以持续进行, 并且通信对端可以根据主机标识 HI 确定移动节点身份。在 HIP 中, HI 是非对称密钥体制中的公钥, 由于不同体制的密钥长度不同, 为了索引方便并与 IPv6 地址长度兼容, 将 HI 进行哈希运算后得到 128 位的 HIT(Host Identity Tag)作为主机标识。HIP 在主机中实现了名址分离, 可利用 HIT 实现主机和消息鉴别, 解决了移动性问题的同时, 也增强了安全性。HIP 只能用于主机之间的端到端身份鉴别, 无法应对地址前缀欺骗。

(3) XIA

XIA[17-20]未来互联网体系结构由 CMU 的研究团队提出, 可演进(Evolvable)、可信(Trustworthy)和灵活路由(Flexible Routing)是其网络体系结构三个主要特点。XIA 使用了标识和地址分离的设计, NID 代表网络域或子网, 路由时用来定位网络地址; HID 是主机标识, 支持域内单播路由寻址。在安全方面, XIA 沿用并扩展了 AIP(Accountable Internet Protocol)[7]的设计思想, 即 NID 和 HID 都是通过对各自公钥哈希得到的 160bit 扁平化网络地址标识。XIA 使用有向无环图(Directed Acyclic Graphs, DAGs)的地址结构, 支持灵活编址和路由, XID 作为 DAG 中的节点(Node), 节点相互连接表示一个地址, 这种方法区别于传统的一维字符串形式, 如 NID→HID。路由器首先将数据包路由到以 NID 为标识的网络, 到达后, 路由器再按照 HID 标识将数据包转发到对应的主机。通过自认证的标识, AIP 协议设计了两处可以对数据包的源地址进行验证的机制: 首先是在第一跳路由器(First-hop Router)上验证与其直连的主机是否有源地址欺骗行为(HID Verification)。另外在数据包所经过的所有边界路由器上, 会检查数据包的上一跳是否合法(NID Verification)。因此, XIA 支持主机鉴别和网络域鉴别。

(4) MobilityFirst

MobilityFirst[21,22]是由美国 Rutgers 大学负责牵头研究的未来互联网体系结构。其目标是针对目前移动接入设备激增的现实, 考虑泛在移动的需求, 设计面向无线移动世界的网络体系结构。MobilityFirst 的两条基本设计原则是: 将无线移动终端作为主流接入设备设计网络架构、设计更为强大的安全和信任机制。MobilityFirst 体系架构的基本技术特征包括: 使用 ID 与 Locator 分离的机制、采用扁平地址结构、支持快速的全局名称解析、采用公钥基础设施实现标识的验证、支持存储转发的路由方式、支持缓存和逐跳的分段数据传输等。

在 MobilityFirst 中网络通信实体标识包括: 用户标识符(Name)、全局唯一标识(GUID)和网络地址(NA)三部分。Name 供应用层使用, 是可读的, 便于记忆和查找, 可以是用户名称、设备名称、内容名称、群组名称等。GUID 是通信实体标识, 采用了扁平化的地址空间, 同时也是通信实体的公钥哈希值, 具有自认证特性。NA 是网络接入点地址, 用来路由。每个 Name 关联到一个 GUID, 每个 GUID 可以关联多个网络地址 NA。

移动性支持是 MobilityFirst 的核心理念。MobilityFirst 通过两级的映射完成 Name—GUID—NA 的动态绑定, 以支持全局的移动性。其中, Name 到 GUID 的绑定由 NCRS(Name Certificate & Resolution Service)负责。NCRS 类似 DNS, 存储着 Name 与 GUID 的对应关系, 通过使用 Name 查询 NCRS 来获取通信对端的 GUID。NCRS 还具备类似公钥基础设施的功能, 负责为设备生成公钥 GUID 证书。GUID 到 NA 的动态绑定由 GNRS(Global Name Resolution Service)负责管理。节点移动后向 GNRS 更新其 GUID 与 NA 的最新绑定, 并利用 GUID 的公钥对绑定更新签名和鉴别, 以防止 GUID 欺骗、NA 绑定伪造等攻击。MobilityFirst 没有给出数据包在不同网络域之间转发的验证方案, 而且它通过公钥基础设施分发公钥证书的做法, 面临对海量用户公钥

管理的挑战, 存在较大的可扩展问题。

(5) NDN

NDN[23]是以内容为中心的未来互联网体系结构, 由 UCLA 大学发起并主导, 其思想来源于对现在互联网应用的观察: 如今互联网的主要应用是内容的获取和分发。NDN 中将内容视为网络中的头等实体, 将当前基于 IP 为中心的网络架构转变为以内容为中心的架构。采用了基于内容的命名、基于命名数据的路由和内容缓存, 以内容名字(Name)代替 IP 地址, 将基于 IP 地址的路由转变为基于内容名字的路由, 并重新设计数据包的格式和各层协议。同时, 通过路由器来缓存内容数据, 试图使数据传输更快, 避免网络拥塞。

NDN 的命名用类似于 URL 的层次化的方式组织, 如“/movies/Disney/LionKing/Theme_Song”。这种层次化的方式可以按照语义进行路由聚合, 如“/movies/Disney/”可以表示更多内容集合, 从而保证采用名称路由的规模扩展性, 使路由快速收敛。从安全的角度看, 这种命名方式将用户标识符和网络标识符合二为一, 可视为一种内生的绑定, 但这种层次化带语义的地址结构, 无法作为公钥的哈希值, 因此其不具备自认证能力, 还需要第三方可信机构提供证书完成内容命名与公钥的绑定。用户需要利用证书中的公钥对收到内容进行验证, 确保该内容确实来自声称的发布者, 实现数据源鉴别。

2.3　面临的主要问题

事实上, 为了更好地支持互联网命名空间安全, 需要建立用户标识符(User-level human-readable name)、网络标识符(Network-level routable ID)和公钥密码三个之间的绑定关系[24]。用户标识符: 是用户可读的名称, 如主机名 server_123、设备名 Alice's phone、服务名称 google.com 等, 需在域名服务中注册, 域名服务如 IP 中的 DNS, XIA 中的 NS(Name Service), MobilityFirst 中的 NCRS。网络标识符: 是网络可寻址的路由地址, 如 XIA 中的 NID、HID、SID、CID, MobilityFirst 中的 GUID 和 NA, 以及 NDN 中的内容名称; 公钥密码: 是用于标识符和网络标识符绑定的公共密钥, 用于数据接收方对发送方实施身份和消息内容的鉴别。

对于标识和地址分离的网络体系结构, 如 XIA 和 MobilityFirst, 其网络标识符是扁平化的二进制数据, 具备了与公钥绑定的先天条件, 它们都使用带自认证功能的主机标识或网络地址标识, 通过公钥签名技术实现实体鉴别。但是, 任何通信都是由用户发起的, 用户标识符如主机名称、域名等, 并不具备自认证特性, 其真实性鉴别还需要 PKI 证书的支持。对于以内容为中心的网络体系结构, 如 NDN, 将内容名称直接作为网络标识符, 实现了用户标识符和网络标识符的天然绑定, 但其结构化特性, 决定了无法实现与公钥的内生绑定, 同样需要 PKI 的支持。所以, XIA、MobilityFirst 和 NDN 都没有实现将用户标识符、网络标识符和公钥的内生绑定, 都至少需要 PKI 的支持实现其中的二者的绑定, 如图 1 所示。

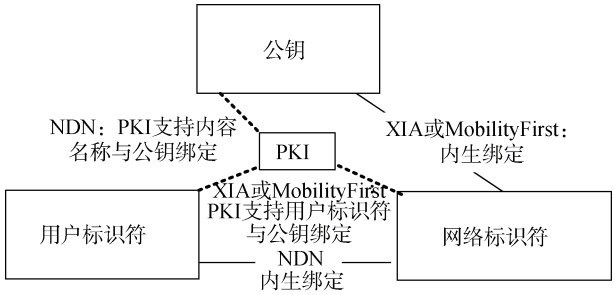


图 1　NDN/XIA/MobilityFirst 标识与公钥的绑定关系

PKI 通用引入可信第三方 CA, 以公钥证书的形式将用户公钥和用户身份进行绑定, 形成了解决网络安全问题的成熟方案。但由此带来证书的管理、存储和计算上的代价: 一是证书的签发、发布、获取、验证、撤销等, 流程较为复杂; 二是需要在线的证书目录为用户随时提供证书下载和状态查询服务, 增加了维护开销; 三是如果用户通信的对象比较多, 用户必须在本地存储和管理这些证书, 增加了用户端使用开销; 四是大规模密钥管理的问题一般是采用物理上增加 CA 的方法, 但是各个 CA 的用户之间还存在交叉认证和信任管理的问题。

随着移动互联网、物联网的蓬勃发展, 接入互联网的传感器、可穿戴设备、智能终端数量剧增, 实体鉴别所需公钥数量巨大, 如何实现高效公钥的管理、远程通信实体如何得到对方的公钥、并确保公钥的真实性, 将成为一项挑战, 也是关系到未来互联网体系结构能否落地的重要问题。

3　基于 CPK 的自认证标识(SCI-CPK)

3.1　组合公钥密码体制

组合公钥体制[25,30](Combined Public Key, CPK), 是基于标识的非对称公共密钥体制, 可以在椭圆曲线密码(ECC)上构建。在 CPK 中, 用户公钥由用户标识符直接导出, 如: 主机名、网络域名、邮件地址、电话和身份证号等, 天然地带有用户身份信息。在一般的公钥体制中, 公钥是直接公布的, 有多少用户就公布多少公钥。而在 CPK 中, 用户的公钥不直接

公布, 而只公开公钥组合矩阵, 公钥由用户身份导出。这样也就无须保存每个用户的公钥证书和公钥信息, 从而减少了证书管理的开销。下面以 CPK-ECC 为例[30], 说明其工作原理。

CPK 密钥分为私有密钥和公有密钥。在有限域 Fp 上, 椭圆曲线 E: $y^2 \equiv (x^3 + ax + b) \bmod p$ 由参数 (a, b, G, n, p) 定义。其中 a, b 是系数, $a, b, x, y \in$Fp, G 为加法群的基点, n 是以 G 为基点的群的阶。令任意小于 n 的整数为私钥, 则 $r \cdot G = R$ 为对应公钥。ECC 具有复合特性: 任意多对私钥之和与对应的公钥之和构成新的公、私钥对。设私钥之和为

$$(r_1 + r_2 + \cdots + r_m) \bmod n = r$$

则对应公钥之和为

$$R_1 + R_2 + \cdots + R_m = R$$

那么, r 和 R 刚好形成新的公、私钥对。这是因为,

$$R = R_1 + R_2 + \ldots + \mathrm{R}_m = (r_1 + r_2 + \cdots + r_m)G = r \cdot G$$

CPK 的组合矩阵分为组合私钥矩阵和组合公钥矩阵, 分别用($r_{i,j}$)或($R_{i,j}$)表示, r 是小于 n 的随机数。私钥矩阵($r_{i,j}$)由 KMC 保有, 用于私钥的生成, 公钥矩阵由私钥矩阵派生 $r_{\mathrm{i,j}} \cdot G = (x_{i,j}, y_{i,j}) = R_{i,j}$, 公钥矩阵分发到每一个实体, 用于公钥的计算。

组合密钥由组合矩阵 A 产生。矩阵 A 的大小为(32×32)。标识到矩阵坐标的映射是由 YS 序列指示的, YS 序列是实体标识(ID)在映射密钥 Hkey 下经 Hash 变换的输出。

$$\mathrm{YS} = \mathrm{Hash}_{\mathrm{Hkey}}(\mathrm{ID}) = w_0.w_1, w_2, \cdots, w_{35};$$

$w_0 \cdots w_{35}$ 分成 4 组, 分别以 $w_{00} \cdots w_{08}$; $w_{10} \cdots w_{18}$; $w_{20} \cdots w_{28}$; $w_{30} \cdots w_{38}$ 标记。其中 $w_{00}, w_{10}, w_{20}, w_{30}$, 的字长为 6-bit, 内容分别指示置换序号(3-bit)和置换起点(3-bit)。

$w_{i,j}$ $(i = 0 \cdots 3; j = 1 \cdots 8)$ 的字长为 5 比特, 指示组合矩阵 A 的行坐标。列坐标则经置换变换。置换表的大小是 8×8, 在 CPK 芯片中加密保护。置换表的列为置换序号, 行为置换起点。经置换后的列坐标, 用 $t_{i,j}$ 表示$(i = 0 \cdots 3, j = 1 \cdots 8)$。

Alice 的组合私钥, 由 KMC 计算:

$$csk_{\mathrm{Alice}} = \sum_{i=0}^{3} \sum_{j=1}^{8} r_{[w_{i,j}, t_{i,j}]} \bmod n$$

Alice 的组合公钥, 由依赖方根据组合公钥矩阵查表得出:

$$CPK_{\mathrm{Alice}} = \sum_{i=0}^{3} \sum_{j=1}^{8} R_{[w_{i,j}, t_{i,j}]}$$

私钥分发有两种形式: 一是面对面的分发; 二是网上远程分发。面对面的分发方式是通用方式, 即用户自报标识, 按规定程序分发私钥。远程分发是在标识能够自动扫描的方式获取的情况下采用, 如 SIM 卡中的电话号码, IC 卡中的帐号等。

不同于 PKI 是通过第三方间接证明的体系, 只要公布了组合矩阵, 任何人想要获得某个用户的组合公钥, 只要按照用户标识和公钥矩阵, 按照查表就能得到组合公钥: CPK_{Alice}。CPK 的突出优势在于, 它通过有限种子密钥组合的方法, 产生数量庞大的共、私钥对, 并基于用户的标识生成公钥解决了实体与公开密钥的解耦, 无需可信第三方的认证, 能够用来解决大规模网络环境下密钥的生产与分发问题。它采用私有密钥集中生产与分发方式, 便于管理并建立网络秩序, 适用于未来互联网环境下海量设备接入的情况。

3.2 基于 CPK 的地址(或标识)安全绑定

基于 CPK 的密钥生成机制能够实现用户标识符、网络标识符和公钥三者的天然绑定:

$$\mathrm{Hash}(\textit{'Alice's Phone'}) \rightarrow \text{routable ID} \rightarrow \sum\sigma(R_{i,\mathrm{j}}) \rightarrow CPK_{\mathrm{Alice}}。$$

给定一个可读的用户标识符, 如"*Alice's Phone*", 得到网络标识为: *ID=Hash (name)*, 对应的组合私钥在密钥管理中心生成, 任何人能够根据组合矩阵($R_{i,j}$)和用户/网络标识符查表得到对应的组合公钥 CPK_{Alice}。通过 CPK 建立的用户标识符、网络标识符和公钥三者的安全绑定关系如图 2 所示。

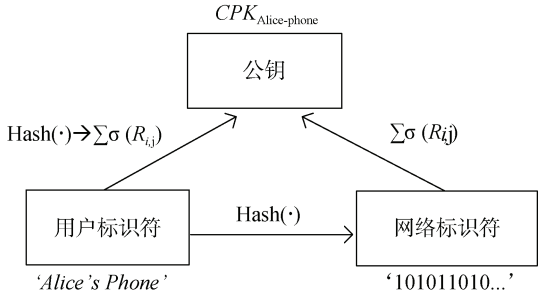


图 2 基于 CPK 的标识安全绑定

3.3 基于 CPK 安全鉴别

令 Alice 的签名函数:

$$\mathrm{SIG}_{alice}(\mathrm{h}) = (s, c)$$

其中, *alice* 是组合私钥, h 是签名对象, 如实体标识或数据的消息鉴别码 HMAC 等, s 是签名码, c 是核对码。

Alice 签名:

选择一个随机数 $k(0<k<n)$,

$$k\,G = (x_1, y_1)$$

$$c = (x_1 + y_1)^2 \bmod 2^m$$

$$s = k^{-1}(h + c \cdot alice) \bmod n$$

其中, 2^m 用于校验码长度的选择。Alice 发送: sign = (s, c)。

Bob 的验证: $\mathrm{VER}_{ALICE}(s) = c'$。

验证过程: Bob 根据 Alice 的标识计算组合公钥: Alice→*ALICE*。

Bob 根据签名码 sign = (s, c) 计算:

$$s^{-1}\, h \cdot \boldsymbol{G} + s^{-1}\, c\, ALICE = (x_1', y_1')$$

$$c' = (x_1' + y_1')^2 \bmod 2^m$$

如果 $c = c'$, 签名被验证。

4　SCI-CPK 在 FIA 中的应用

本节给出 SCI-CPK 在三个具有代表性的未来互联网体系结构中的应用方案, 包括 XIA 中的源地址鉴别、路由通告鉴别和数据加密, MobilityFirst 中的绑定更新鉴别, 以及 NDN 中的数据源鉴别。

4.1　SCI-CPK 应用于 XIA

如图 3 所示, Alice 接入网络后, 发送信息给位于另一个网络域的 Bob, Bob 希望消息确实来自 Alice 并且没有被篡改。经 Alice 签名的消息从 Alice 发出之后, 首先由接入路由器对主机 HID 进行鉴别, 其次, 在数据包所经过的路由器上对上一跳 NID 进行验证, 最后, 由 Bob 对 Alice 进行身份认证和消息鉴别, 对收到的消息进行解密。整个过程主要包括: 密钥生成、HID 网络接入鉴别、NID 转发鉴别、路由通告鉴别和消息加解密。

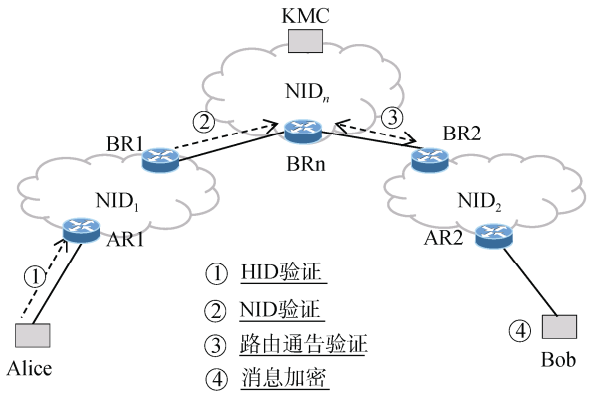


图 3　XIA 中的内生安全

(1) 组合密钥生成与获取

假设接入的网络设备名称为“Alice's Phone”(简称 A), 以此作为通信实体标识发送到 KMC 中生成该设备的组合密钥, 如图 4 所示。

KMC 根据标识字符串“Alice's Phone”进行散列变换后, 生成映射序列 YS, 取映射序列的前 160bit 作为该设备的主机标识 $\mathrm{HID_A}$, 根据映射序列

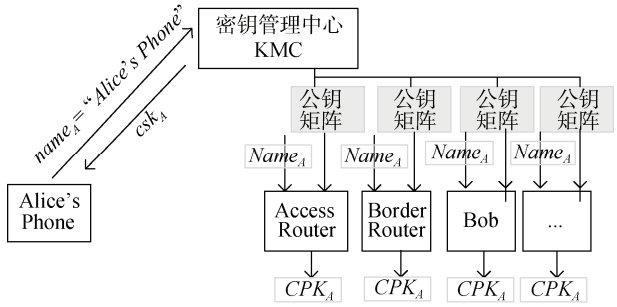


图 4　组合密钥生成与获取

的行列坐标得到组合矩阵, 然后按照有限域上的加法得到组合私钥 csk_A, KMC 将组合私钥发送给 A(或写入 Alice's Phone 的硬件卡), 并删除 csk_A。公钥矩阵以文件形式公布。其它用户按照根据标识字符串“Alice's Phone”和公钥矩阵, 查表获得 *Alice* 组合公钥 CPK_A。

(2) HID 鉴别

为了防止源地址伪造, Alice 首次接入网络后需进行网络接入鉴别, 图 5 给出了对 Alice 发出的数据包进行网络接入鉴别的流程。

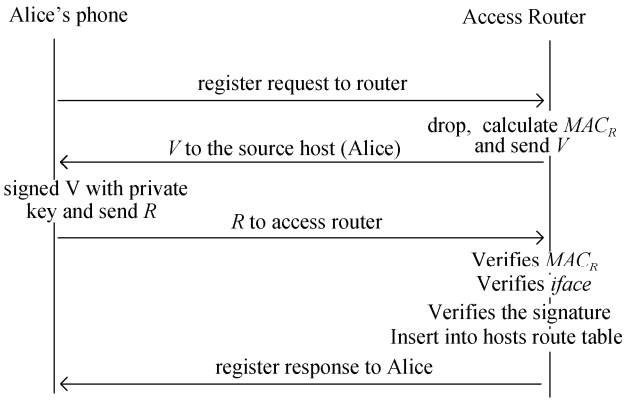


图 5　HID 接入鉴别流程

A 入网后, 获得子网 NID 和接入路由器地址, 完成 DAG 自动配置: NID1→$\mathrm{HID_A}$, 然后向接入路由器发送主机注册消息。

一般地, 接入路由器收到来自主机的数据包, 首先会检查数据包源主机标识 HID 是否存在于本地路由表中。若已经为该 HID 建立路由表项, 则表明该主机已经完成源地址鉴别, 是一个可信终端, 放行来自该主机的数据包。否则, 将来自该主机的数据包丢弃, 并向源主机发送一个验证包 $V = \{HID_{src}, HID_{dst}, iface, MAC_R\}$。

其中, HID_{src} 和 HID_{dst},代表初始数据包中源主机和目的主机标识, HID_{src} 同时也是验证包的目的地主

机标识, 这里是 HID_A。若初始数据包是主机注册消息, 则 HID_{dst} 是路由器标识, 若初始数据包是主机发往通信对端 Bob 的消息, 则 HID_{dst} 是通信对端主机标识 HID_B。*iface* 是路由器收到初始数据包的端口号, MAC_R 是接入路由器所发出验证包的消息鉴别码: $MAC_R=prf\ (\ k_R,\ HID_{src}||HID_{dst}||iface\ ),\ k_R$ 是接入路由器的秘密值。验证包的消息鉴别码 MAC_R 用来匹配之后的验证包响应消息, 也避免了接入路由器在本地对所有发出验证包状态进行缓存, 节省了存储资源。

A 收到验证数据包 *V*, 将 *V* 作为输入, 并用组合私钥 *csk* 签名, 之后返回验证包响应消息 $R = \{V, Sig_A\}$。其中, $Sig_A= Sig_{csk}(V)$。

接入路由器收到响应数据包 *R*, 进行如下判断:

根据 *R* 重新计算 MAC_R, 验证之前是否发出过与该响应消息 *R* 对应的验证消息;

判断收到响应消息 *R* 的路由器端口号, 是否等于该响应消息 *R* 中的 *iface* 值;

使用组合矩阵生成 CPK_A 对 *R* 进行关于 A 的签名验证, 即判断 $Ver_{CPK}\{V, Sig_A\}$是否为真。

如果以上条件都成立, 表明源地址验证成功, Alice 所声称的身份是真实的, 接入路由器将该移动节点的 HID_A 其加入到本地主机路由表中, 并在接下来转发来自 HID_A 的数据包。

(3) NID 鉴别

Alice 发出的数据包通过网络接入鉴别后, 由接入路由器 AR1 按照 Bob 的目的地网络标识 NID2 查询路由表进行转发, 将依次经过网络域 1 的内部路由器、边界路由器 BR, 最后转发到 Bob 所在的接入路由器上。每个路由器还要对数据包上一跳的 NID 地址进行鉴别。路由器对来自上一跳路由器的数据包进行源地址鉴别的逻辑如图 6 所示。

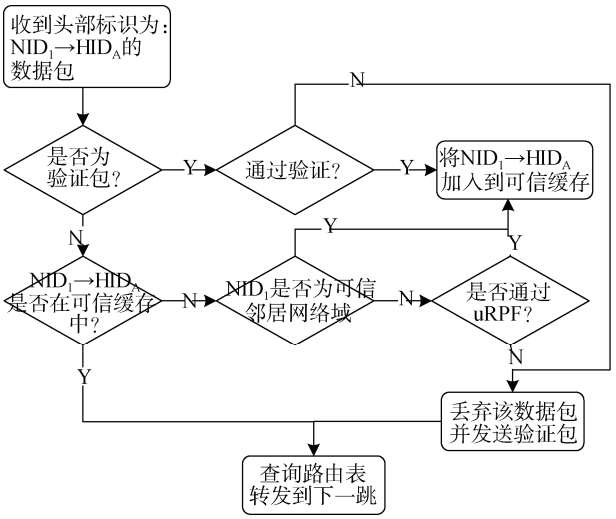


图 6　路由转发源地址鉴别逻辑

如果 NID_1 不在可信缓存中, 判断 NID_1 是否为可信的邻居网络域标识, 如果是, 则将 NID_1→HID_A 加入可信缓存, 并转发;

如果 NID_1 并非可信的邻居网络域, 执行 uRPF (universal Reverse Path Forwarding)验证, 判断去往 NID_1 的路由器端口是否与接收到来自该网络域数据包的路由器端口相同, 如果是, 则转发;

如果以上检测都失败, 则向数据源主机发送验证包, 验证过程类似 HID 验证过程。如果验证通过, 将 NID_1→HIDA 加入路由表中, 并转发。为保证可信缓存的可扩展性和响应速度, 若可信缓存中来自 NID_1 的主机大于一定数量, 则将 NID_1→*全部加入可信缓存。

(4) 路由通告鉴别

网络域内部路由器和边界路由器中路由表的建立, 需要网络域内部路由器之间通过 OSPF(Open Shortest Path First)或 RIP(Routing Information Protocol)、边界路由器之间通过 BGP(Border Gateway Protocol)交换子网或网络域的路由可达通告消息。每个路由器需要对来自其它路由器尤其是其他网络域边界路由器的路由通告消息进行鉴别, 以防止路由劫持和路由伪造的发生。在 IP 网络中保证路由通告的真实性通过 S-BGP 实现, 但其需借助公钥基础设施将用户公钥、网络前缀和证书绑定, 而绑定数据库的建立、维护和部署需要花费较大的代价。使用 CPK 的方式实现路由器之间的路由器通告消息鉴别, 能够避免上述弊端。每个路由器发布路由通告消息时用组合私钥进行签名, 其他路由器只要按照组合矩阵和网络标识就能够生成对方的组合公钥, 进而协商用于路由通告会话的对称密钥, 之后就能验证路由通告消息的真实性, 实现路由系统之间建立可信的路由关系。

(5) 消息加密

来自 Alice 的数据包经过多个路由器转发到达 Bob 所在的主机。Bob 利用组合矩阵和已知的“Alice's Phone”, 查表得出组合公钥 CPK_A, 验证 Alice 的签名, 如果签名验证正确, 即可保证该消息确实来自 Alice, 且中途没有被篡改。

如果 Alice 不希望发给 Bob 的消息中途被泄漏, 还可以将所发的消息进行加密。用对方 Bob 公钥来加密传送对称加密的会话密钥并进行加解密的过程如下。

Alice 给 Bob 的加密函数:

$$ENC_{BOB}(key) = \beta$$

$$E_{key}(data) = code$$

其中, ENC 是非对称加密函数, *BOB* 是对方公钥,

r 是随机数。

Alice 加密: 计算 Bob 的组合公钥: Bob→*BOB*

Alice 选择随机数 r, 计算

$$r\cdot BOB = \beta$$

$$r\cdot G = (x_1, y_1)$$

$$\text{key} = (x_1+y_1)^2 \bmod 2^{64}$$

$$E_{key}(\text{data}) = \text{code}$$

Alice 将{code, β}发送给 Bob

Bob 解密:

$$DEC_{bob}(\beta) = \text{key}$$

$$D_{key}(\text{code}) = \text{data}$$

其中, DEC 是非对称解密函数, *bob* 是自己的私钥。

Bob 的解密过程: 用自己的组合私钥 *bob* 计算出解密密钥

$$(bob)^{-1}\beta = r\cdot G = (x_1, y_1)$$

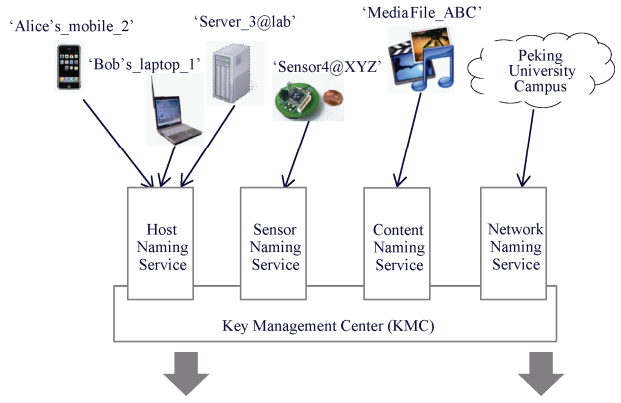
$$\text{key} = (x_1+y_1)^2 \bmod 2^{64}$$

Bob 解密后得到数据: $D_{key}(\text{code})=\text{data}$。

另外, 对于 XIA 中支持移动性的情况, 基于 CPK 的公钥签名和验证方案, 能够实现对移动节点绑定更新消息的鉴别, 对于节点频繁移动的情况, 通过基于 CPK 交换共享密钥的方式, 也能够解决绑定更新消息的快速鉴别[27]。

4.2　SCI-CPK 应用于 MobilityFirst

MobilityFirst 通过两级的映射完成 Name—GUID—NA 的动态绑定, 以支持全局的移动性。NCRS 存储着 Name 与 GUID 的对应关系, 通过使用 Name 查询 NCRS 来获取通信对端的 GUID。但 NCRS 还需要利用 PKI 生成 GUID 证书, 将 name 与对应的 GUID 绑定。本文利用 CPK 中的 KMC 即可实现 name 与 GUID 的天然绑定, 同时可以利用 NCRS 发布公钥矩阵 $R_{i,j}$), 如图 7 所示。



Name	GUID	NA
Alice's_mobile_2	11100101010...	-
Bob's_laptop_1	01010111010...	-
Server_3@seclab	10111100010...	5...
Sensor4@XYZ	10101011100...	-
Peking University	-	5...
Media File_ABC	00010111010...	3...

图 7　MobilityFirst 中融合 CPK 的 NCRS 服务

支持移动性是 MobilityFirst 的核心理念。GUID 到 NA 的动态绑定由 GNRS 负责管理。节点移动后向 GNRS 更新其 GUID 与 NA 的最新绑定, 并利用 GUID 的公钥对绑定更新签名和鉴别, 以防止 GUID 欺骗、NA 绑定伪造等攻击。利用 KMC 发布的组合公钥矩阵($R_{i,j}$)生成对应的公钥, 进而由 GNRS 对移动节点实时上报的位置信息进行鉴别, 能够满足现有方案[22]的安全要求。

4.3　SCI-CPK 应用于 NDN

在 NDN 中需要应对的一种安全威胁是内容的拒绝服务, 即如果不能确定内容所对应的名称由合法的内容发布者提供, 攻击者就能够恶意地将大量的非法内容赋予合法的内容名称, 进而引起拒绝服务攻击[28]。目前 NDN 中的解决方案是内容接收者利用 PKI 提供内容名称对应的公钥对内容进行签名验证。而利用 CPK 的方案, 内容名称可以由 KMC 生成唯一的公钥, 内容发布者通过私钥对内容签名后, 内容接收者而无需第三方的证书支持, 就能实现对内容的签名验证。

4.4　优点分析

将命名空间中通信实体标识与 CPK 公钥签名技术结合, 能够实现用户标识符、网络标识符和公钥的绑定, 为地址真实性提供证据(地址的签名), 并且任何路由器均可鉴别其真伪(验证签名)。可方便地实现主机鉴别、路由通告鉴别与消息加密, 能够从数据源端到目的端, 保证用户身份和信息内容的真实性, 保证转发过程中的真实性, 从源头上保证了网络层的内生安全。

CPK 公钥体制解决了数字签名和密钥交换以及对超大规模密钥的水平化管理, 能以较小的组合矩阵生成大量的公私钥对。如果组合矩阵大小为 $M\cdot N$, 那么存储量为 $M\cdot N$, 可组合出的密钥数量为 M^N。当 $M=N=32$ 时, $M\cdot N=1024$, 而 $M^N=2^{160}$, 从而实现了由较小的组合矩阵生成大量的密钥。同时, 基于椭圆曲线的密码生成机制还具有计算开销低的优势[25,29]。CPK 的标识认证, 只需要一次签名, 其签名长度仅为 3 字节, 而用 PKI 实现标识认证, 至少需要 3 次签名, 其签名长度长达 384 字节以上[29]。因此, CPK 能够解决未来互联网环境下海量地址鉴别的难题。

5　结论

基于组合公钥的命名方式, 区别于现有通过公钥的哈希值生成实体标识或网络地址的方案, 能够使得用户标识符、网络标识符和公钥三者天然绑定, 也同样具备自认证能力, 其无需借助公钥基础设施

便能通过公钥签名技术实现实体鉴别和消息鉴别的特点, 为身份或地址鉴别提供了极大便利。本文提出的 SCI-CPK 方案既适用于标识和地址分离的未来互联网体系结构(如 XIA 和 MobilityFirst), 又适用于命名数据网络(如 NDN), 并能以较小的组合矩阵生成大量的公私钥对, 为将来物联网和移动互联网海量设备接入场景下的大规模密钥分发和地址验证提供了技术支持。

参考文献

[1] J.P. Wu, Y. Liu, Q. Wu, "Advaces in New Generation Internet Arechitecture Theory," *Science in China (Series E: Information Sciences*), 2008, 38(10): pp. 1540 -1564 (in Chinese)
吴建平, 刘莹, 吴茜, "新一代互联网体系结构理论研究进展", *中国科学(E 辑: 信息科学)*, 2008, 38(10): pp.1540 ~ 1564.

[2] K. Xu, L. Zhu, M. Zhu, "Architecture and Key Technologies of Internet Address Security," Journal of Software, 2014, 25(1): pp. 78−97 (in Chinese)
徐恪, 朱亮, 朱敏, "互联网地址安全体系与关键技术", *软件学报*, 2014,25(1): pp.78−97.

[3] J. Pan, S. Paul, and R. Jain, "A Survey of the Research on Future Internet Architectures," IEEE Communications Magazine, July 2011.

[4] G. F. Marias, J. Barros, "Security and privacy issues for the network of the future," Security & Communication Networks, 2012, 5(9): pp. 987-1005.

[5] Z. Qazi, C. Tu, et al. "SIMPLE-fying Middlebox Policy Enforcement Using SDN," SIGCOMM'13, August 12–16, 2013, Hong Kong, China.

[6] S. Kent, C. Lynn, and K. Seo, "Secure border gateway protocol (S-BGP)," IEEE JSAC, 18(4): pp.582–592, Apr. 2000.

[7] D. Andersen, H. Balakrishnan, N. Feamster, T. Koponen, D. Moon, and S. Shenker, "Accountable Internet Protocol (AIP)," SIGCOMM'08, 2008, pp.17 – 22.

[8] "NSF FIA Project," http://www.nets-fia.net/, 2013.

[9] "NSF FIA Next Phase," http://www.nsf.gov/news/news_summ. jsp?cntn_id=131248, 2014.5.

[10] "NDN Project", http://www.named-data.net./, 2013.

[11] "MobilityFirst Project," http://mobilityfirst.winlab.rutgers.edu/, 2013.

[12] "XIA Project," http://www.cs.cmu.edu/~xia/, 2013.

[13] T. Aura, "Cryptographically Generated Addresses (CGA)," Internet Engineering Task Force, Mar. 2005. RFC 3972.

[14] D. Lewis et al. "Locator/ID Separation Protocol (LISP)," draft-ietf-lisp-22, February 2012.

[15] T. Li, "Recommendation for a Routing Architecture," RFC 6115, IETF, Feb 2011.

[16] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, "Host Identity Protocol," RFC 5201, IETF, Apr 2008.

[17] Anand, F. Dogar, et al. "XIA: An architecture for an evolvable and trustworthy Internet," Technical Report CMU-CS-11-100, Carnegie Mellon University, Feb. 2011.

[18] D. Han, A. Anand, et al. "XIA: Efficient Support for Evolvable Internetworking," The 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI'12), San Jose, CA, April 25-27, 2012.

[19] Anand, F. Dogar, D. Han, et al. "XIA: An Architecture for an Evolvable and Trustworthy Internet," Tenth ACM Workshop on Hot Topics in Networks (HotNets-X), November 14-15, 2011, Cambridge, MA.

[20] D. Naylor, M. K. Mukerjee, P. Agyapong, R. Grandl, R. Kang and M. Machado, "XIA: Architecting a More Trustworthy and Evolvable Internet," ACM SIGCOMM Computer Communication, Volume 44, Number 3, pp. 50-57, July 2014.

[21] D. Raychaudhuri, K. Nagaraja and A. Venkataramani, "MobilityFirst: A Robust and Trustworthy MobilityCentric Architecture for the Future Internet," ACM SIGMobile Mobile Computing and Communication Review (MC2R), Volume 16 Issue 4, October 2012

[22] X. Liu, W. Trappe and Y. Zhang, "Secure Name Resolution for Identifier-to-Locator Mappings in the Global Internet," IEEE International Conference on Computer Communications and Networks (ICCCN), Nassau, Bahamas, July, 2013.

[23] L. Zhang, et al. "Named Data Networking," ACM SIGCOMM Computer Communication Review (CCR), July 2014.

[24] Ghodsi, A., Teemu, K., Rajahalme, J., sarolahti, P., Shenker, S, "Naming in content-oriented architectures," Proceedings of the ACM SIGCOMM Workshop on Information-centric Networking, August 19, 2011, Toronto, Ontario, Canada.

[25] W. Tang, X. Nan and Z. Chen, "Combined public key cryptosystem," Proceedings of International Conference on Software, Telecommunications and Computer Networks (SoftCOM'04), 2004.

[26] 南湘浩, "CPK 组合公钥体制 (v8.0)", *金融电子化*, 2013(3): pp.12-16.
X.H. Nan, "Combined Public Key (v8.0)," *Electronic Finance*, 2013(3): pp.12-16.

[27] H. Meng, Z. Chen, Z. Meng and C. Song, "A Secure Route Optimization Mechanism for Expressive Internet Architecture (XIA) Mobility," The International Conference on Information and Communications Security (ICICS), 2015, pp. 269–281.

[28] D. Naylor, M. Mukerjee, and P. Steenkiste, "Balancing Accountability and Privacy in the Network," ACM Sigcomm Conference, Chicago, August 2014.

[29] 陈钟, 关志, 孟宏伟, 孟子骞, "未来网络体系结构及安全设计综述", *信息安全研究*, 2015, 1(1): pp.9-18.
Z. Chen, Z. Guan, H.W. Meng, and Z.Q. Meng, "A Survey of Future Internet Architecture and Security Design," *JOURNAL OF INFORMATION SECURITY RESEARCH*, 2015, 1(1): pp.9-18.

[30] 南相浩, 陈钟, "网络安全技术概论", 国防科学出版社, 2003.
X.H. Nan, Z. Chen, "A profile to Network Security Techniques," National Defense Science Press, 2003.

陈钟　教授, 博士生导师, 现任北京大学网络和软件安全保障教育部重点实验室主任。研究领域为计算机软件与理论、密码学、网络与信息安全。研究兴趣包括未来互联网体系结构、网络与信息安全。
Email: zhongchen@pku.edu.cn

关志　北京大学副教授。研究领域为计算机软件与理论、密码学、网络与信息安全。研究兴趣包括基于身份的密码学、网络与信息安全。
Email: guan@pku.edu.cn

孟宏伟　于 2007 年在吉林大学通信与信息系统专业获得硕士学位, 现在北京大学计算机软件与理论专业攻读博士学位。研究领域为网络与信息安全。研究兴趣包括: 未来互联网体系结构、网络与信息安全。
Email: menghw@pku.edu.cn