

广播加密方案研究

陈燕俐^{1,2}, 杨庚¹, 曹晓梅¹

(1. 南京邮电大学 计算机学院, 江苏 南京 210003;

2. 福建师范大学 网络安全与密码技术重点实验室, 福建 福州 350007)

摘 要:广播加密作为一种将数据内容通过广播信道安全地分发给合法用户的安全机制,目前在付费电视、视频会议、无线传感网络等方面得到了广泛的应用。密钥存储量、通信开销和计算开销是评价广播加密方案性能的主要指标。介绍了广播加密方案的发展和研究现状;对各类广播加密方案的基本原理、特点进行了阐述,并对方案的性能和应用进行了比较和总结;重点研究了其中的公钥广播加密方案,指出了由于公钥广播加密方案不需要信任中心,并且具有任何一个用户都可以广播数据的特点,在无线传感器网络方面有着很大的应用前景。

关键词:广播加密;子集覆盖;无状态接收者;无线传感器网络

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2010)10-0189-05

A Survey of Research on Broadcast Encryption

CHEN Yan-li^{1,2}, YANG Geng¹, CAO Xiao-mei¹

(1. College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;

2. Key Lab of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China)

Abstract: Broadcast encryption provides a convenient way to distribute digital content to subscribers over an insecure broadcast channel. It has been applied to various applications such as satellite TV subscription services, audio/video, wireless sensor networks, etc. The efficiency of a broadcast encryption scheme is mainly measured by three parameters: length of transmission messages, users' storage, and computational overhead. In this paper the current research and development of broadcast encryption schemes are introduced. Mechanisms and characteristic of various broadcast schemes are described, performances of schemes are compared and application scenarios are discussed. The application prospect of public-key broadcast schemes in wireless sensor network is pointed out lastly.

Key words: broadcast encryption; subset-cover; stateless receiver; wireless sensor networks

0 引言

广播加密提供了一种在非安全的信道上以便捷的方式来分发数字信息给用户的方法,在付费电视、视频会议和无线传感网络等场合有着很广阔的应用前景。在付费电视实时点播中,要确保只有付费用户才能看到节目内容;在视频会议中,通常需要确保会议内容的保密性。作为目前计算机科学领域研究热点的无线传感器网络,它的主要通信模式就是广播,安全广播已成为无线传感器网络的重要研究内容。

广播加密是在广播信道上传输加密的消息,只有发送者选定的授权(或称合法)用户才能解密,得到明文消息。和点对点通信加密相比,不安全的广播信道,以及用户可以随时加入和退出授权用户集的动态变化都对广播加密提出了更高的安全要求。设 N 为广播用户集,包括所有的广播用户 $\{U_1, U_2, \dots, U_n\}$, $n = |N|$ 为广播用户总数, TA 为信任中心; 2^N 表示所有用户子集的集合(含空集), $S \subseteq N$ 表示当前广播的授权(或称合法)用户的集合, $m = |S|$ 为授权用户数, $ST \subseteq 2^N$ 表示所有授权子集的集合,称为特权子集; $R = N \setminus S$ 表示当前非授权的撤销(或称退出)用户的集合, $r = |R|$ 为撤销用户数, $RT \subseteq 2^N$ 表示所有撤销子集的集合,称为禁止子集。 MT_S 表示对 S 可能广播的消息集合,对所有的 S , 假定 $MT_S = MT$, 更进一步可以假定存在 MT 上概率分布, TA 根据概率分布选择明文 $M_S = MT$, K_i 表示用户 U_i 的密钥信息, 那么广播的密文 C_S 是关于 M_S 和用户集 S 对应的密钥信息集 K_S

收稿日期:2010-01-28;修回日期:2010-04-30

基金项目:国家自然科学基金(60873231);江苏省自然科学基金(08KJB520006);福建省网络安全与密码技术重点实验室开放课题(09A010)

作者简介:陈燕俐(1969-),女,江苏常熟人,副教授,博士生,研究方向为计算机网络、信息安全;杨庚,教授,博士生导师,博士后,研究方向为计算机通信与网络、网络安全、分布与并行计算等。

的函数,对每个用户 $U_i \in S$,都能独立地解密 C_S 得到 M_S ;而 $\forall R \in RT$ 不能计算出 M_S (注:下文中所用符号的含义同上,不再重复说明)的函数,对每个用户 $U_i \in S$,都能独立地解密 C_S 得到 M_S ;而 $\forall R \in RT$ 不能计算出 M_S (注:下文中所用符号的含义同上,不再重复说明)。

广播加密方案需要解决的基本问题:

(1)保密:只有拥有解密密钥的授权用户才能获得广播明文。

(2)抗同谋:撤销用户即使联合起来,也无法获得广播明文。如果所有的撤销用户联合起来也无法解密得到明文,则称该方案可抗完全同谋。

(3)用户的动态加入和退出:应保证前向安全,即退出的用户无法利用它们所知的密钥解密后继的广播密文;在某些情况下还应保证后向安全,即新加入的成员无法破解它加入之前的广播密文。

评价广播加密方案性能的主要指标有:

1)密钥存储量,主要是指接收用户需要存储的密钥大小和数量;

2)通信开销,即广播密文包的长度;

3)计算量,即加密、解密的计算开销。

1 广播加密方案

广播加密的提出来自于 1991 年 Berkovits 的《How to broadcast a secret》^[1],1993 年 Amos Fiat 和 Moni Naor 所写的《broadcast encryption》^[2]确立了 this 领域。自此广播加密得到了广泛的关注和多方面的研究,大量相关的广播加密方案被提出。根据使用场景不同,主要可分为有状态广播加密(stateful broadcast)和无状态广播加密(stateless broadcast)两类。

1.1 有状态广播加密

有状态广播加密方案是针对有状态接收者的,指接收者可以保存接收信息,用户可以根据接收到的广播信息对存储的密钥进行更新。该类方案的特点:由于密文是用当前组用户(即授权用户)共享的组密钥进行加密,密文短 $O(1)$,计算量小,但当组用户发生动态变化时,即有用户加入和退出,此时为了保证广播安全,组内的其它用户的密钥都必须更新,此时通信量较大。另外有状态加密要求所有用户一直处于在线状态,因此在实际应用中受到一定的限制。

最典型有状态广播加密方案即 1997 年和 1998 年由 Wallner 和 Wong 分别独立提出的基于逻辑密钥树(LKH)的组播方案^[3,4],方案可抗完全同谋。LKH 方案中,当前的授权用户共享一个相同的对称密钥,称为组密钥。每个用户除了存储组密钥外,还存储一系列

更新密钥。一棵高为 h 的二叉平衡逻辑密钥树,它的授权用户(组用户)个数 m 为 2^{h-1} ,每个授权用户保存的密钥数量为 h ,组控制器保存的密钥数量为 $2^h - 1$ 。当有用户加入和退出,密钥更新需要的通信量为 $O(2r \log_2 m)$, r 为加入或退出的用户数。之后又出现了很多基于树结构的改进方案^[5-9],对逻辑密钥树的改进包括以下几个方面:降低组控制器和接收用户需要保存的密钥数量;减少密钥更新所需要的通信量;提高对频繁的动态用户关系变化的适应性,但除非方案的接收用户密钥存储量很大,否则通信量仍然为 $O(r \log_2 m)$ 。

1.2 无状态广播加密

无状态广播加密是指接收者不能改变其初始状态(例如修改用户密钥),仅按照初始设置的密钥处理接收到的广播数据,由于接收用户密钥不需要更新,因此不要求用户一直处于在线状态。无状态广播加密方案可分为基于对称密钥的广播加密和基于公钥的广播加密两类。前者的特点是网络中必须有一个信任中心,信任中心产生并拥有所有用户的密钥,只有信任中心才能广播信息,这类方案对信任中心的依赖性会导致单一失效点问题。而基于公开密钥的加密方案克服了这个缺点,公钥可以存储在每一个用户或任一个用户都可以存取的共享存储设备上,也可以广播给用户,因此所有的用户都可以用公钥加密并广播消息。

1.2.1 基于对称密钥的广播加密

2001 年,Naor 提出了一个应用于无状态接收者(stateless receiver)的“子集覆盖”框架(Subset - Cover)^[10],基于该框架的广播加密方案由三个算法组成:

(1)初始化:将所有的用户集合 N 分成不同的子集 $L_1, L_2, \dots, L_w \subseteq N$,每个集合 L_i 分配一个密钥 k_i ($1 \leq i \leq w$),系统分配给每个用户 u 秘密信息 P_u ,使得对于 $\forall u \in L_i$ 的用户可通过 P_u 计算出 L_i ,即每个用户属于若干个集合,该用户持有其所属所有集合对应的密钥。

(2)广播加密:调用 Cover 算法将授权用户集合 $N \setminus R$ 划分为互不相交的子集 $\{p_{i_1}, p_{i_2}, \dots, p_{i_m}\}$,这些集合的并集覆盖了所有的授权用户 S ,即每个合法用户属于且仅属于这其中的某一个集合。广播方选取会话密钥 K ,分别用这些划分子集对应的密钥 $\{k_{i_1}, k_{i_2}, \dots, k_{i_m}\}$ 对会话密钥 K 进行加密,而发送的消息 M 用会话密钥 K 进行加密,密文形如 $\langle [i_1, i_2, \dots, i_m, E_{k_{i_1}}(K), E_{k_{i_2}}(K), \dots, E_{k_{i_m}}(K)], E_k(M) \rangle$,方括号内的部分称为广播头, $E_k(M)$ 称为广播体。

(3)用户端解密:每个合法用户接收到加密消息

后,在广播头中寻找到用自身所属集合的密钥加密的数据,使用自身持有的密钥对其进行解密后即可获得会话密钥 K ,并用 K 对广播体进行解密获得消息 M 。

文献[10]还给出了基于该框架的两种具体实现方法:完备子树(Complete Subtree, CS)法和子集差分(Subset Difference, SD)法,两种方案均可抗完全同谋,保证前向安全,但不提供后向安全。

基于子集覆盖框架下的进一步研究成果是 Halevy 和 Shamir 的 LSD(Layered Subset Difference)方法^[11], Goodrich 的 SSD(Stratified Subset Difference)方法^[12],它们通过对二叉树特殊层进行标号或进一步分层将子集差分法进一步完善,降低了通信开销。方案在较低的密钥存储情况下,还可以保持 $O(r)$ 的传输成本。四种方法的性能比较见表 1。

1.2.2 基于公钥的广播加密

第一个公钥广播加密方案是由 Naor 和 Pinkas^[13]于 2000 年提出的,方案采用了门限秘密共享方法。公钥密码体制的引入可解决对称密钥带来的安全性问题以及只有信任中心才能广播加密信息的缺点。此后公钥广播加密得到更多人的研究和关注,相关文献不断发表,研究内容主要集中在如何减小公私钥大小、密文大小和加密解密的计算复杂度。

基于公钥的广播加密方案的安全性基本上都是基于 BDH 假设(Bilinear Diffie-Hellman assumption)及其广义变形,如 BDHE 假设(Bilinear Diffie-Hellman Exponent assumption)。在 2001 年 Boneh 和 Franklin 提出的第一个实用的基于身份加密(Identity Based Encryption, IBE)方案中^[14],形式化定义了 BDH 假设,此后 BDH 假设的几种变形也相继被提出。

(1)多公钥广播加密。

2002 年 Dodis and Fazio^[15]将“子集覆盖”对称广播加密转换为公钥广播加密,即将原方案中划分成的每个子集所对应的密钥转化为一对公钥/私钥,广播方在广播时选取一会话密钥,分别用这些划分子集对应的公钥对会话密钥 K 进行非对称加密,而发送的消息 M 用会话密钥 K 进行对称加密。为减少大量公钥带来的存贮开销,在 CS 方法中使用了基于身份的公钥加密^[14],而在更高效的 SD 和 LSD 方法中,使用了分层

结构的基于身份的公钥加密算法(Hierarchical Identity Based Encryption, HIBE)^[16,17]。基于身份加密的基本思想是公钥可以是任何唯一的字符串,如 e-mail 地址、身份证或其他标识^[18]。采用 IBE 和 HIBE,发布方不再需要发布大量的用户公钥,用户也不再需要存贮大量公钥,私钥存贮量、通信开销和对称密钥相同。

文献[19,20]提出了一种基于身份的广播加密方案,安全性基于 BDH 假设。方案实际上是采用了基于身份的多接收者公钥加密(Multi-Receiver Identity-Based Encryption)的思想,每个用户只存贮一对公钥/私钥(pki, ski)以及很少的一些公共参数,广播方用各授权用户的公钥对信息进行加密,授权用户可以用自己的私钥解密密文得到明文。多公钥广播加密方案的用户存贮开销小,但密文的长度为 $O(m)$,因此当授权用户较多时,通信开销较大。

(2)固定公钥广播加密。

2005 年 Boneh, Gentry, and Waters 提出公开密钥广播加密方案(BGW 方案)^[21],方案安全性基于 BDHE 假设,抗完全同谋,广播密文长度短,克服了以往密文长度会随着授权用户的个数而线性增加的缺点。和多公钥广播加密方案有多个公钥不同,该类方案的公钥只有一个。方案由三个算法组成:Setup, Encrypt 和 Decrypt 分别完成系统公钥、私钥的建立,广播加密和用户端解密。

Setup: 给定所有的广播用户数 n ,生成公钥 PK , n 个用户的私钥 d_1, d_2, \dots, d_n ,

Encrypt: 给定当前授权用户集 $S \subseteq \{1, \dots, n\}$, 公钥 PK , 输出会话密钥 K , 广播头 Hdr 。设 M 为广播信息,广播密文由 (S, Hdr, C_M) 三部分组成, C_M 为采用对称加密算法加密的广播信息,密钥为 K 。由于 BGE 基本方案中的 $Hdr = (C_0, C_1)$,仅包含两个群元素,因此不包括 S 的情况下,密文长度和授权用户无关,始终为固定值。

Decrypt: 用户 i 收到密文后,首先通过广播头 Hdr 和该用户的私钥 d_i ,计算得到会话密钥 K ,然后通过 K 解密 C_M 得到广播明文 M 。

方案中,各用户私钥的大小为 $O(1)$,密文包的长度以及公钥的大小均为 $O(\sqrt{n})$,或密文包的长度固

表 1 基于子集覆盖框架的广播加密方案性能比较

方法	信息包长度	密钥存贮量(接收方)	广播方处理时间	接收方处理时间
完全子树法(CS)	$O(r \log n / r)$	$O(\log n)$	$O(\log \log n)$	$O(1)$
子集差分法(SD)	$O(r)$	$O(\log^2 n)$	$O(\log n)$	$O(1)$
层次子集差分法(LSD)	$O(r)$	$O(\log^{3/2} n)$	$O(\log n)$	$O(1)$
分层子集差分法(SSD)	$O(r)$	$O(\log n)$	$O(\log n)$	$O(n^{l/k})$ k 为常量

定,公钥的大小为 $O(n)$ 数量级。该方案虽然密文包或私钥的长度固定,但由于用户执行解密时需要用到公钥,因此不论公钥是存贮在接收用户,还是需传送给接收用户,都会导致系统存贮开销为 $O(n)$ 或通信开销为 $O(n)$ 。

针对 BGW 方案的问题,2008 年 Jong Hwan Park 提出的公开密钥方案^[22]通过解密时只需要用到部分公钥的方法,达到减少通信量的目的。方案利用了双线性对以及强 Diffie-Hellman 元组(Strong Diffie-Hellman tuples)的代数特性,由于在解密时只需用到公钥的一部分和 S 相关的子集,因此在传递公钥的情况下,该方案的通信量为 $O(m)$, m 为授权用户数;而 BGE 方案的通信量为 $O(n)$, n 为所有的广播用户数。值得注意的是,该方案经过修改,通信量可为 $O(r)$,因此在撤销用户数量 r 较小的情况下,采用该方案可以进一步提高通信效率。方案的缺点是解密时计算开销加大。

(3) 动态公钥广播加密。

文献[23,24]方案采用了动态广播加密^[25]的部分思想,在系统初始建立时,广播用户的总数不固定,可以动态发生变化。方案由于采用基于身份的公钥广播加密,发送者能发送密文给任何接收者,这些接收者不需要在系统建立过程中出现,因此公钥大小不依赖于广播用户总数 n (包括潜在的接收者),而是和授权用户的最大数目成比例关系,而密文和私钥的大小和 BGW 方案相同,是固定常量,这在以前的广播加密中是没有实现过的一个优良特性。而且该方案还具有当授权用户不发生动态变化时,计算量很小的优点。方案的缺点是当接收用户集合发生变化时,如有用户加入或离开时,计算开销比 BGW 方案要大。因此该方案适合 n 较大,但授权用户的最大数量较少,并且授权用户集合不经常发生变化的情况。

三种可抗完全同谋的公钥广播加密方案性能比较如表 2 所示。

表 2 三种公钥广播加密方案的性能比较

	方案[19]	方案[21]	方案[23]
信息包的长度	$O(m)$	$O(1)$	$O(1)$
私钥的长度	$O(1)$	$O(1)$	$O(1)$
公钥的长度	$O(1)$	$O(n)$	$O(l)$
加密解密的计算量 (S 不发生变化)	$O(m)$	$O(1)$	$O(1)$
加密解密的计算量 (S 发生变化)	$O(m)$	$O(t^2)$	$O(t)$

注: l 为接收用户集的最大数, t 为集合动态变化的用户数。

2 广播加密在无限传感器网络的应用

无线传感器网络(Wireless Sensor Networks, 简称 WSNs)^[26]目前已成为计算机科学领域一个活跃的研究分支,应用前景十分广阔。和 Internet 网络中通常采用点对点单播通信方式不同,它的主要通信模式是广播,因此安全广播是无线传感器网络安全的重要研究方向。

由于 WSN 是一种资源受限的网络,计算速度、电源能量、通信能力和存储空间都是非常有限的,传统网络的广播加密方案并不能完全适合 WSN 广播安全的应用。

到目前为止,国内外针对传感器网络的广播加密方案,基本是都是采用通信量较小的有状态广播加密,而对无状态广播加密的研究基本上还是一片空白,目前只有文献[19,20]中的公钥广播加密方案是针对传感器网络的。

笔者认为无状态广播加密在无线传感器网络中有着很大的应用前景:

(1) 由于受无线信道的不稳定、恶劣的工作环境等条件的限制,传感器节点并不能保证一直处于在线状态以及及时更新密钥;

(2) 一些可防篡改的传感器网络节点中的密钥是不可修改的;

(3) 无线传感器网络具有无中心和自组网特性,通常情况下,所有节点的地位都是平等的,没有预先指定的中心,而公钥广播加密方案不需要信任中心的特点正适合无线传感器网络的这种拓扑结构。

笔者认为:通过将传统的针对有限网络的公钥广播加密方案进行修改、优化;分析算法的复杂性、安全性、能量和存贮需求等,提出一种在计算复杂性、存贮需求、能量消耗以及通信带宽需求均有效的,适合于无线传感器网络的基于 ECC 的广播加密方案是非常有意义的,也是可行的。

3 结束语

广播加密方案是把数据内容通过广播信道安全地分发给经过授权的合法用户的安全机制,它在付费有线电视和卫星电视、视频会议、无线传感网络、在线数据库中起着愈加重要的作用,其安全性已成为目前研究的热点。

文中对有状态广播加密方案和无状态广播加密方案,特别是对其中的公钥广播加密方案进行了深入的研究,并对方案的性能做了分析和比较。由于有状态广播加密方案当有用户加入和退出广播时通信量较大,通常适用于用户一直处于在线状态,或授权用户集

基本是固定的情况;无状态加密广播密文长度大于有状态广播加密,但当用户动态发生变化时不需要密钥更新。

它适用于以下一些情况:

- (1) 用户不能改变其初始设置状态;
- (2) 用户有时会处于离线状态;
- (3) 授权用户数较多,撤销用户数较少。

由于公钥广播加密方案不需要信任中心,并且具有任何一个用户都可以广播数据的特点,在传感器网络方面有着很大的应用前景。

参考文献:

- [1] Berkovits S. How to broadcast a secret[C]//Proceedings of Eurocrypt. [s.l.]:Springer - Verlag,1991:536 - 541.
- [2] Fiat A, Naor M. Broadcast encryption[C]//Proceedings of Crypto. [s.l.]:Springer - Verlag,1993:480 - 491.
- [3] Wallner D M, Harder E J, Agee R C. Key management for multiast: issues and architectures[S]. RFC 2627. 1999.
- [4] Wong C K, Gouda M, Lam L S. Secure group communications using key graphs[C]//ACM SIGCOMM. [s.l.]: [s.n.], 1998:68 - 79.
- [5] Perrig A, Song D, Tygar J D. A new protocol for efficient large - group key distribution[C]//Proceedings of the IEEE Symposium on Security and Privacy. [s.l.]: IEEE, 2001: 247 - 262.
- [6] Waldvogel M, Caronni G, Sun D, et al. The VersaKey framework: Versatile group key management[J]. IEEE J. Sel. Areas Commun(Special Issue on Middleware), 1999, 17(9): 1614 - 1631.
- [7] McGrew D A, Sherman A T. Key establishment in large dynamic groups using one way function trees[J]. IEEE Transactions on Software Engineering, 2003, 29(5): 444 - 458.
- [8] Canetti R, Garay J, Itkis G, et al. Multicast Security: A Taxonomy and Some Efficient Constructions[C]//proceedings of the IEEE INFOCOM. [s.l.]: IEEE, 1999: 708 - 716.
- [9] Canetti R, Malkin T, Nissim K. Efficient communication - storage tradeoffs for multicast encryption[C]//Advances in Cryptology EUROCRYPT. [s.l.]: Springer - Verlag, 1999: 459 - 474.
- [10] Naor D, Naor M, Lotspiech J. Revocation and Tracing Schemes for Stateless Receivers[C]//Proceedings of Crypto. [s.l.]: Springer - Verlag, 2001: 41 - 62.
- [11] Dani H, Adi S. The lsd broadcast encryption scheme[C]//Advances in Cryptology - Crypto. [s.l.]: Springer - Verlag, 2002: 47 - 60.
- [12] Goodrich Michael T, Sun Jonathan Z, Tamassia R. Efficient tree - based revocation in groups of low - state devices[C]//Advances in Cryptology - Crypto. [s.l.]: Springer - Verlag, 2004: 511 - 527.
- [13] Naor M, Pinks B. Efficient trace and revoke schemes[C]//Financial cryptography: 4th international conference. [s.l.]: IEEE, 2001: 1 - 20.
- [14] Boneh D, Franklin M. Identity - based encryption from the Weil pairing [C]//Advances in Cryptology Crypto. [s.l.]: Springer, 2001: 213 - 229.
- [15] Dodis Y, Fazio N. Public broadcast encryption for stateless receivers[C]//DRM Workshop. [s.l.]: IEEE, 2002: 61 - 80.
- [16] Horwitz J, Lynn B. Toward hierarchical identity - based encryption[C]//Advances in Cryptology - EuroCrypt. [s.l.]: Springer, 2002: 466 - 481.
- [17] Dan B, Xavier B, Goh Eu - Jin. Hierarchical identity based encryption with constant size ciphertext[C]//Advances in Cryptology - EuroCrypt. [s.l.]: Springer, 2005: 440 - 456.
- [18] Shamir A. Identity - based cryptography and signature schemes[C]//Advances in Cryptology Crypto. [s.l.]: Springer, 1984: 47 - 53.
- [19] Du X, Wang Y J, Wang Ge Y. An ID - based broadcast encryption scheme for key distribution[J]. IEEE Transaction on broadcasting, 2005, 31(2): 264 - 266.
- [20] Yang Geng, Wang Jiangtao, Cheng Hongbing, et al. An Identity - Based Encryption Scheme for Broadcasting[C]//IFTP International Conference on Network and Parallel Computing. [s.l.]: IEEE, 2007: 123 - 126.
- [21] Boneh D, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys[C]//Advance in Crypto. [s.l.]: Springer, 2005: 258 - 275.
- [22] Park Jong Hwan, Kim Hee Jean, et al, and Lee Dong Hoon. Public Key Broadcast Encryption Schemes With Shorter Transmission[J]. IEEE Transactions on Broadcasting, 2008, 54(3): 401 - 411.
- [23] Ryuichi S, Jun F. Identity - based broadcast encryption[EB/OL]. 2007 - 02 - 15. <http://eprint.iacr.org/2007/217>.
- [24] Delerablee Cecile. Identity - based broadcast encryption with constant size ciphertexts and private keys[C]//Proceedings of Asiacypt. [s.l.]: IEEE, 2007: 200 - 215.
- [25] Cecile D, Pascal P, David P. Fully collusion secure dynamic broadcast encryption with constant - size ciphertexts or decryption keys[C]//PAIRING 2007. [s.l.]: Springer - Verlag, 2007: 39 - 59.
- [26] Liu D, Ning P, Li R. Establishing pairwise keys in distributed sensor networks[J]. ACM Transactions on Information and System Security, 2005, 8(1): 41 - 77.