基于几何方法与二叉密钥树的群组密钥管理

葛丽娜[1,2] 唐韶华[1]
(华南理工大学计算机科学与工程学院 广州 510640)[1]
(广西民族大学数学与计算机科学学院 南宁 530006)[2]

摘 要 目前越来越多的应用需要群组通信的模式。利用多维空间圆的几何性质设计了安全群组通信密钥管理方案,该方案分为用户注册、分配组密钥影子、成员计算组密钥等3个阶段。用户注册阶段使成员与群组管理器共享一个长期秘密;在分配组密钥影子阶段,群组管理器利用几何方法为成员分配组密钥影子;在成员计算组密钥阶段,成员通过公告牌上的公开信息与自己拥有的私有信息重构圆而获得组密钥。在简单群组密钥分配的基础上,建立二叉树结构的密钥树进行组密钥分配,其组密钥更新的计算代价从O(m)降低到O(log(m)),公开信息无需变化,无需安全信道,使方案具可有扩展性。

关键词 组密钥分配,安全群组通信,几何方法,n维空间,二叉树
中图法分类号 TP393 **文献标识码** A

Group Key Management Protocol by Using Geometric Approach and Binary Key Tree

GE Li-na[1,2] TANG Shao-hua[1]
(School of Computer Science and Engineering, South China Univ. of Tech., Guangzhou 510640, China)[1]
(School of Mathematics and Computer Science, Guangxi Univ. of nationalities, Nanning 530006, China)[2]

Abstract Many emerging applications are based upon a group communications model. A new group key management scheme for a secure group communication system based on a geometric approach was proposed. The proposed scheme can be divided into three phases: user registration, group key assignment, and group key computation. In the user registration phase, the group manager computes and gives a secret to the new user based on geometric approaches over a secure channel. In the group key assignment phase, the group manager first constructs a secret circle using the group key. Then it computes a shadow of the group key for each member based on the member's private key. Finally, each member obtains an additional secret point based on his private key. The member reconstructs the secret circle by its shadow and the public information, and then obtains the group key in the group key computation phase. Based on simple scheme of group key management, a binary tree of keys is set up to redesign the scheme and demonstrate it. The computation complexity for rekeying decreases from O(m) to O(log(m)). The public information on the note board keeps the same. No a secure channel is needed when the group key is updated. So this scheme is scalable.

Keywords Group key management, Secure group communication, Geometric approach, n-dimensional space, Binary tree

一个安全群组通信系统提供的基本安全服务应包括数据保密性、完整性、成员认证和存取控制等。如果所有的群组成员都共享一个密钥,就很容易实现这些安全服务,这个共享的密钥称为组密钥。已有的群组密钥管理有Centralized Key Distribution (CKD)[1], Group Diffie-Hellman (GDH)[2], Tree-Based Group Diffie-Hellman (TGDH)[3], Burmester-Desedt (BD)[4], Dynamic Multicast Groups (DMG)[5]和Local Key Hierarchy(LKH)[6]。还有一些文献[7-9]对这些方案做了改进。文献[6,9]中方案在密钥更新时虽然有较高的性能,但依赖于安全信道;另外一些基于Diffie-Hellman密钥交换方案[1-4]虽然不需要安全信道,但涉及到大量的模指运算,计算复杂、性能较低。

文献[10-17]将几何方法应用于信息安全,其中文献[10-15]是身份认证方案,文献[16,17]是秘密共享方案。文献[13,16,17]的数学理论论据是:在n维空间中,通过不同在$n-1$维空间的$(n+1)$点唯一地构造一个n维圆;而已知圆上不多于n点则不能获取该圆更多的知识。本文借助该性质设计一个安全群组通信密钥管理方案,首先利用组密钥作为半径平方构造一个n维空间圆;然后在圆上随机选取n个不同在$(n-1)$维空间的点,作为公开的信息;再给群组中的每个成员分配该圆上另外一点(与公开的n个点不同在$n-1$维空间中),称为组密钥影子,则成员拥有该圆上的$(n+1)$个点,由

到稿日期:2008-12-11 返修日期:2009-04-23 本文受国家"863"项目(2007AA01Z424),国家自然科学基金资助项目(60572139),国家科技支撑计划(2007BAH13B03),教育部新世纪优秀人才支持计划(NCET-06-0744),霍英东教育基金资助项目(101069)资助。
葛丽娜(1969-),女,博士生,主要研究方向为信息安全,E-mail:gelina100@gmai.com;唐韶华(1970-),男,教授,博士生导师,主要研究方向为信息安全、计算机网络等。

这些点重构圆，从而获得组密钥。在此基础上，本文还设计了基于二叉树结构的密钥树，进行群组密钥分配，以提高性能，使群组密钥分配有良好的扩展性。当群组动态变化时，即密钥更新、成员加入/退出时，公开信息无需改变、所传送的消息无需加密。

1 数学背景

1.1 几何方法

文中运算定义于有限域 GF(p)上。

定理 1[16] 假设已知 n 维空间中的 $n+1$ 个点，如果这些点不同在 $n-1$ 维空间中，那么它们就可以唯一地确定一个圆方程：$\sum_{i=1}^{n}(x_i-c_i)^2=R(\bmod p)$。

定理 2[16] 令 p 为一奇素数，如果 2 是模 p 下的非二次剩余，那任意 $z\in[0,p)$可以表示为模 p 下任意 $k(k\geqslant 2)$个整数的平方之和。

定理 2 为以下的算法 1 提供了理论基础。对于圆$\sum_{i=1}^{n}(x_i-c_i)^2=R(\bmod p)$，其半径平方 R 可以分解为 n 个整数模 p 平方之和，由此可获得该圆上的一点。

算法 1 根据两个输入参数，在 n 维圆 Ω 上取一点

函数：PickPointByTwo($n,r,s,(c_1,c_2,\cdots,c_n,R)$)

输入：n 是几何空间维数，整数 $s,r\in(0,p)$，Ω 的圆方程为

$$\sum_{i=1}^{n}(x_i-c_i)^2=R(\bmod p)$$

f 是一个单向散列函数：$[0,p)\to[0,p)$。

输出：Ω 上一点。

(1)计算 $x_1,x_2,x_3,\cdots,x_{(n-2)}$：$e=r+s(\bmod p)$，$x_1=f(e)$，$x_2=f^2(e)$，$x_3=f^3(e)$，$\cdots$，$x_{(n-2)}=f^{(n-2)}(e)$。

(2)令
$$\begin{cases}d_1=x_1-c_1(\bmod p)\\ d_2=x_2-c_2(\bmod p)\\ \cdots\\ d_{n-2}=x_{n-2}-c_{n-2}(\bmod p)\end{cases}$$

(3)计算 $e_1=d_1^2(\bmod p)$，$e_2=d_2^2(\bmod p)$，$\cdots$，$e_{(n-2)}=d_{(n-2)}^2(\bmod p)$。

(4)重复计算：

随机生成 $d_{n-1}\in(0,p)$，计算 $e_{n-1}=d_{n-1}^2(\bmod p)$，$e'_n=R-\sum_{j=1}^{n-1}e_j(\bmod p)$，则 $d_n=e_n'^{(p+1)/4}(b \bmod p)$；

计算 $e_n=d_n^2(\bmod p)$。

直到 $e_{n-1}+e_n=R-\sum_{j=1}^{n-2}e_j(\bmod p)$。

(5) 令 $x_{n-1}=d_{n-1}+c_{n-1}(\bmod p)$，$x_n=d_n+c_n(\bmod p)$。

(6) 令 $B=(x_1,x_2,\cdots,x_n)$，输出 B。

由定理 1 知，通过不同在 $(n-1)$维空间的$(n+1)$个点唯一确定一个 n 维空间圆。以下算法 2 是求解该圆的一种方法。

算法 2 在 n 维空间中过$(n+1)$个点构造一圆方程

函数：CircleByPoints($n,G_1,G_2,\cdots,G_{n+1}$)

输入：n 为几何空间维数，$(n+1)$个点坐标

$G_1(x_{11},x_{12},\cdots,x_{1n})$，$\cdots$，$G_{n+1}(x_{(n+1)1},x_{(n+1)2},\cdots,x_{(n+1)n})$。

输出：圆心与圆半径的平方。

(1)设 n 维圆的圆心为$(c_1,c_2,\cdots,c_n)$，半径平方为 R，则圆方程表示为

$$\sum_{i=1}^{n}(x_i-c_i)^2=R(\bmod p)\qquad(1)$$

(2)将 $G_1,\cdots,G_{n+1}$的坐标代入圆方程(1)，可以得到$(n+1)$个方程组成的方程组：

$$\begin{cases}\sum_{i=1}^{n}(x_{1i}-c_i)^2=R(\bmod p)\\ \sum_{i=1}^{n}(x_{2i}-c_i)^2=R(\bmod p)\\ \cdots\\ \sum_{i=1}^{n}(x_{(n+1)i}-c_i)^2=R(\bmod p)\end{cases}\qquad(2)$$

(3)利用式(2)中的下一个方程减去上一个方程，可得到式(3)

$$\begin{cases}2\sum_{i=1}^{n}(x_{2i}-x_{1i})c_i=\sum_{i=1}^{n}x_{2i}^2-\sum_{i=1}^{n}x_{1i}^2(\bmod p)\\ 2\sum_{i=1}^{n}(x_{3i}-x_{2i})c_i=\sum_{i=1}^{n}x_{3i}^2-\sum_{i=1}^{n}x_{2i}^2(\bmod p)\\ \cdots\\ 2\sum_{i=1}^{n}(x_{(n+1)i}-x_{ni})c_i=\sum_{i=1}^{n}x_{(n+1)i}^2-\sum_{i=1}^{n}x_{ni}^2(\bmod p)\end{cases}\qquad(3)$$

由方程组(2)中任何两个方程相减后产生 C_{n+1}^2个线性方程，则方程组(3)是其中的一个极大线性无关组，它含 n 个方程的 n 元一次线性方程组，$c_1,c_2,\cdots,c_n$ 为未知数。由于 $G_1,\cdots,G_{n+1}$不同在 $n-1$ 维空间中，系数行列式不为 0，可以求出方程组的唯一解，获得该圆的圆心。将圆心的值代入式(2)中的任意一个式子，可求出 R。

(4)输出圆$(c_1,c_2,\cdots,c_n,R)$。

1.2 中国剩余定理

设 $p_1,p_2,\cdots p_k$ 是互为素数的 k 个正数，$k\geqslant 2$，令 $P=p_1p_2\cdots p_k=p_1P_1=p_2P_2=\cdots=p_kP_k$，其中 $P_i=P/p_i$，$i=1,2,\cdots,k$，则同时满足同余方程组

$$\begin{cases}X\equiv y_1(\bmod p_1)\\ X\equiv y_2(\bmod p_2)\\ \quad\vdots\\ X\equiv y_k(\bmod p_k)\end{cases}\qquad(6)$$

的正整数解是

$$X=\sum y_iP_iP_i'(\bmod P)\qquad(7)$$

其中，$P_i'=P_i-1\ (\bmod p_i)$，$i=1,2,\cdots,k$。

显然，若已定义 $p_1,p_2,\cdots,p_k$，则既可利用式(7)将$(y_1,y_2,\cdots,y_k)$合并成一个整数 X，又可利用式(6)将$(y_1,y_2,\cdots,y_k)$恢复。这样，可以将 k 个数合并为一个数后进行网络传送，到目的地后再将该数恢复为原来的 k 个数，能有效地减少网络通信量。

2 本文方案

基于几何方法设计群组密钥管理，不需要大量模指运算，也不需要安全信道(用户注册阶段除外)，因而计算简单，可适用于终端低计算能力的应用。在此基础上，设计二叉树结构的密钥树，增强了方案的可扩展性，使其适用于大规模的、动态的网络环境。

系统中含有一个群组管理器 G，负责产生组密钥 k、将组密钥 k 分发给群组中的 m 个成员$\{M_1,M_2,\cdots,M_m\}$。

确定系统参数：空间维数 $n(n>2)$；大素数 $p(p\equiv 3(\bmod 4))$，建立有限域 GF(p)；单向散列函数 $f:[0,p)\to[0,p)$，基于 f 定义一个嵌套函数 $f^t(s)=\underbrace{f(\cdots(f}_{t}(s)))$；$G$ 选取 $s_G\in(0,p)$作为其私钥。

群组密钥分配划分为 3 个阶段：用户注册、分配成员的组密钥影子、成员计算群组密钥。还设计了一些辅助操作：成员的动态加入与退出、组密钥更新。

2.1 用户注册

当用户 M_i 向群组注册时，G 依据自己的私钥 s_G 与 M_i 的唯一身份标识 ID_i 为 M_i 计算一个秘密，其作为 M_i 与 G 共享的长期秘密 s_i，也称为 M_i 的私钥，G 无需保存 s_i。此过程在安全信道中完成，G 执行如下步骤。

算法 3 用户注册

(1) 选取 M_i 唯一身份标识 ID_i；

(2) 计算 $s_i=f(s_G\times ID_i)$；

然后，G 将 s_i 通过安全信道交给 M_i。

2.2 简单的群组密钥管理

在本节中，G 首先生成组密钥，然后将组密钥的不同影子分别分配给群组中的所有成员。本节的方案简称为 SKMBGA(Simple Group Key Management Protocol Based on Geometric Approach)。

2.2.1 初始化

G 依照算法 4 进行初始化操作。

算法 4 组密钥初始化

(1)随机生 $c_1,c_2,\cdots,c_n\in(0,p)$，即点 $O\in(c_1,c_2,\cdots,c_n)$；

(2)生成一个随机数：$r\in(0,p)$；

(3)生成一个随机数 $k\in(0,p)$作为群组密钥；

(4)以 O为圆心，k 为半径平方构造一个 n 维空间圆 $\sum_{i=1}^{n}(x_i-c_i)^2=k(\mathrm{mod}\ p)$，记为 Ω；并秘密保存之；

(5)For $i=1$ to n do {

生成随机数 $b_i\in(0,p)$，

以 r,b_i 与圆 Ω 为输入，调用算法 1 生成点 W_i：

$W_i=$PickPointByTwo(n,r,b_i,Ω)。}

保证 $W_1,\cdots,W_n$ 不同在$(n-1)$维空间中，否则重复该步骤；

(6) 在系统公告牌上公布信息 Pub-meg$=\{f,p,n,W_1,\cdots,W_n\}$。

2.2.2 群组密钥影子生成

算法 5 给群组成员分配组密钥影子

G 执行如下步骤：

For $i=1$ to m do {

(1)令 $s_i=f(s_G\times ID_i)$，以 r,s_i 与圆 Ω 为输入参数，调用算法 1 在圆 Ω 上选取一点 $Q_i(x_{i1},x_{i2},\cdots,x_{in})$，并保证{ $W_1,\cdots,W_n,Q_i$}不同在$(n-1)$维空间中，Q_i 就是 M_i 的群组密钥的影子；计算 Q_i 点的消息摘要，设为 SHA_i；

(2)将 $r,(x_{i(n-1)},x_{in}),SHA_i$ 交给 M_i。}

G 将$(x_{i(n-1)},x_{in})$明文传给 M_i，因只有 M_i 已知$(x_{i1},x_{i2},\cdots,x_{i(n-2)})$，即使$(x_{i(n-1)},x_{in})$是公开的，其他人也不可能得到 $Q_i(x_{i1},x_{i2},\cdots,x_{in})$。

之后，M_i 计算 Q_i 点及其消息摘要，验证是否与收到的 SHA_i 一致，不一致表示 M_i 收到的组密钥影子不正确。

2.2.3 群组密钥计算

算法 6 群组成员计算组密钥

(1)成员 M_i 从公告牌上下载 Pub-meg，获 $W_1,\cdots,W_n$。

(2)计算：

(2-1)取出秘密 s_i；

(2-2)取出 r；

(2-3)计算 $e=r+s_i(\mathrm{mod}\ p)$，$x_{i1}=f(e)$，

$x_{i2}=f(f(e))$，$x_{i3}=f(f(f(e)))$，$\cdots$，

$x_{i(n-2)}=f_{(n-2)}(e)$；

(2-4)取出 $x_{i(n-1)},x_{in}$。

记点 $Q_i=(x_{i1},x_{i2},\cdots,x_{in})$。

(3)由 $W_1,\cdots,W_n,Q_i$ 调用算法 2 重构圆，其半径平方为 R，则组密钥为 k：$k=R$。

命题 1 群组成员均能重构群组密钥 k。

证明：每个成员都可从群组管理器的公告牌下载 n 个点 $W_1,W_2,\cdots,W_n$，再根据组密钥分配时所获信息、注册阶段从 G 处得到的一个秘密计算出 n 维空间中的一点，共计$(n+1)$个点。由定理 1 可知$(n+1)$个不同在$(n-1)$空间中的点可以唯一确定一个 n 维空间圆，圆半径的平方为 R，则组密钥 $k=R$。证毕。

命题 2 非群组成员不能获得组密钥。

证明：只要证明了只有 n 个或少于 n 个 n 维空间中的点，不能唯一确定一个 n 维空间中的圆，也就表明了非群组成员不能获得组密钥。

以反证法证明之。假设少于$(n+1)$个点也能唯一确定一个 n 维空间圆，不妨设 n 个点 $W_1,W_2,\cdots,W_n$ 唯一确定一个圆，记为 Ω_1。找出空间一个点 G 不在 Ω_1 上，并使 $W_1,W_2,\cdots,W_n$ 与 G 不在同一个 $n-1$ 维空间中，由定理知 $W_1,W_2,\cdots,W_n,G$ 唯一确定一个圆，并记为 Ω_2。由于 G 不在 Ω_1 上，故 $\Omega_1\neq\Omega_2$，但 $W_1,W_2,\cdots,W_n$ 即在 Ω_1 上又在 Ω_2 上，与 $W_1,W_2,\cdots,W_n$ 唯一确定一个 n 维空间圆矛盾。所以，少于$(n+1)$个点不能唯一确定一个 n 维空间圆。因此，非群组成员不能得到群组密钥。证毕。

命题 3 抵抗联合攻击

证明：作为群组内的成员，利用公开的信息与自己的组密钥影子计算出组密钥，也可由此推出其它成员的影子。然而，被攻击成员的影子本身对攻击者成员并没有意义，因为攻击者并不需要被攻击者的影子来计算组密钥。显然，被攻击者的影子是含了随机数(即随机数 r，随组密钥的变化而变化)与其私钥的单向散列函数值，不可能由这些信息而推出被攻击成员的私钥，更不能推知 G 的私钥。证毕。

2.2.4 群组密钥更新

当群组动态变化时，需要更新组密钥，以保证组密钥的前/后向安全性。若公开参数 Pub-meg 中值不变，则可以减少由于密钥更新带来的通信量。

算法 7 群组密钥更新

(1)随机生成一个 n 维点 W；并且 $W_1,\cdots,W_n$ 与 W 不同在 $(n-1)$维空间中；

(2)利用 Pub-meg 的 n 个点 $W_1,\cdots,W_n$ 与 W 调用算法 2 构圆 Ω'：$(c_1',c_2',\cdots,c_n',R')=$CircleByPoints$(n,W,W_1,\cdots,W_n)$。$R'$就是新的组密钥；

(3)生成一个随机数：$r'\in(0,p)$；

(4)For $i=1$ to m do {//为成员更新群组密钥影子

(4-1)计算 $s_i=f(s_G\times ID_i)$，输入 r',s_i 与圆 Ω'调用算法 1 在圆 Ω'上选取一点 $Q_i'(x'_{i1},x'_{i2},\cdots,x'_{i(n-1)},x'_{in})$，计算 Q_i'点的消息摘要 SHA_i'；

(4-2)将新 $r',(x'_{i(n-1)},x'_{in}),SHA'_i$ 交给用户 M_i。}

M_i 更新相应信息为 $r',(x'_{i(n-1)},x'_{in}),SHA'_i,i=1,2,\cdots,m$。

当有成员加入，新成员注册之后，G 为包含有新成员在内的群组执行群组密钥更新过程；当有成员退出时，G 为除了退出成员之外的所有成员更新组密钥。

2.3 基于二叉密钥树的可扩展群组密钥管理

当群组成员数量很多、动态性很强时，密钥更新的频率就

会很高。SKMBGA 方案随着成员数量的增加，密钥更新所需的时间消耗呈线性增长趋势，因此不适用于超大规模、高动态性的群组通信。若将密钥分配建立层次的树型结构，则密钥更新的时间消耗将由 $O(m)$ 降低为 $O(\log m)$。因此，在 SKMBGA 方案的基础上，这一节设计基于二叉密钥树的群组密钥管理方案，简称为 KTGA(Group Key Management Protocol By Using Key Tree and Geometric Approach)。

2.3.1 二叉密钥树的建立

首先建立二叉树结构的密钥树。为方便说明，采用四维几何空间，涉及的几何图形是四维圆(即四维球面)。依照定理 1 知，5 个四维空间点可以构造唯一四维圆。

在二叉树结构的密钥树中，子结点依据父结点公开的四点、父结点给该结点分配的影子(一个点)来重构父结点的密钥。

简单地，以含 8 个成员的群组为例(见图 1)：成员结点均作为叶子结点 V_{Mi} ($i=1,\cdots,8$)，拥有的私钥记为 k_{Mi} (即上面提及的 s_i)；群组密钥 GK 作为根结点；中间结点用于传送群组密钥给群组成员，这些非叶子结点的密钥值(k_{12}，k_{14}，k_{24}，k_{56}，k_{78}，k_{58}，GK_{18})由群组管理器随机生成。例如成员 M_1 注册为群组成员后获得秘密 k_{M1} (即 3.2 节中的 s_1)，而 k_{M1}，k_{12}，k_{14}，GK_{18} 是 M_1 获得群组密钥 GK_{18} 的路径，即群组管理器采用几何方法将 k_{12}，k_{14}，GK_{18} 的值告知 M_1。管理器采用基于几何的方法建立二叉树型的密钥树：以 k_{12} 为半径平方构造四维圆，取圆上四点 $W_{v12,1}$，$W_{v12,2}$，$W_{v12,3}$，$W_{v12,4}$ 公开(方法同算法 4)；利用 M_1 的秘密 k_{M1} 在圆上取一点 Q_{M1} 交给 M_1(方法同算法 5)，则 M_1 凭借 $W_{v12,1}$，$W_{v12,2}$，$W_{v12,3}$，$W_{v12,4}$ 与 Q_{M1} 重构圆而获得 k_{12}(方法同算法 6)。同理，G 以 k_{14} 为半径平方构造四维圆、公开圆上四点、利用 k_{12} 计算 V_{12} 的影子 Q_{12} 并交给结点 V_{12}(实际上就该点的最后两个坐标值，其它的坐标值由 k_{12} 计算而得)，则 M_1 可利用 k_{12} 与 V_{14} 公开的四点重构圆而得到 k_{14}。依此方法将路径上所有的密钥分配给成员，最终建立了二叉树结构的密钥树。成员顺着路径可获得作为根结点的群组密钥。

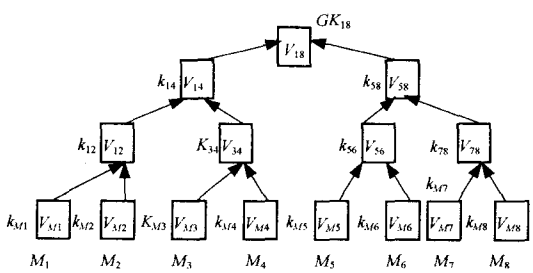

图 1 密钥树

成员 M_i 计算组密钥时，首先获取由代表他的叶子结点到二叉密钥树根结点的路径，设求路径的函数为 KeyPath(M_i)，例如 M_1 的密钥路径为 KeyPath(M_1)=$\{V_{M1}, V_{12}, V_{14}, V_{18}\}$，相应的密钥串为$\{k_{M1}, k_{12}, k_{14}, GK_{18}\}$。

以下是成员 M_i 计算群组密钥的算法。

算法 8 计算群组密钥

(1)求密钥路径 VectorSet=KeyPath(M_i)；

(2)Vector=FirstVector(VectorSet)；//求路径上的第一个结点，即成员结点；

(3)While Vector< >nil do{

(3-1) UpVector=NextVector(Vector,VectorSet) //当前结点的父结点

(3-2)读取 UpVector 的四个公开点：W_1，W_2，W_3，W_4；

(3-3) k=Vector 的密钥；r=UpVector 的随机数；

(3-4)利用 r 与 k 获取 Vector 的影子 Q；

(3-5)重构圆：(c_1, c_2, c_3, c_4, R)= CircleByPoints $(4, W_1, W_2, W_3, W_4, Q)$，即 R 为 UpVector 的密钥；

(3-6) Vector=UpVector。}

(4) 群组密钥为 $GK=R$。

2.3.2 成员的加入/退出

以成员 M_8 加入含有 7 个成员的群组为例描述成员加入的方法(见图 2)。

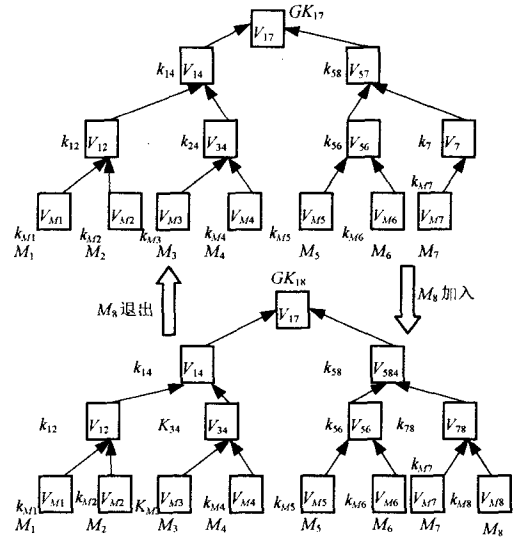

图 2 一个成员加入/退出后的密钥树

M_8 加入时，为了保证组密钥的后向安全性，密钥树上 M_8 到根路径上的各个非叶子结点的密钥都需要改变，即需要生成新的 GK_{18}，k_{58}，k_{78}，代替原来的 GK_{17}，k_{57}，k_7，并且将这些新密钥分配给相应的成员。

以 k_{58} 的分配为例(GK_{18}，k_{78} 的分配与之相同)，V_{57} 原有四个公开点 $W_{v57,1}$，$W_{v57,2}$，$W_{v57,3}$，$W_{v57,4}$，更新后的 V_{58} 仍以这四点为公开点(只是将它们相应地称为 $W_{v58,1}$，$W_{v58,2}$，$W_{v58,3}$，$W_{v58,4}$)，秘密生成一个随机点 W，由 $W_{v58,1}$，$W_{v58,2}$，$W_{v58,3}$，$W_{v58,4}$ 与 W 构造圆 Ω_{58}：CircleByPoints(4，W，$W_{v58,1}$，$W_{v58,2}$，$W_{v58,3}$，$W_{v58,4}$)，则该圆的半径平方就是新的 k_{58}，再为 V_{58} 的两个子结点 V_{56} 与 V_{78} 更新影子 Q_{v56}，Q_{v78}：Q_{v56} = PickPointbyTwo(4，r_{58}，k_{56}，Ω_{58})，Q_{v78} = PickPointbyTwo(4，r_{58}，k_{78}，Ω_{58})。将 Q_{v56}，Q_{v78} 分别传给相关成员。密钥 k_{58} 更新步骤如下：

(1) 随机生成一个点生成 W，保证 W 与 $W_{v58,1}$，$W_{v58,2}$，$W_{v58,3}$，$W_{v58,4}$ 不同在三维空间中；

(2) 计算 Ω_{58}：

$(c_1, c_2, c_3, c_4, k_{58})$ = CircleByPoints(4，W，$W_{v58,1}$，$W_{v58,2}$，$W_{v58,3}$，$W_{v58,4}$)；

(3) 随机生成新的 r_{58}；

(4) 更新 Q_{v56}，Q_{v78}，使这两点在新圆 Ω_{58} 上：

Q_{v56} = PickPointbyTwo(4，r_{58}，k_{56}，Ω_{58})，

Q_{v78} = PickPointbyTwo(4，r_{58}，k_{78}，Ω_{58})。

(5) 设更新后的 Q_{v56}，Q_{v78} 两点的最后两个坐标值为 x_1，x_2，x_3，x_4，利用中国剩余定理将这四个数与 r_{58} 表示成一个数 X：$X=\sum_{i=1}^{5} y_i P_i P_i' \pmod P$，其中 p_1，p_2，p_3，p_4，p_5 为公开数

据，P_i，P_i'的含义见2.2节。并将X传送给成员，成员再将X分离成x_1，x_2，x_3，x_4，r_{58}，从而更新了点Q_{u56}，Q_{u78}及其父结点的随机数。

同理，为了保证组密钥的前向安全性，成员M_8退出也需要更新群组密钥，即密钥树上的$\{k_{78}, k_{58}, GK_{18}\}$更新为$\{k_7, k_{57}, GK_{17}\}$，其过程与成员加入时所作的密钥更新相似，只是不再为退出的成员M_8计算新的k_7的影子，使得M_8不能计算k_7，从而也无法计算k_{57}与GK_{17}。

3 性能分析

从“计算复杂性”、“通信带宽”、“存储需求”、“群组密钥更新需传送的消息数”等方面对KTGA方案与LKH方案进行分析，详见表1。

表1 与LKH的比较

协议	计算复杂性	通信带宽	存储需求	消息个数
LKH	$2\log_2 mE$	$2\|p\|\log_2 m$	$(2m-1)\|p\|$	$2\log_2 m$
KTGA	$\log_2 mC+2\log_2 mP+\log_2 mCR$	$\|p\|\log_2 m$	$(m+1)(n^2+n+2)\|p\|$	$\log_2 m$

表1中的符号含义如下。m：群组成员个数；C：函数CircleByPoints()的时间；P：在四维圆上取一点的时间；CR：由(x_1, x_2, x_3, x_4)计算中国剩余定理值X的时间。

计算复杂性考虑的是群组管理器分配群组密钥所花的时间；通信带宽是指更新群组密钥时群组管理器所发送的消息量；存储需求统计了群组管理器所需要保存的所有信息，包括秘密保存与公开发布的所有消息；群组密钥更新需传送的消息数是指更新群组密钥时群组管理器需要发送的消息条数。

由表1知，与LKH相比，KTGA密钥更新时的通信带宽较小，交换的消息数也较少；由于KTGA群组管理器需要保存公开点的信息，每个点均含多个坐标值，故其存储需求稍多于LKH，但这些公开信息对系统的安全性无影响。

此外，KTGA还有其它的安全优势，如除了用户注册阶段外，不需要安全信道，即传送的成员影子的有关信息均是公开的，无需加密。

4 实验数据与分析

利用JAVA语言实现了文中的SKMBGA与KTGA两个方案，硬件环境是CPU频率为2.5GHz、内存为512MB、操作系统为Window XP的3台机器，JDK版本是1.5，采用Eclipes-SKD-3.0.1的集成工具。一台机器运行G的应用程序，其余两台运行成员应用程序。网络环境为支持TCP/IP协议的校园网。实验用于分析比较文中的SKMBGA与KTGA两个方案。实验数据基于空间维数为4，p的二进制位数为512，讨论它们的时间性能变化与群组成员个数变化的关系，见图3、图4与图5。

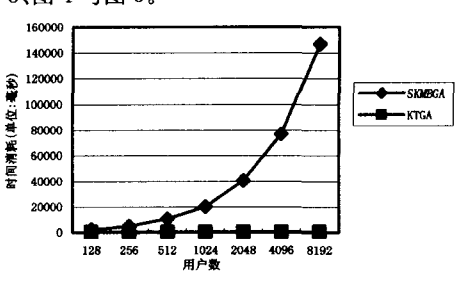

图3 密钥更新时间性能比较

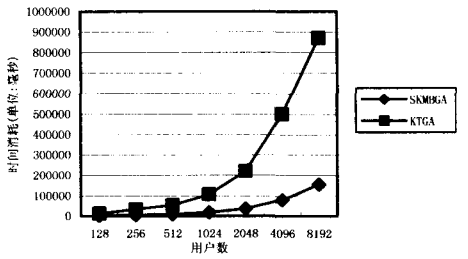

图4 密钥生成与最初影子分配

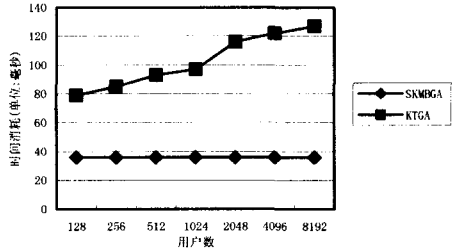

图5 成员计算群组密钥

群组密钥分配中的主要过程含有3个：一是群组生成时的群组密钥生成、分配密钥影子给所有的群组成员，在群组的生命周期该过程只需要执行一次；二是群组成员在获得群组密钥影子之后，利用其影子与公开的信息计算群组密钥，所有成员可并行执行该过程；三是在群组的活动周期内，成员动态加入与退出时群组管理器所执行的群组密钥更新。显然，在大型的、动态的群组通信中，群组密钥更新的性能决定方案的性能。图3表明采用了二叉密钥树结构的KTGA方案的性能远远优于SKMBGA方案。同时，图4与图5表明了KTGA的优势以群组生成、成员计算群组密钥的时间消耗相对较高为代价，这些优势保证了KTGA有高的动态性与可扩展性。

结束语 不同在$n-1$维空间中的$n+1$个n维空间点，能唯一确定一个n维空间圆。基于这个几何性质，本文提出了群组密钥分配方案，在此基础上，采用二叉树结构的密钥树，进一步提出了具有良好扩展性的群组密钥分配协议。群组管理器由它的私钥s_G与成员M_i的身份标识来计算他们之间共享的长期秘密s_i，不需要存储s_i，提高了系统的安全性、计算性能。本方案能够高效处理群组中成员的加入/退出，具有良好的可扩展性。与LKH相比，KTGA无需安全通道(用户注册阶段除外)，也能确保组密钥的前向和后向安全性。

参考文献

[1] Stein M, Tsudik G, Waidner M. Key Agreement in Dynamic Peer Groups[J]. IEEE Trans on Parallel and Distributed Systems, 2000, 11(8): 769-780

[2] Stein M, Tsudik G, Waidner M. Diffie-Hellman Key Distribution Extended to Groups[C]// Proc. 3rd ACM Conf. Computer Communication Security. Mar. 1996: 31-37

[3] Kim Y, Perrig A, Tsudik G. Simple and Fault-tolerant Key Agreement for Dynamic Collaborative Groups[C]// Proceedings of the 7th ACM Conference on Computer and Communication Security. 2000: 235-244

[4] Burmester M, Desmedt Y. A Secure And Efficient Conference Key Distribution System[C]// Advances in Cryptology-Eurocrypt'94. LNCS, 1994: 275-287

(下转第119页)

用户设备之间进行内容传输之前必须通过身份证书进行身份验证，保证了数据传输的安全性。

2)在本系统中，如果要解密数字内容进行使用，必须获取内容解密密钥，而内容解密密钥必须用用户设备的私钥来解密，因此数字内容加密方法的安全性等同于 RSA 算法的安全性。而对 RSA 算法最常用的攻击方式是分解 N_i，N_i 的位数越多，分解的难度就越大。这里 N_i 的位数为 512bit，足以保证系统的安全性。

3)实际使用的 DRM 系统常常采用某些方式进行版权的跟踪(如数字水印技术等)。如果家庭网关发现某用户设备有版权侵害行为，可将其从合法用户列表中清除；如果 DRM 服务器发现某家庭网络内的用户设备有版权侵害行为，可降低该家庭网络的信用等级，情况严重时可能会撤销该家庭网关的身份证书，使该家庭网络无法继续使用系统提供的服务。这种手段能够在很大程度上遏制数字版权侵害行为的发生。

4.2 与其它 DRM 系统的比较

微软公司的 WMRM(Windows Media Rights Manager)、Intertrust 公司的 DRM 系统以及本文所提出的 DRM 之间的比较如表 1 所列。

表 1 与现有的 DRM 系统的比较

	微软的 WMDM 系统	Intertrust 公司的 DRM 系统	本文所提出的系统
版权保护	能够实现	能够实现	能够实现
网络依赖	很高	非常高	较低
证书共享	不支持	不支持	支持

在版权保护方面，这 3 个 DRM 系统都能够实现对数字内容版权的保护，而本文提出的 DRM 系统主要侧重于保护家庭网络内的数字内容；在对网络的依赖性方面，由于微软的 WMDM 系统和 Intertrust 的 DRM 系统需要时刻保持在线连接以确保内容的安全性，因此对网络的依赖性很大，而本文提出的系统由于家庭网关设备的存在，使得 DRM 的大部分功能可以在本地完成，因此对网络的依赖性较低；在对数字许可证的共享方面，微软的 WMDM 系统和 Intertrust 的 DRM 系统都不支持，即每当内容重新传递后，都需要重新请求数字许可证，而本文提出的 DRM 系统则允许用户设备共享该内容的数字许可证。因此，相对现有的这些 DRM 系统来说，本系统更适合家庭网络这个特定的应用环境。

而通过和一些已提出的面向家庭网络的 DRM 研究方案相比(如前文所提到的 Lee Young Gu 等人及 Azfar Moid 等人提出的 DRM 方案)，本系统的管理模式更为灵活，通过组密钥技术和对内容超级分发的支持可方便地实现内容的共享，且对用户设备的硬件并无特殊要求，在实际环境中能得到较好的应用。

结束语 本文针对家庭网络的用户需求，提出了一种对家庭网络内的数字内容进行版权保护的 DRM 系统。系统中家庭网关通过组密钥技术，使得 DRM 服务器针对特定的数字内容只需传输一次数字许可证，并且只有合法用户设备才能使用该数字许可证。用户设备还可通过对数字内容进行超级分发来实现数字内容的共享。与已有的一些 DRM 系统相比，本系统的扩展性好，管理方式灵活，可方便地实现家庭网络用户设备之间数字内容的共享。

参 考 文 献

[1] 彭海清，冯涛，童登金. 家庭网络的关键技术、业务及标准化[J]. 研究与设计，2004(11)：5-8

[2] 房胜，钟玉琢. 蓝牙-家庭网络中服务的调用和实现[J]. 计算机科学，2004，31(2)：36-39

[3] Lin E T, Eskicioglu A M, Lagendijk R L, et al. Digital Video Content Protection[J]. Advances in Video Coding and Delivery, 2005, 93(1): 171-182

[4] Dhamija R, Wallenberg F. A framework for evaluating digit rights management proposals[C]// Proceedings of the 1st International Mobile IPR Workshop. Helsinki Finland, 2003

[5] Koster P, Montaner J, Koraichi N, et al. Introduction of the Domain issuer in OMA DRM[C]// The 4th Annual IEEE Consumer Communications and Networking Conference. Las Vegas NV USA, 2007

[6] Lee Young Gu , Lee Chang Bo . A Study on Secure Contents Transmission in Home Domain[C]// 2008 International Conference on Convergence and Hybrid Information Technology. Daejeon South Korea, 2008

[7] Moid A, Fapojuwo A O, Davies R J. Secure and Scalable Video Streaming over IEEE 802. 11e based Home Networks[C]// 2007 Canadian Conference on Electrical and Computer Engineering. Vancouver BC Canada, 2007

(上接第 105 页)

[5] Caronni G, Waldvogel M, Sun D. Efficient security for large and dynamic multicast groups[C]// Stanford. Proc the 7th Workshop on Enabling Technologies (WETICE'98). Washington: IEEE Computer Society Press, 1998: 376-383

[6] Wong C K, Gouda M, Lam S S. Secure group communications using key graphs[J]. IEEE/ACM Trans. Networking, 2000, 8(1): 16-30

[7] Kwak Deuk-whee, Kim Jong won. A Decentralized Group Key Management Scheme for the Decentralized P2P Environment [J]. IEEE Communications Letters, 2007, 11(6): 555-557

[8] Duta R, Barua R. Provably Secure Constant Round Contributory Group Key Agreement in Dynamic Setting[J]. IEEE Transactions on Informations Theory, 2008, 54(5): 2007-2025

[9] Song Ronggong, Korba L, Yee G O M. A Scalable Group Key Management Protocol[J]. IEEE Communication Letters, 2008, 12(7): 541-543

[10] Wu T C. Remote Login Authentication Scheme Based on a Geometric Approach[J]. Computer Communications, 1995, 18(12): 959-963

[11] Hwang M S. Cryptanalysis of a Remote Login Authentication Scheme[J]. Computer Communications, 1999, 22(8): 742-744

[12] Chien H Y, Jan J K, Tseng Y M. A Modified Remote Login Authentication Scheme Based on Geometric Approach[J]. Journal of Systems and Software, 2001, 55(3): 287-290

[13] Wang S J. Yet another login authentication using N-dimensional construction based on circle property[J]. IEEE Trans. on Consumer Electronics, 2003, 49(2): 337-341

[14] Wang S H, Feng B, Wang J. Comments on Yet Another Log-in Authentication Using N-dimensional Construction [J]. IEEE Transaction on Consumer Electronics, 2004, 50(2): 606-608

[15] Yang F Y, Jan J K. Cryptanalysis of Log - in Authentication Based on Circle Property [J]. IEEE Transaction on Consumer Electronics, 2004, 50(2): 625-628

[16] Wu T C, He W-H. A geometric approach for sharing secrets[J]. Computer & Security, 1995: 135-145

[17] Chor L P , Jing H W , Chong T P . A geometric approach for shared secrets, a refinement[J]. Computers & Security, 1998, 17(10): 725-732