安全组播密钥管理的层次结构研究 [1]

朱文涛 熊继平 李津生 洪佩琳

(中国科学技术大学电子工程与信息科学系 合肥 230027)

摘 要: 组播是面向组接收者的有效数据通信方式，其重要性正日益突出。组管理协议 (IGMP) 不提供成员接入控制。为保护通信机密性，安全组播使用不为组外成员所知的业务密钥来加密数据，并随组成员关系变化而动态更新。密钥管理成为安全组播研究的核心问题。为支持大规模安全组播，引入了逻辑密钥层次结构，以使密钥管理具有可扩展性。在对逻辑密钥层次作具体分析的基础上，本文就密钥树最优结构问题作了理论上的探讨，并取得了与实验一致的结论。

关键词: 安全组播，密钥管理，层次结构，密钥树

中图分类号: TN919 **文献标识码**: A **文章编号**: 1009-5896(2004)01-0007-07

Hierarchical Key Management in Secure Multicast

Zhu Wen-tao Xiong Ji-ping Li Jin-sheng Hong Pei-lin

(*Dept. of Electron. Eng. and Info. Sci., Univ. of Sci. and Tech. of China, Hefei* 230027, *China*)

Abstract Multicast is a preferred communication technique in multiple recipients and its importance is rapidly growing. The Internet Group Management Protocol(IGMP) does not provide access control of the members. To provide communication confidentiality, traffic in secure multicast is encrypted with a session key known only by certified group members. Whenever there is a change in the group membership, the key has to be updated dynamically, thus key management is indicated as the sticking point in secure multicast research. To be applicable to large scale multicast, hierarchical structure is introduced as a solution to the scalability problem of group key management. The paper addresses the logical key hierarchy and concentrates on the optimal structure problem of the key tree. A theoretical analysis is given in the paper with the result in correspondence with a previous experimental conclusion.

Key words Secure multicast, Key management, Hierarchical structure, Key tree

1 组播及组的管理

组播是基于 UDP/IP 协议、面向多接收者的数据分发方式。图 1 是组播源 S 向成员 $M_1 \sim M_5$ 组播数据的示意图，S 传至路由器 R_1 的每一份 UDP 报文都被复制为 3 份，一份给 M_1，一份送至 M_2 和 M_3 所在的网段 (广播链路)，一份给路由器 R_2，而 R_2 再将报文生成两份拷贝分发给 M_4 和 M_5。组播数据仅在执行组播路由协议的路由器处进行最少次数拷贝 (组播树的 "分叉")，相比单播能有效节省服务器资源和网络带宽。随着 Internet 宽带化、多媒体化和商业化，组播应用也越来越广泛，如远程会议、联网游戏、电视直播及一些军用场合等。

[1] 2003-04-09 收到，2003-09-12 改回

国家 863 信息技术领域 "宽带网络中的组播安全协议及应用研究" (编号 2002AA121067) 和国家自然科学基金 "宽带网络中的组播安全模型及其机制的研究" (编号 60272043) 资助课题

因特网组管理协议 (IGMP) 用于管理组播。当前的 IGMPv2[1] 规定了主机向路由器注册组播组的操作规程，例如图 1 中 $M_1 \sim M_3$ 向组播路由器 R_1 注册，M_4 和 M_5 向 R_2 注册。IGMPv2 报文本身由目的地址为组播地址且 TTL 值为 1 的 IP 分组封装，并像 Internet Control Message Protocol(ICMP) 一样被认为是 IP 协议的一部分。图 2 给出了 IGMPv2 报文的格式，长度为 8 字节，各域的含义说明如下：

(1) "类型" 表示 IGMP 报文种类，有成员报告、退出通告和成员查询三类，其中成员报告和退出通告由主机发送，而成员查询由路由器发送；成员查询又可细分为普通查询 (路由器仅希望查询子网内哪个群组还存在成员) 和特定查询 (路由器查询某一特定群组)；

(2) "最大响应时间" 只用于查询报文，是成员应答查询的最大允许延时，单位为 0.1 s；

(3) "校验和" 对作为 IP 分组之协议净荷的整个 IGMP 报文提供保护；

(4) "组播地址" 是路由器特定查询及主机加入或退出的组地址，普通查询时该值置零。

IGMP 第三版 [2] 允许主机指定接收或拒收来自某特定地址的组播数据，并提供对 IGMPv2 的兼容。IGMPv3 才标准化不久，要得到设备生产商的支持还需一段时日。

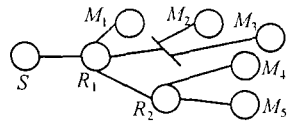

图 1 组播源向五个成员组成的群组发送数据

类型	最大响应时间	校验和
组播地址		

图 2 IGMPv2 的报文格式

2 安全组播及密钥管理

如前所述，组管理协议并不提供成员接入控制，用户只要获知特定业务使用的组播地址就可向路由器发送 IGMP 成员报告，不经审核地加入群组并获得 UDP 数据的拷贝。保护组播数据机密、建立安全通信系统是安全组播研究的主要目标。相比于端到端的单播情形，组播通信的安全问题更为复杂。将现有单播安全技术直接移植到组播应用上往往不可行或是低效的。安全组播在协议设计、策略控制及算法应用等各个方面都存在大量需要研究的问题 [3,4]。

支持安全组播的基本方法是所有成员共享一个不为组外用户所知的业务加密密钥 SEK (Session Encryption Key)。SEK 是对称密钥，组内所有通信都使用该密钥进行加密和解密。每当有用户加入或离开群组时必须更新 SEK，以使新加入成员无法访问过去的历史数据 (后向安全性 [2])，且离开的成员无法解读当前及将来的通信 (前向安全性)。该过程称为 rekey，其目的是为在成员关系变动、密钥过期或被泄露时维持 SEK 的机密性。SEK 的分发和更新是安全组播研究的核心问题，必须采用有效的密钥管理方案以减少系统付出的开销。

密钥管理的研究通常基于集中式管理和分布式管理两类基本模型。后者的特点是所有群组成员通过密钥协商 (key agreement) 来共同建立 SEK，其缺点是计算复杂导致延时很大，故难以适用于成员关系频繁变化的大规模动态群组。分布式管理不在本文的讨论范围之内。

[2] 有一些组播应用中可以不考虑后向安全性，而只需当成员退出时才更新 SEK，见文献 [10] 中的有关论述。

集中式密钥管理中存在专门的组控制者 GC(Group Controller) 负责生成通信密钥 SEK 并通过特定算法分发给规模为 N 的群组中的每个成员。本文以图 3 表示组播功能模型，其中图 3(a) 示意的是组播基本模型，图 3(b) 是引入数据加密之后的安全组播模型。从网络实际构成看(如图 1)，路由器位于组播源和组成员之间，负责拷贝和转发 UDP 数据，但在功能上可认为组播源是直接将数据 (明文或用 SEK 加密后的密文) 分发给组成员。在电视直播等场合，组播源只有一个且自身不必作为成员加入组播，而在另外一些场合如联网游戏中，所有用户在功能上都既是组播源又是数据接收者。在图 3(b) 中，GC 同时向组播源和组成员播送 SEK [3]。

一般而言，新成员加入引起的 rekey 操作相对比较容易，难点是成员删除时触发的密钥更新 [4]。例如，当新成员加入时，GC 用自己和该成员共享的密钥加密 SEK 后单播给它，并用原有成员皆知的旧 SEK 加密新 SEK 后向其余成员组播 [5]。

本文余下章节组织如下：第 3 节介绍平坦密钥管理并指出其缺陷，第 4 节论述两类典型的层次结构密钥管理，第 5 节就逻辑密钥层次结构作深入讨论，第 6 节对全文进行总结。

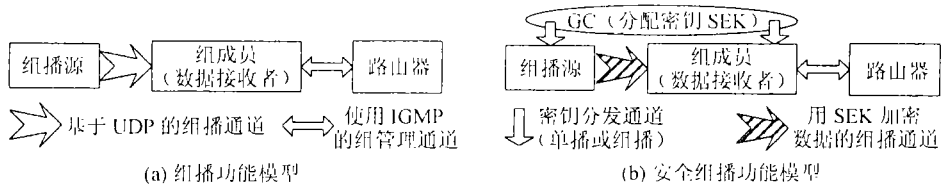

图 3　组播与安全组播 (集中式密钥管理) 的基本功能模型

3 平坦密钥管理

集中式密钥管理可进一步划分为平坦 (flat) 型和层次 (hierarchical) 型 [3]。平坦密钥管理的特点是 GC 直接向组成员分发密钥，其 rekey 开销正比于组规模 N。组密钥管理协议 GKMP[5] 是平坦密钥管理的代表，此方案中全体成员除共享 SEK 外，还使用一个加密 SEK 的组 KEK(Key Encryption Key，密钥加密密钥)。例如，当 SEK 过期时，GC 使用它加密 SEK，记作 KEK(SEK) [6]，并组播更新到组内所有成员。每个成员 M_i 还各自与 GC 共享一个秘密的 KEK$_i$ [7]。当有新成员 M_j 加入时，GC 生成 SEK$^{\text{new}}$ 和 KEK$^{\text{new}}$，用原有成员皆知的 KEK 加密它们，然后将 KEK(SEK$^{\text{new}}$, KEK$^{\text{new}}$) 组播给所有 $M_i(i \neq j)$；GC 再把 KEK$_j$(SEK$^{\text{new}}$, KEK$^{\text{new}}$) 单播给 M_j。这样新成员加入的 rekey 操作只包括一次组播和一次单播。当规模为 N 的群组中有成员 M_k 退出时，GC 依次对所有成员 $M_i(i \neq k)$ 单播 KEK$_i$(SEK$^{\text{new}}$, KEK$^{\text{new}}$)，共是 $N-1$ 次单播。

GKMP 去掉组 KEK 后可抽象为简单密钥分发中心 SKDC(Simple Key Distribution Center)，在 SKDC 中，GC 向各 M_i 依次单播 KEK$_i$(SEK)。GC 存储所有 N 个 KEK$_i$ 并负责[8]

[3] 就 GC 而言，组播源和成员都是其客户，只不过源通常具有非退出性。有些文献中“成员”也泛指包括源。

[4] 因此，下文中如未作特殊说明，rekey 均指成员退出事件所触发的密钥更新。

[5] 这涉及到组播传递密钥的可靠性问题。为简明起见，安全组播研究中通常不考虑可靠组播。IETF 的可靠组播 (Reliable Multicast Transport) 工作组见 http://www.ietf.org/html.charters/rmt-charter.html。

[6] $K(X)$ 表示用 K 来加密 X，X 是待加密消息，例如 KEK$_i$(SEK, KEK) 表示用第 i 个成员的 KEK$_i$ 加密 SEK 和 KEK。

[7] 这个带脚标的 KEK$_i$ 又叫 individual 或 pair-wise KEK，它本身由成员 M_i 经专门的身份认证后登记，例如离线注册或通过公钥体制在线传送。KEK$_i$ 不为 M_i 之外的任何用户所知，只用于 M_i 与 GC 间的保密单播通信。

生 SEK, M_i 存储仅为自己与 GC 所知的 KEK_i 并用之解密出 SEK 。 SKDC 排除一个成员时执行的 rekey 需要 $N-1$ 次加密传送， GC 的存储复杂度和通信复杂度都是 $O(N)$, 故只适合小规模组播。

已有的研究指出， rekey 通信开销和存储开销是密钥管理的一对矛盾，密钥管理往往是在通信和存储这对开销中取得一个折衷 [6−8], 其中以前者更为突出，一方面为了节省网络带宽资源，另一方面为了减少 rekey 延时，以保证组播应用的服务质量 (QoS) 。通信复杂度是当前安全组播的最大瓶颈 [7], 降低通信次数成为当前安全组播密钥管理研究所致力的目标。

SKDC 是最简单的平坦密钥管理。学术界基于数论知识提出了一些其他的方案。文献 [9] 给出了一种基于中国剩余定理的安全锁 (secure lock) 方案，可将 SEK 安全广播到每个成员，rekey 报文尺寸也不随组规模 N 增长。但安全锁的生成需要巨大的计算开销，且锁的自身长度正比于 N, 故安全锁的传送仍要产生 $O(N)$ 的通信开销，该方案也只适合于小的群组。除此之外还有安全滤波器 (secure filter) 等方案 [10,11], 它们同样具有 $O(N)$ 的通信开销。

4 层次结构密钥管理

平坦型密钥管理方案的共同特点是只适合于小型组播，随组规模 N 的增大其性能显著下降。例如， SKDC 中通信开销随 N 线性增长，是一个明显的瓶颈。为支持大规模安全组播，密钥管理方案应具有可扩展性。引入层次结构来处理大型群组的频繁密钥更新。

密钥树 (key tree) 方案通过引入中介 KEK 构造逻辑结构 [12,13], 故被称为逻辑密钥层次 LKH(Logical Key Hierarchy), 由此派生而出的一系列方案统称为树型 (tree-based) 密钥管理。图 4 所示的是一棵拥有 8 个叶节点的二叉密钥树，对应于一个成员个数为 8 的群组：树根代表 GC, 拥有的 K_0 即为业务加密密钥 SEK [8] ；叶节点代表组成员，分别拥有的 $K_{3,1} \sim K_{3,8}$ 为 M_i 与 GC 共享的 KEK_i, $i \in [1,8]$ ；虚拟的内部节点对应于中介 KEK, 用于 SEK 更新时向组内特定范围的成员传递新密钥，新密钥既包括 SEK, 也包括那些需要更换的中介 KEK 。

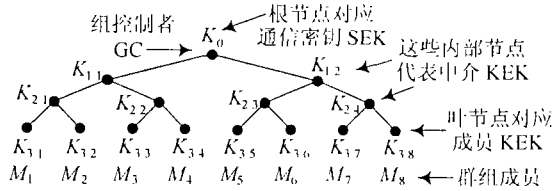

图 4 一棵度为 2 、叶节点个数为 8 的逻辑密钥树

每个成员拥有从代表它的叶节点到根节点这条路径上的所有密钥，例如成员 M_1 拥有的密钥是 $\{K_{3,1}, K_{2,1}, K_{1,1}, K_0\}$, 其中 K_0 是为所有成员共有的 SEK, $K_{3,1}$ 是仅为 GC 和 M1 所知的 KEK_1, 而 $K_{1,1}$ 和 $K_{2,1}$ 则从 GC 处获得，并用来限制密文消息只组播到包含 M_1 在内的有限集合。例如， $M_5 \sim M_8$ 不能解读用 $K_{1,1}$ 加密的消息， M_3 和 M_4 能解读用 $K_{1,1}$ 加密的消息但不能解读用 $K_{2,1}$ 加密的消息。

LKH 能有效降低 rekey 通信次数。例如，为了删除成员 M_7, GC 需向 $M_1 \sim M_6$ 及 M_8 发送 $\mathrm{SEK}^{\mathrm{new}}$, 并更换 M_7 所拥有的中介 KEK($\mathrm{K}_{2,4}$ 和 $\mathrm{K}_{1,2}$, 它们被认为是已泄密的), 为此需要 3

[8] K_0 为所有成员共享，故取 K_0 作为 SEK 。但有的文献如 [11] 认为 SEK 应再额外设置，并用 K_0 加密 SEK 。

次 rekey 通信：(1) 向 M_8 单播 $K_{3.8}(K_{2.4}^{\text{new}}, K_{1.2}^{\text{new}}, K_0^{\text{new}})$, (2) 向 M_5 和 M_6 组播 $K_{2.3}$ $(K_{1.2}^{\text{new}}, K_0^{\text{new}})$, (3) 向 $M_1 \sim M_4$ 组播 $K_{1.1}(K_0^{\text{new}})$ 。对一棵度为 d 、深度为 $\log_d N$ 的密钥树，更新 SEK(即 K_0) 所需的通信次数是

$$C_{\text{LKH}} = (d-1)\log_d N \tag{1}$$

图 3 中 d=2, N=8, 故 C=3 。研究中常取树为全满情况 (即 N 为 d 的整次幂) 作分析；若不为全满，为提高效率应将密钥树组织为平衡树或接近平衡 [14], 此时树深为 $\lceil \log_d N \rceil$ 。LKH 把通信开销降低为 $O(\log N)$ 。GC 存储所有的 KEK(包括 K_0 、各中介 KEK 和各 KEK_i), 总量是

$$S_{\text{LKH}} = \sum_{i=0}^{\log_d N} d^i = \frac{dN-1}{d-1} > N \tag{2}$$

与 SKDC 相比，LKH 牺牲密钥存储开销 (GC 和各成员都必须存储额外的中介 KEK) 换来了 $O(\log N)$ 的通信开销。当 $d = N$ 时，式 (1) 变为 $C = N-1$, 式 (2) 变为 $S = N+1$, LKH 就退化为 SKDC 。LKH 用中介 KEK 构造逻辑层次，解决了密钥管理的扩展性问题。

5 对密钥树结构的探讨

LKH 方案解决了安全组播中密钥管理的可扩展性问题，为近年来的安全组播研究所重视。本文将对 LKH 的结构参数进行研究。为说明该问题，视组规模 N 为常量参数，把式 (1) 看作密钥树度数 d 的函数：

$$C(d) = (d-1)\log_d N = \frac{d-1}{\ln d}\ln N \tag{3}$$

对 $d \geq 2$ 有 $C'(d) > 0$, 故 $C(d)$ 是递增序列，选取较小的 d 可降低通信开销。而由式 (2) 又有

$$S(d) = \frac{dN-1}{d-1} = N + \frac{N-1}{d-1} \tag{4}$$

对 $d \geq 2$ 显然 $S(d)$ 是递减序列，可见对于给定的组规模 N, 选取较大的 d 可降低存储开销。

作者认为，密钥树度数 d 的选取应使得在大多数情况下 (尤其当 N 很大时), 降低安全组播系统中最核心的开销。在 4.2 节描述的 rekey 过程中，通信和存储两方面的开销都不应是 GC 处理器的瓶颈，真正成为系统性能瓶颈的是 GC 所作的加密运算，其基本操作表现为使用一个密钥去加密另一个密钥 (例如，使用 DES 等加密算法) 。图 4 的例子中 d=2, N=8, 共存在 6 次这样的加密运算。

因此，本文认为可从 GC 端计算开销的角度来考查密钥树的结构。当树保持平衡且接近全满时，相应于式 (1) 给出的 C 次通信，GC 进行一次 rekey 操作所要完成的加密次数是

$$E_{\text{LKH}} = (d-1)\sum_{i=1}^{\lceil \log_d N \rceil} = \frac{(d-1)\lceil \log_d N \rceil \lceil 1+\log_d N \rceil}{2} \tag{5}$$

例如当 N=10000 (用科学记数法记为 1e4, 下同) 时，按式 (5) 依次对 $d = 2, 3, 4, \cdots, 20$ 计算 E_{LKH}, 其结果如表 1 所示 [9] ：

[9] 因无法保证密钥树全满，式 (3) 的计算结果与实际情况会有略微出入，再考虑到为保持密钥树平衡或基本平衡所作的结构调整，以及具体实现 LKH 时的技术细节，GC 的开销实际上不可能用解析公式精确刻画出。

表 1 N=1e4 时 GC 端为完成一次 rekey 所做的加密次数

d	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
E	105	90	84	84	105	90	105	120	90	100	110	120	130	140	150	160	170	180	190

由表 1 可求得 N=1e4 时密钥树的最优度数为 d_{opt}=4 或 5 。依次令 N=1e4, 2e4, 3e4, $\cdots$, 100e4, 类似求解 E_{LKH} 达到最小值时的 d_{opt}, 其结果如图 5 所示。作者注意到很难对 d_{opt} 随 N 增长而变动的现象给予规律性的描述。当 N=2e4 和 3e4 时, d_{opt} 与表 1 中情况相仿, 都存在两个解, 这一现象在图 5 中以三角符号标明。从这 100 个采样点求得的 d_{opt} 来看, d=4 占据了 59% 的份额。进一步的计算表明, 在 N 从 200e4 到 400e4 的范围内 (采样间隔仍取 1e4), d_{opt}=4 的比率高达 95% 。因此, 本文认为取度数 d=4 是 LKH 方案中密钥树的最优结构。

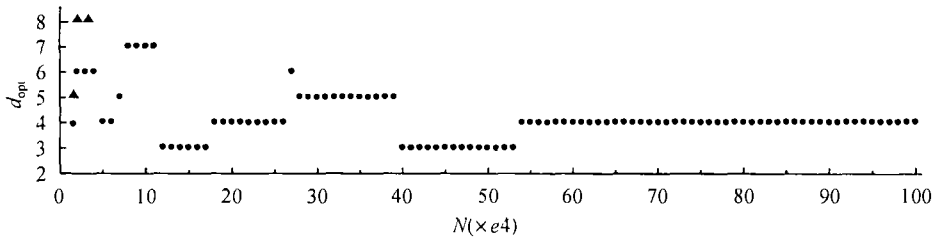

图 5 组规模 N 从 1e4 到 100e4 时 d_{opt} 的分布情况

作者注意到曾有学者以完全不同的方法就相同的问题作了研究。文献 [12] 通过搭建测试平台模拟 GC 与大规模组播成员进行通信的过程, 实验测得, 为了减小 GC 端的运行负荷, 密钥树的最优度数应取为 d_{opt}=4 附近。进一步, 文献 [15] 对 LKH 进行了改进, 通过将时间上相邻的多个变动成员按批集中进行 rekey 来减少 GC 的工作量, 实验结果也表明密钥树的最优度数应取 d_{opt}=4 。这与本文的分析结果相符, 从而验证了本文所作的理论研究。

6 结论

安全组播正在逐渐成为一个活跃的研究领域, 密钥管理作为其关键研究内容必须解决在大规模组播情况下的可扩展性问题。近年来, 基于逻辑密钥树的 LKH 方案成为密钥管理的研究基础。本文对密钥管理及其层次化方案作了论述, 提出了最优层次结构的问题。作者用数值分析的方法证明了 LKH 方案中逻辑密钥树的最优度数是 d=4, 该结果与使用实验方法进行独立研究获得的结论是一致的。

参 考 文 献

[1] Fenner W. Internet group management protocol, Version 2. IETF RFC2236, November 1997.

[2] Cain B, Deering S, Kouvelas I, Fenner B, Thyagarajan A. Internet group management protocol, Version 3. IETF RFC3376, October 2002.

[3] Krusus P S, Macker J P. Techniques and issues in multicast security. Military Communications Conference, Boston, USA, 1998, Vol.3: 1028–1032.

[4] Canetti R, Pinkas B. A taxonomy of multicast security issues. Internet Draft, http.// www.securemulticast.org/smug-drafts.htm, August 2000.

[5] Harney H, Muckenhirn C. Group Key Management Protocol (GKMP) architecture. IETF RFC2094, July 1997.

[6] Mingyan Li, Poovendran R, Berenstein C. Design of secure multicast key management schemes with communication budget constraint. *IEEE Communications Letters*, 2002, 6(3): 108–110.

[7] Snoeyink J, Suri S, Varghese G. A lower bound for multicast key distribution. IEEE INFOCOM 2001, Anchorage, USA, 2001, Vol.1: 422–431.

[8] Poovendran R, Baras J S. An information-theoretic approach for design and analysis of rooted-tree-based multicast key management schemes. *IEEE Trans. on Information Theory*, 2001, 47(7): 2824–2834.

[9] Guang-Huei Chiou, Wen-Tsuen Chen. Secure broadcasting using the secure lock. *IEEE Trans. on Software Engineering*, 1989, 15(8): 929–934.

[10] Kuen-Pin Wu, Shanq-Jang Ruan, Feipei Lai, Chih-Kuang Tseng. On key distribution in secure multicasting. 25th Annual IEEE Conference on Local Computer Networks, Tampa, USA, 2000: 208–212.

[11] Trappe W, Jie Song, Poovendran R, Liu K J R. Key distribution for secure multimedia multicasts via data embedding. Acoustics, Speech, and Signal Processing, Salt Lake City, USA, 2001, Vol.3: 1449–1452.

[12] Chung Kei Wong, Gouda M, Lam S S. Secure group communications using key graphs. *IEEE/ACM Trans. on Networking*, 2000, 8(1): 16–30.

[13] Wallner D, Harder E, Agee R. Key management for multicast: Issues and architectures. IETF RFC2627, June 1999.

[14] Moyer M, Rao J, Rohatgi P. Maintaining balanced key trees for secure multicast. Internet Draft, http.//www.securemulticast.org/smug-drafts.htm, June 1999.

[15] Xiaozhou Steve Li, Yang Richard Yang, Mohamed G. Gouda, Lam S S. Batch rekeying for secure group communications. 10th International Conference on World Wide Web, Hong Kong, May 2001: 525–534.

朱文涛：　男，1979 年生，博士生，主要研究方向为通信协议和网络安全.

熊继平：　男，1982 年生，硕士生，主要研究方向为安全组播和下一代互联网技术.

李津生：　男，1937 年生，教授，博士生导师，主要研究领域为下一代网络体系结构.

洪佩琳：　女，1961 年生，教授，博士生导师，主要研究领域为网络策略控制和信息安全.