基于访问结构上秘密共享的自治愈群组密钥分发方案

彭清泉 裴庆祺 庞辽军
(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)

摘 要 自治愈的群组密钥分发能够在不可靠的网络中建立安全的群组会话密钥。基于用户可自行选取子秘密访问结构上的秘密共享方法,提出了一个自治愈的群组密钥分发方案,该方案能够让群组成员自行选取个人秘密信息,而不需要在群组管理员和每个群组成员之间建立安全信道。安全性分析表明,该方案是一个具有撤销能力的、保证前向保密性和后向保密性的、计算上安全的自治愈群组密钥分发方案。性能分析表明,该方案具有较小的存储开销和通信开销。

关键词 群组密钥分发,自治愈,秘密共享,访问结构
中图法分类号 TP393.08 **文献标识码** A

Self-healing Group Key Distribution Scheme Based on Secret Sharing with Access Structures

PENG Qing-quan PEI Qing-qi PANG Liao-jun
(Ministry of Education Key Laboratory of Computer Networks and Information Security, Xidian University, Xi'an 710071, China)

Abstract Self-healing group key distribution enables group of users to establish group session keys for secure communication over an unreliable networks. Based on a secret sharing method with access structures in which each user's secret shadow is selected by the user himself, a self-healing group key distribution scheme was proposed. The scheme enables each group member's personal secret key is selected by the member himself, the group manager dose not have to distribute each member's personal secret key, no secure channel is required to be established between the group manager and each member. The security of the scheme was analyzed in a system security model, the analysis results show that it is a computational secure self-healing group key distribution scheme with revocation capability and achieves both forward and backward secrecy. Finally, the performance analysis results show that the proposed scheme has less storage cost and communication cost.

Keywords Group key distribution, Self-healing, Secret sharing, Access structures

1 引言

安全的群组通信服务在现代计算中发挥着重要的作用,得到了广泛的研究和关注。其所面临的最重要的问题是群组密钥的管理,为了保证群组通信的安全性,需要在群组成员之间共享一个群组会话密钥,群组内的所有通信都使用该共享会话密钥进行加、解密,只有授权的群组成员才能得到该密钥进而参与群组会话。群组密钥分发的目的就是让一个群组中的所有成员安全地共享一个密钥。针对有线网络中的群组密钥分发研究已取得了许多进展,提出了多种安全高效的群组密钥分发协议和算法[1,2]。但是,无线网络中的群组通信一般是在不可靠的信道中进行,数据包很容易在通信过程中被丢失。如果包含群组会话密钥的数据包被丢失,授权的群组成员就可能收不到群组会话密钥,需要群组管理员重传群组会话密钥信息,从而增加了网络负载。为此,Staddon 等人[3]提出了自治愈的群组密钥分发思想:在群组密钥分发过程中,群组管理员广播的群组密钥分发消息仅仅对被授权的群组成员是有用的,合法群组成员结合预先分配的个人秘密信息,能够从群组管理员的广播消息中自动恢复出共享的群组会话密钥,而被撤销的以及恶意的用户从广播消息中得不到有关会话密钥的信息。研究具有自治愈属性的群组密钥分发方案,在面向军事应用、紧急救援等无线网络环境中有着重要的应用价值。

文献[3]最先提出可撤销的自治愈群组密钥分发的形式化定义、资源占用下界以及几个构造方案。后来,Liu 等人[4]推广了上述定义,通过引入一个新的个人秘密分发技术,提出了一个新的具有撤销能力的高效自治愈群组密钥分发方案,减少了通信负载和存储开销。Blundo 等人[5]指出了文献[3]中构造方案存在的一个攻击,并开发了一个新的自治愈群组密钥分发方法。文献[6]基于单向密钥链,提出了一个新的自治愈群组密钥分发方法,并设计了一个具有较少计算和通信开销的计算上安全的自治愈群组密钥分发方案。文献[7]提出了一种基于向量空间访问结构上的秘密共享而非采用 Shamir 秘密共享的自治愈群组密钥分发方案。在现有的这

到稿日期:2008-12-24 返修日期:2009-03-05 本文受国家自然科学基金(60803151,60803150)资助。
彭清泉 博士研究生,主要研究方向为无线网络安全,E-mail:qingquanpeng@sina.com;**裴庆祺** 博士,副教授,主要研究方向为信息安全、传感器网络及安全;**庞辽军** 博士,副教授,主要研究方向为密码学、电子商务中的安全理论与技术。

些自治愈群组密钥分发方案中大都需要一个重要的假设，即在系统设置阶段群组管理员和群组成员之间存在一条安全的信道，用来分发群组管理员为群组成员选取的个人秘密信息。但在军事、应急救援等移动无线网络应用场景中，这样的安全信道实际上是很难建立的。

本文基于一种访问结构上的秘密共享方案，提出了一个具有撤销能力的自治愈群组密钥分发方案。该方案的优点在于，在系统初始化设置阶段群组成员可以自行选取个人密钥信息，不需要群组管理员为每个群组成员选取并通过安全信道进行分发。在系统安全模型下对方案进行的安全性分析表明，该方案是一个具有撤销能力的、保证前向保密及后向保密的、计算上安全的自治愈群组密钥分发方案。通过性能比较分析表明，该方案在存储开销和通信开销方面具有较大的改进。

2 预备知识

2.1 访问结构上的秘密共享

门限秘密共享概念最早是由 Shamir[8] 和 Blakley[9] 在1979年分别提出，它是指一个秘密被 n 个参与者分享，只有 t 个或更多的参与者联合才可以重构该秘密，而参与者少于 t 个时不能得到该秘密的任何信息。后来，Benaloh 等人[10]指出门限秘密共享方案存在其局限性，提出了一般访问结构上的秘密共享概念和方案。秘密分发者将所要共享的秘密 s 分成 n 个子秘密分发给 n 个参与者，使得每个参与者只知道自己的子秘密而不知道其它参与者的子秘密。然后秘密分发者定义一些授权子集，使得只有授权集合中的参与者联合才可以恢复出共享秘密 s，而非授权集合中的参与者联合不能得到秘密 s 的任何信息。由所有授权子集构成的集合称为访问结构，通常用 Γ 表示。如果对于任何 $A\subseteq B$ 且 $A\neq B$，有 $A\notin\Gamma$，则称 $B\in\Gamma$ 是最小授权子集。Γ 的所有最小授权子集构成的集合 Γ_0 称为 Γ 的基，Γ 可由 Γ_0 唯一确定，即 $\Gamma=\{C\mid B\subseteq C, B\in\Gamma_0\}$，其中 C 为由参与者组成的集合。

大多秘密共享方案都建立在两个基本假设之上：一是参与者的子秘密都是由秘密分发者生产并安全地分发给各参与者，秘密分发者掌握着所有参与者的子秘密；二是在秘密分发者和各参与者之间存在一条安全信道。这些假设必然会影响到秘密共享方案的应用，例如当参与者和秘密分发者之间不可能存在安全信道时，这些方案将不再实用。文献[11]基于Shamir秘密共享方案和RSA密码体制提出了一个一般访问结构上的秘密共享方案，该方案中参与者的秘密份额由参与者自行选取，秘密分发者不需要向各参与者传递秘密信息，因而它们之间不需要安全信道，每个参与者只需维护一个秘密份额就可以实现对多个秘密的共享，而且允许参与者的动态加入与退出、访问结构的变动以及所共享秘密的动态更新。该方案能够较好地应用于建立自治愈的群组密钥分发方案。

2.2 系统安全模型

设 $U=\{U_1,U_2,\cdots,U_n\}$ 是网络中用户的总体，U_i 表示群组中的用户 i，n 是网络中总的用户数。网络中存在一条不可靠的广播信道，群组管理员 GM 通过群组的建立、用户的加入和撤销操作来维护一个通信群组，群组中的成员是集合 U 的动态子集。m 是群组生存周期内的最大会话数，$G_j\in U$ 是在会话 j 中由 GM 建立的通信群组，$\mathscr{R}\subset 2^U$ 是可被撤销的用户子集的单调递减访问结构。S_i 表示用户 U_i 的个人秘密信息，K_j 是会话 j 的群组密钥，B_j 表示在会话 j 中 GM 广播的群组密钥分发消息，$Z_{i,j}$ 表示用户 U_i 通过 B_j 和 S_i 所获得的信息。

定义 1(群组会话密钥分发方案 D[3]) 令 $i\in\{1,\cdots,n\}$，$j\in\{1,\cdots,m\}$

1) D 是保密的群组会话密钥分发方案，如果满足以下条件：

(a) 对于任意的用户 $U_i\in G_j$，群组会话密钥 K_j 能够由 B_j 和 S_i 有效确定；

(b) 对任意的集合 $F\subseteq U$，其中 $F\in\mathscr{R}$，并且 $U_i\notin F$，F 中的用户要确定 U_i 的个人密钥 S_i 在计算上是不可行的；

(c) 如果单独考虑 m 个广播消息集合 $\{B_1,\cdots,B_m\}$ 或者 n 个个人秘密集合 $\{S_1,\cdots,S_n\}$，从其中一个集合要计算出群组会话密钥 K_j 在计算上是不可行的。

2) D 具有 R-撤销能力，如果对于任意 $R_j\subseteq U$，$R_j\in\mathscr{R}$，群组管理员 GM 能生成一个广播消息 B_j，使得对所有 $U_i\notin R_j$ 能够有效地恢复出群组会话密钥 K_j，但被撤销的用户从 B_j 和 $\{S_r\}_{U_r\in R_j}$ 中恢复出 K_j 在计算上是不可行的。

3) D 是自治愈的，如果对于任意的 j，$1\leqslant j_1<j<j_2\leqslant m$，满足对于任意既是会话 j_1 中成员又是会话 j_2 中成员的用户 U_i，群组会话密钥 K_j(对所有 $j_1<j<j_2$)可以通过集合 $\{Z_{i,j_1},Z_{i,j_2}\}$ 有效确定，即对任意 $U_i\in G_{j_1}$，如果其在会话 j_1 之后和会话 j_2 之前没有被撤销，那么对于任意 $j=j_1,\cdots,j_2$，它能从广播消息 B_{j_1} 和 B_{j_2} 中恢复出所有会话密钥 K_j。

定义 2($\mathscr{R}$-对前向和后向保密[4]) 令 $i\in\{1,\cdots,n\}$，$j\in\{1,\cdots,m\}$

1) 密钥分发方案 D 保证 $\mathscr{R}$-对前向保密性，如果对于任意集合 $R_j\subseteq U$，$R_j\in\mathscr{R}$，并且所有 $U_l\in R_j$ 是在会话 j 之前被撤销的用户，R_j 中的成员合谋得到有关 K_j 的信息在计算上是不可行的，即使它们知道会话 j 之前所有的群组会话密钥 $K_1,\cdots,K_{j-1}$。

2) 密钥分发方案 D 保证 $\mathscr{R}$-对后向保密性，如果对于任意集合 $J_j\subseteq U$，$J_j\in\mathscr{R}$，并且所有 $U_l\in J_j$ 是在会话 j 之后加入的用户，J_j 中的成员合谋得到有关 K_j 的信息在计算上是不可行的，即使它们知道会话 j 之后所有的群组会话密钥 $K_{j+1},\cdots,K_m$。

3 基于一般访问结构的自治愈群组密钥分发方案

设 $U=\{U_1,U_2,\cdots,U_n\}$ 是群组通信中用户的集合，群组管理员 GM 通过加入和撤销用户操作来建立并维护通信群组。网络中存在一条不可靠的广播信道。系统中有一个公告牌，只有 GM 可以修改和更新公告牌上的内容，群组中的用户只能下载其内容。令 J_j 表示在会话 j 中加入的用户集合，R_j 表示在会话 j 中被撤销的用户集合，有 $R_j\subseteq G_{j-1}$ 且 $R_1=\emptyset$，$G_j=(G_{j-1}\cup J_j)-R_j$ 表示会话 j 中的用户集合。令 $\mathscr{R}\subset 2^U$ 是被 GM 撤销用户集合的单调递减访问结构，$\Gamma=2^U-\mathscr{R}$ 是一个单调递增访问结构，不失一般性，令单调递增访问结构 $\Gamma=\{\gamma_1,\gamma_2,\cdots,\gamma_t\}$。

3.1 初始化设置

(1) GM 首先随机选取两个素质 p 和 q，令 N 是 p 和 q 的乘积，且满足在不知道 p 和 q 的情况下分解 N 在计算上是

不可行的。GM从$[N^{1/2},N]$中随机选取一个整数g，满足$g\neq p$且$g\neq q$。GM随机选取一个大于N的素数Q。然后，GM在公告牌上公布系统参数$\{g,N,Q\}$，并销毁p和q。

(2) 每一个用户U_i随机地从$[2,N]$中选取一个整数x_i，计算$y_i=g^{x_i} \bmod N$。U_i将x_i保密，并将其身份ID_i和y_i一起发送给GM。GM检查并确保不存在两个不同用户$ID_i\neq ID_j$使得$y_i=y_j$成立，从而避免不同用户使用相同的秘密信息。如果出现此情况，GM要求用户重新选取不同的整数，直到满足所有的用户都有不同的秘密为止。

(3)GM独立均匀地选取m个一次多项式：$f_j(x)=s_j+b_jx \bmod Q(j=1,\cdots,m)$，其中$b_j(j=1,\cdots,m)$均随机地从$GF(Q)$选取，在公告牌上公布信息$f_j(1)$。GM再独立均匀地从$GF(Q)$中选取$m$个群组会话密钥$\{K_j\}_{j=1,\cdots,m}$。对每一个群组会话$j=1,\cdots,m$，定义$z_j=K_j+s_j$。

3.2 群组会话密钥分发广播

(1) 在群组会话j中，GM随机从$[2,N]$中选取一个整数x_0^j，满足x_0^j与$(p-1)$和$(q-1)$互素，计算$y_0^j=g^{x_0^j} \bmod N$。从$[1,Q-1]$中随机选取t个数$d_1,d_2,\cdots,d_t$分别标识访问结构Γ中的每一个授权子集。对于Γ中的每一个授权子集$\gamma_i^j=\{P_{1i},P_{2i},\cdots,P_{ji}\}$，群组管理员GM计算：$H_i^j=(f(d_i) \bmod Q)\oplus((y_{1i})^{x_0^j} \bmod N)\oplus\cdots\oplus((y_{ji})^{x_0^j} \bmod N)$，并在公告牌上公告$\Gamma$中每一个授权子集的信息$\{(d_i,H_i^j)\}_{i=1,\cdots,t}$。

(2) 令$R=R_2\cup\cdots\cup R_{j-1}\cup R_j$表示群组会话$j$及其之前会话所有被撤销的用户集合，且满足$R\in\mathcal{R}$。在群组会话$j$中，GM选择最大非授权用户子集$W_j\in\mathcal{R}_0$，满足$R\subset W_j$且$G_j\cap W_j=\emptyset$。对于$W_j$中的每一个用户，GM计算$S_{kj}=((y_{kj})^{x_0^j} \bmod N)|_{k\in W_j}$，并在公告牌上公布$\{W_j,S_{kj}\}$。

(3) GM在公开广播信道上广播消息：$B_j=\langle z_1,z_2,\cdots,z_j\rangle$。

3.3 群组会话密钥恢复

(1) 当访问结构Γ上的任何授权子集γ_i中的未被撤销的用户U_v在收到第j个群组会话密钥分发广播消息时，由于W_j是最大非授权子集，因此$W_j\cup\{U_v\}\in\Gamma$，它下载公告牌上的信息$\{(d_i,H_i^j)\}_{i=1,\cdots,t}$和$\{W_j,S_{kj}\}$，利用公告信息和个人秘密信息，$U_v$可以计算出：$H_i^j\oplus S_{1j}\oplus\cdots\oplus S_{kj}\oplus((y_0^j)^{x_v} \bmod N)=f(d_i)$，从而得到一次多项式$f_j(x)$上两个点$(1,f_j(1))$和$(d_i,f_j(d_i))$。

(2) 用户U_v利用Lagrange插值公式重构出一次多项式$f_j(x)$，从而恢复出个人秘密信息$s_j=f_j(0)$。

(3) 用户U_v利用收到的广播消息中的z_j和s_j，恢复出第j个群组会话密钥$K_j=z_j-s_j$。

3.4 新的群组成员加入

当一个新的用户$U_v(v\neq 1,\cdots,n)$需要从会话j开始加入群组时，可能会增加新的授权子集。如果没有增加新的授权子集，则U_v首先随机地从$[2,N]$中选取一个整数x_v，并计算$y_v=g^{x_v} \bmod N$，然后将x_v保密，并将ID_v和y_v发送给GM。群组管理员GM检查并确保对每个$U_i(i=1,\cdots n)$有$y_i\neq y_v$，若成立则将用户U_v作为合格成员加入群组中。如果U_v的加入导致产生了新的授权子集γ_d，GM只需为该授权子集选取一个唯一的整数d_d，并计算H_d^j，然后公布(d_d,H_d^j)。

3.5 重新初始化设置

当m个会话密钥都使用完之后，为了继续进行下一次m个会话，需要对系统重新进行初始化设置。由于每个参与者的个人秘密x_i可以重复使用，因此重新初始化设置时，只需要将前m个会话中被撤销的用户和下一次m个会话中需要加入的用户重新选择个人秘密x_i，并将它们的身份ID_i和$g^{x_i} \bmod N$的值发给群组管理员GM，然后GM检查这些值的有效性，就可以完成系统的重新初始化。

3.6 自治愈机制

令$1\leqslant j_1<j<j_2\leqslant m$，群组成员$U_i$分别收到会话$j_1$和$j_2$的群组会话密钥分发广播消息$B_{j_1}$和$B_{j_2}$，但没有收到会话$j$的广播消息$B_j$，$U_i$仍然能够自动恢复出所有丢失的群组会话密钥$K_j(j_1<j<j_2)$。这是因为群组管理员GM在每一次会话$j$中都在公告牌中公布了访问结构$\Gamma$中每一个授权子集的信息$\{(d_i,H_i^j)\}_{i=1,\cdots,t}$以及$\{W_j,S_{kj}\}$和一次多项式$f_j(x)$上的点$(1,f_j(1))$，$U_i$利用个人秘密$x_i$可以计算出另一个点$(d_i,f_j(d_i))$，从而得到一次多项式$f_j(x)$上的两个点，利用Lagrange插值公式可以恢复出$f_j(x)$，得到$s_j=f_j(0)$。因此对所有$j=j_1+1,j_1+2,\cdots,j_2-1$，$U_i$都能计算出$s_j$，再利用广播消息$B_{j_2}$中收到的$z_{j_1+1},z_{j_1+2},\cdots,z_{j_2-1}$，便能够恢复出群组密钥$K_j(j_1<j<j_2)$。

4 安全性分析

在系统安全模型下对提出的方案进行了安全性分析，证明该方案是一个具有撤销能力的、保证前向保密性及后向保密性的、计算上安全的自治愈群组密钥分发方案。

定理1 本文提出的方案是满足定义1的具有保密和$\mathcal{R}$-撤销能力的计算上安全的自治愈群组密钥分发方案。

证明：1) (a) 方案的第三步群组会话密钥恢复过程实现了对于任意的用户$U_i\in G_j$，能够由B_j和S_i中恢复出群组会话密钥K_j；

(b) 对于任意集合$F\subseteq U,F\in\mathcal{R}$，未被撤销的用户$U_i\notin F$，可以证明$F$中用户的合谋不能得到有关用户$U_i$的个人秘密$S_i$的任何信息。因为对于每一次会话$j$，$U_i$的个人秘密$S_i=f_j(0)$是一次多项式$f_j(x)$的一个取值，$F$中用户最多只能知道公告牌上公布的关于$f_j(x)$的一个点，利用一个点重构一次多项式$f_j(x)$的难度相当于攻破了Shamir的$(t,n)$门限秘密共享方案，这在计算上是不可行的。因此，$F$中用户的合谋不能得到$U_i$的个人秘密$S_i$；

(c) 因为群组会话密钥K_j是从均匀分布中选取的，而且独立于用户的个人秘密，因此单独从个人秘密集合中不能获得有关会话密钥K_j的信息；另外，对每一次会话$j=1,\cdots,m$，由于$z_j=K_j+s_j$，z_j通过个人秘密s_j完美地隐藏了会话密钥K_j，因此单独从广播消息集合中也不能得到有关会话密钥K_j的信息。

2) ($\mathcal{R}$-撤销能力) 对于未被撤销的用户利用广播消息和公告牌上公告的信息以及自己的个人秘密，按照会话密钥恢复步骤能够有效地恢复出群组会话密钥K_j；但是对于被撤销的任意$R_j\subseteq U,R_j\in\mathcal{R}$中的用户，它们最多只能得到公告牌上公布的一次多项式$f_j(x)$上的一个点，而利用一个点重构一次多项式$f_j(x)$在计算上是不可行，所以R_j中的用户合谋不能恢复出$f_j(0)$，而$K_j=z_j-f_j(0)$，因此它们通过广播消息B_j及其个人秘密$\{S_r\}_{U_r\in R_j}$恢复出群组会话密钥K_j在计算上是不可行的。

3) (自治愈能力) 对于任意的$j,1\leqslant j_1<j<j_2\leqslant m$，则有：

(a) 对于用户 U_i，它既是会话 j_1 又是会话 j_2 中的成员，并且收到了广播消息 B_{j_1} 和 B_{j_2}，但没有收到广播消息 B_j（$j_1<j<j_2$）。U_i 利用自己的个人秘密 x_i 和公告牌上公告的信息可以计算出一个点 $(d_i, f_j(d_i))$，结合公告牌上公告的一个点 $(1, f_j(1))$，利用一次多项式 $f_j(x)$ 上的这两个点，根据 Lagrange 插值公式，U_i 可以恢复出 $f_j(x)$，得到 $s_j=f_j(0)$，再利用 B_{j_2} 中收到的 z_j（$j_1<j<j_2$），便能够恢复出群组会话密钥 K_j（$j_1<j<j_2$）。

(b) 由于在会话 j_1 之前被撤销的用户合谋不能得到关于会话密钥 K_j（对于所有 $j>j_1$）的信息，在会话 j_2 之后加入群组的用户合谋不能获得关于会话密钥 K_j（对于所有 $j<j_2$）的信息，且 $R_j \cup J_j$ 中的用户最多只能得到公告牌上公告的关于一次多项式 $f_j(x)$ 上的一个点，它们不能恢复出 $f_j(x)$，得不到 $f_j(0)$，从而不能计算出会话密钥 K_j（$j_1<j<j_2$）。

定理 2 提出的方案具有 $\mathcal{R}$-对前向保密和 $\mathcal{R}$-对后向保密的属性。

证明：通过证明所提出的方案满足定义 2，说明其满足 $\mathcal{R}$-对前向保密性和后向保密性。

1）（$\mathcal{R}$-对前向保密性） 令 $R_j \subseteq U, R_j \in \mathcal{R}$，所有 $U_l \in R_j$ 是在会话 j 之前被撤销的用户。集合 R_j 中的用户合谋即使知道会话 j 之前所有的群组会话密钥，也不能得到关于当前会话密钥 K_j 的任何信息。因为，R_j 中的合谋用户要知道会话密钥 K_j，必须要能够恢复出 $f_j(0)$，但它们只能得到公告牌上公布的关于多项式 $f_j(x)$ 上的一个点，不能重构出一次多项式 $f_j(x)$，也就得不到 $f_j(0)$。因此，方案是 $\mathcal{R}$-对前向保密安全的。

2）（$\mathcal{R}$-对后向保密性） 令 $J_j \subset U, J_j \in \mathcal{R}$，所有用户 $U_l \in J_j$ 是在会话 j 之后加入群组的。集合 J_j 中的用户合谋即使知道了会话 j 之后所有的群组会话密钥，也不能得到关于以前的会话密钥 K_{j_1}（$j_1 \leqslant j$）的任何信息。因为，为了得到 K_{j_1}，用户 $U_l \in J_j$ 至少需要两个点恢复出 $f_{j_1}(x)$，从而获得 $f_{j_1}(0)$，而对于在会话 j 之后加入的用户 U_l 最多只能得到关于一次多项式 $f_{j_1}(x)$ 上的一个点，因此方案是 $\mathcal{R}$-对后向保密安全的。

5 性能分析

本文提出的方案最主要的优点在于，群组成员可以自行选取个人秘密信息，而不需要群组管理员通过安全信道进行分发，每个群组成员只需要存储自己选取的个人秘密。表 1 从存储开销、通信开销方面，将本文方案与相关方案进行了性能对比分析。其中，t 表示系统中合谋成员的最大数，m 表示群组生命周期内的会话数，q 是满足密码学密钥需求足够大的素数。

从表 1 可以看出，所提方案由于群组成员可以自行选取个人秘密信息，在自治愈群组密钥分发过程中，每个群组成员只需存储一个自己选取的个人密钥，而其它方案中群组成员则需要存储群组管理员分发的个人秘密多项式值，这使得方案中的存储开销减少到一个常数。另外，本文方案的通信开销一方面来自群组管理员向群组成员广播的消息开销 $|B_j| = j \log q$，一方面来自群组成员从公告牌上下载公告信息 $\{(d_i, H_i^j)\}_{i=1,\cdots,t}$ 所需的通信开销 $2tj \log q$，所以方案中总的通信开销跟文献[5]中方案是一样的。总的来看，本文方案除了具有用户可自行选取个人秘密信息的特殊性质，在存储开销和通信开销等性能上也是较优的。但是，本文方案在安全性上只能达到计算上的安全。

表 1 性能比较

方案	存储开销	通信开销
文献[3]的构造 3	$(m-j+1)^2 \log q$	$(mt^2+2mt+m-t) \log q$
文献[4]的方案 3	$2(m-j+1) \log q$	$[(m+j+1)t+(m+1)] \log q$
文献[5]的方案 3	$(m-j+1) \log q$	$(2tj+j) \log q$
文献[6]的构造 1	$(m-j+1) \log q$	$(t+1) \log q$
本文的方案	$\log q$	$(2tj+j) \log q$

结束语 自治愈的群组密钥分发方案在面向军事应用、应急救援等无线网络群组通信中有着重要的应用前景。本文基于参与方可自行选取秘密份额访问结构上的秘密共享方法，提出了一个具有撤销能力的自治愈群组密钥分发方案，该方案不需要在群组管理员和每个群组成员之间建立一条安全信道来分发群组成员的个人秘密信息。在特定系统安全模型下，对所提出的方案进行安全性分析表明，该方案是一个具有可撤销能力的、保证前向保密及后向保密的、计算上安全的自治愈群组密钥分发方案。通过与相关方案进行性能对比分析表明，该方案在存储开销和通信开销等性能上都是较优的。但是，本文的方案只能达到计算上的安全性，下一步的工作是研究既能够具有让群组成员自行选取个人秘密信息，又能达到无条件安全性的高效自治愈群组密钥分发方案。

参 考 文 献

[1] Rafaeli S, Hutchison D. A Survey of Key Management for Secure Group Communication [J]. ACM Computing Surveys, 2003, 35(3): 309-329

[2] Challal Y, Seba H. Group Key Management Protocols: A Novel Taxonomy[J]. International Journal of Information Technology, 2005, 2(1): 105-119

[3] Staddon J, Miner S, Franklin M, et al. Self-healing Key Distribution with Revocation[C] // Proceedings of IEEE Symposium on Security and Privacy'02. Los Alamitos: IEEE, 2002: 224-240

[4] Liu D, Ning P, Sun K. Efficient Self-healing Group Key Distribution with Revocation Capability[C] // /Proceedings of the 10th ACM Conference on Computer and Communications Security. New York: ACM, 2003: 231-240

[5] Blundo C, D'Arco P, Santis A, et al. Design of Self-healing Key Distribution Schemes [J]. Design Codes and Cryptography, 2004, 32(1): 15-44

[6] Dutta R, Chang E C, Mukhopadhyay S. Efficient Self-healing Key Distribution with Revocation for Wireless Sensor Networks Using One Way Key Chains[C] // Proceedings of the 5th International Conference on Applied Cryptography and Network Security, LNCS 4521. Berlin: Springer-Verlag, 2007: 385-400

[7] Dutta R, Mukhopadhyay S, Das A, et al. Generalized Self-healing Key Distribution Using Vector Space Access Structure[C] // NETWORKING 2008, LNCS 4982. Berlin: Springer-Verlag, 2008: 612-623

[8] Shamir A. How to Share a Secret[J]. Communications of the ACM, 1979, 22: 612-613

[9] Blakley G. Safeguarding Cryptographic Keys[C] // The National Computer Conference 1979. New York: AFIPS Press, 1979: 313-317

[10] Benaloh J, Leichter J. Generalized Secret Sharing and Monotone Functions[C] // Advances in Cryptology'88, LNCS 403. Berlin: Springer-Verlag, 1990: 27-35

[11] 庞辽军，姜正涛，王育民. 基于一般访问结构的多重秘密共享方案[J]. 计算机研究与发展，2006，43(1)：33-38