基于 Merkle 身份树的动态对等群组密钥协商 *

陈礼青
(淮阴工学院 计算机工程学院, 江苏 淮安 223003)

摘 要: 针对设计高效的分布式密钥协商方案是动态对等群组组播通信的难点,提出了一个新的基于 Merkle 身份树的密钥协商方案,并具体地分析了子组之间的通信过程,以及组成员动态变化时密钥的更新过程。结果表明该方案在降低计算和通信代价方面取得了较好的效果。

关键词: 动态对等群组; 密钥协商; 身份树; 双线性对
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2010)02-0682-03
doi:10.3969/j.issn.1001-3695.2010.02.077

Key agreement scheme for dynamic peer groups based on Merkle identity tree

CHEN Li-qing
(*School of Computer Engineering, Huaiyin Institute of Technology, Huai'an Jiangsu* 223003, *China*)

Abstract: Designing efficient distributive key agreement scheme was a difficult problem in multicast communication of dynamic peer groups. This paper proposed a new key agreement scheme for multicast groups based on Merkle identity tree . Then analyzed the procedures of secret communications between subgroups and updating of group keys with the dynamic change of group members in detail. The analysis shows that the new scheme is efficient in computation and communication.
Key words: dynamic peer groups; key agreement; identity tree; bilinear pairing

组播提供了一种发送者可以同时发送信息到多个接收者的高效通信机制,其通过在路由器上合并重复信息的传输,从而有效地节约了带宽,降低了服务器的负担。组播通信的方式大致可分为三类:a)一对多,一个发送者和多个接收者,如视频点播;b)少对多,少数发送者和多个接收者,如 GPS;c)多对多,所有成员都是对等体,可以动态地成为发送者或接收者,如分布式系统、视频电话会议、网络游戏等。这种方式的组播组又称为动态对等群组(dynamic peer groups)。

安全组播的一个主要难点是如何确保只有合法的组注册用户才能接收到组播通信数据。其中,动态对等群组(DPG)由于显著的对称性和动态性,又无疑是最具挑战性的课题。近年来将密码学新技术,如基于身份的密码系统应用到 DPG 的分布式密钥协商中,已成为新的研究热点[1~5]。文献[6]中提出的方案很好地解决了基于身份的密码系统下单个 KGC 容易成为整个组播体系性能瓶颈的问题,但是其只适用于发送者在组播组外的应用。在其方案中,KGCs 不仅是组成员注册和密钥分发的中心,还承担了外部发送者与组播组之间的消息转发任务,即 KGCs 将消息分别用各个子组协商出的密钥加密后转发给各个子组。而对于那些组内部分或所有成员之间需要相互通信的 DPG 应用,如视频电话会议,若采用这个方案则存在着 KGCs 计算代价较高、通信延迟等不足。为此,本文在其基础上提出了一个新的基于 Merkle 身份树的 DPG 密钥协商方案,较好地解决了不经过 KGCs 而实现组内成员保密通信的问题。本方案所适用的 DPG 组播体系结构如图 1 所示。

Merkle 树是一种特殊的二叉树,其在每个节点中存储一个值:对于每一个叶子节点是一条指令加上该指令的 hash 值构成;每个父节点下面的所有子节点的 hash 值组合到一起,再进行 hash 运算就得到它们的父节点。这个过程一直进行下去,直至得到树的根节点。Merkle 树的主要优点是仅需通过对树根节点的一次签名运算就可以对树上所有的叶子节点独立地提供完整性认证。本文为应用基于身份的密码系统进行 DPG 组会话密钥的协商,提出了 Merkle 身份树的概念。在 Merkle 身份树中,叶子节点存储 DPG 组成员身份信息的 hash 值。

1 预备知识

1.1 双线性映射

设 G_1、G_2 都是阶为素数 q 的循环群,G_1 的运算记为加法,G_2 的运算记为乘法。一个双线性映射(bilinear maps) $\hat{e}: G_1 \times G_1 \to G_2$ 是满足如下三条性质的映射:

a)双线性。对于所有的 $P, Q \in G_1$,以及 $a, b \in Z_q^*$,$\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$。

b)非退化性。若 P 是 G_1 的一个生成元,$\hat{e}(P, P) \neq 1_{G_2}$。

c)可计算性。存在一个有效的算法来计算 $\hat{e}(P, Q)$。

1.2 计算复杂性假设

定义 1 离散对数问题(DLP)。给定加法循环群 G_1,G_1 的一个生成元 P 及任意 $Q \in G_1$,求最小非负整数 x,使得 $Q = xP$。

定义 2 计算 Diffie-Hellman 问题(CDHP)给定加法循环

收稿日期: 2009-05-26; **修回日期**: 2009-10-20 **基金项目**: 国家自然科学基金资助项目(60673070);江苏省自然科学基金资助项目(BK2006217);淮阴工学院青年教师科研基金项目(HGC0916)

作者简介:陈礼青(1982-),男,江苏东台人,讲师,硕士,主要研究方向为网络与信息安全、安全组播与密钥协商(quietloner@sina.com).

群 G_1,G_1 的一个生成元 P 和随机的 $aP, bP \in G_1$(a, b 未知),计算 abP。

定义 3　双线性逆 Diffie-Hellman 问题(BIDHP) G_1, G_2, P 和 $\hat{e}$ 如前面所定义,给定(P, aP, bP)。其中 $a, b \in Z_q^*$,计算 $\hat{e}(P,P)^{a^{-1}b}$。

复杂性假设:在 G_1、G_2 中的 DLP,CDHP 和 BIDHP 都是困难问题,即不存在一个多项式时间算法能以不可忽略的概率解决其中任何一个问题。

2　基于 Merkle 身份树的 DPG 密钥协商方案

2.1　变量标记说明及系统初始化

本方案涉及到如下一些变量标记:

SG_{ID}为子组的身份标志;Q_{ID}为子组的身份标志的 hash 值;$P_{pub_{ID}}$为子组的公钥参数;D_{ID}为子组的私钥;h 为子组 Merkle 身份树的最大高度;U_i 为子组中的第 i 个成员,$i \in \{1,2,\cdots,t\}$;ID_i 为 U_i 的身份标志;N_i^j 为子组 Merkle 身份树中第 i 层的第 j 个节点;Q_i^j 为节点 N_i^j 身份标志的 hash 值;P_i^j 为节点 N_i^j 的私钥;BK_i^j 为节点 N_i^j 的盲密钥;K_i^j 为节点 N_i^j 的生成密钥;KGC_i 为第 i 个 KGC;s_i 为 KGC_i 的主密钥;n 为组播消息的 bit 长度。

给定系统安全参数 1^k($k = |q|$),KGCs 运行双线性 Diffie-Hellman 参数生成算法Ig,生成如前定义的 G_1、G_2,以及一个双线性映射 $\hat{e}: G_1 \times G_1 \to G_2$,$G_1$ 是阶为素数 q 的循环加法群,G_2 是与 G_1 相关的阶同为 q 的乘法群,选择 G_1 的生成元为 P。定义一组 hash 函数:$H_1: \{0,1\}^* \to Z_q^*$,$H_2: Z_q^* \times Z_q^* \to Z_q^*$,$H_3: G_2 \to Z_q^*$,$H_4: \{0,1\}^* \to G_1^*$,$H_5: G_2 \to \{0,1\}^n$,$H_6: \{0,1\}^n \to Z_q^*$,$H_7: \{0,1\}^n \to \{0,1\}^n$。KGCs 发布系统的公共参数为 $params = \{G_1, G_2, \hat{e}, P, H_1, H_2, H_3, H_4, H_5, H_6, H_7, n\}$,组播消息明文空间为$M = \{0,1\}^n$,密文空间为$C = G_1 \times \{0,1\}^n$。

2.2　DPG 组播成员注册及子组密钥协商过程

希望加入 DPG 组播组的用户向 KGCs 注册成为组的合法成员。KGCs 按照组成员所在的地理位置将整个大的 DPG 组播组划分为多个子组,为保证一定的通信效率,各个子组的成员数应控制在 2^{h-1}(h 为实际组播应用中子组 Merkle 身份树的最大高度)以内。对于任一个子组,KGCs 采用一棵逻辑意义上的平衡二叉树结构将所有组成员安排在叶子节点。所有的子组 Merkle 身份树信息都作为公共信息发布。由图 2 可见一棵子组 Merkle 身份树的结构。Merkle 身份树中节点采用由上至下、从左向右的标号顺序,这种方式更加合理,在子组成员发生变化时,可以使需要更改标记的节点数最少。

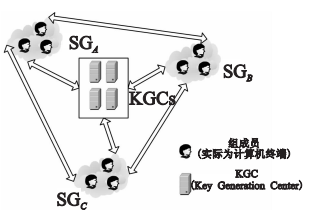

图1　DPG组播体系结构

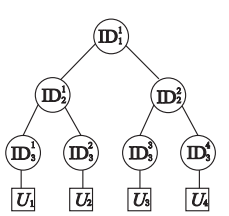

图2　子组Merkle身份树示例

Merkle 身份树中的每一个节点分别关联三个密钥,即私钥、盲密钥和生成密钥。组成员在注册时,KGCs 将从根节点到此组成员所在叶子节点这条路径上所有节点(不包括根节点)的私钥通过秘密信道发送给组成员。此秘密信道是在组成员注册时与 KGCs 建立的。叶子节点的生成密钥也在注册时各自发送给组成员。所有节点的盲密钥作为公共信息发布。而中间节点的生成密钥则要由各个组成员借助已有密钥由下至上逐层协商得到,最终协商出的根节点的生成密钥结合子组的身份信息即作为子组成员共享的私钥,以用于解密接收到的 DPG 组播消息。

对于叶子节点,$Q_i^j = H_1(ID_i^j)$;对于中间节点,$Q_i^j = H_2(Q_{i+1}^{2j-1}, Q_{i+1}^{2j})$。假定当前处于工作状态的是 KGC_v,则其为节点 N_i^j 生成私钥和盲密钥的过程为,KGC_v 首先计算 $P_i^j = (Q_i^j + s_v)^{-1}P$ 和 $TK_i^j = (Q_i^j + s_v)P$。其中 s_v 为 KGC_v 的主密钥,P_i^j 和 TK_i^j 分别作为 N_i^j 的私钥和临时密钥,且临时密钥仅为 KGCs 所掌握。KGC_v 为组成员随机选择一个生成密钥 $K_i^j \in Z_q^*$,并连同从根节点到此组成员所在叶子节点这条路径上所有节点(不包括根节点)的私钥一起通过秘密信道安全单播发送给注册组成员。定义 $K_{i+1}^{2j-1}TK_{i+1}^{2j}$ 和 $K_{i+1}^{2j}TK_{i+1}^{2j-1}$ 为节点 N_i^j 的一对盲化因子,则节点 N_{i+1}^{2j-1} 和 N_{i+1}^{2j} 的盲密钥分别为 $BK_{i+1}^{2j-1} = K_{i+1}^{2j-1}TK_{i+1}^{2j}$,$BK_{i+1}^{2j} = K_{i+1}^{2j}TK_{i+1}^{2j-1}$。所有盲密钥作为公共信息发布。利用已知的私钥和盲密钥,中间节点 N_i^j 的左孩子节点 N_{i+1}^{2j-1} 和右孩子节点 N_{i+1}^{2j} 可分别计算其父节点 N_i^j 的生成密钥 K_i^j。

对于左孩子节点 N_{i+1}^{2j-1}:

$$K_i^j = H_3(\hat{e}(P_{i+1}^{2j-1}, BK_{i+1}^{2j})^{K_{i+1}^{2j-1}}) = H_3(\hat{e}((Q_{i+1}^{2j-1} + s_v)^{-1}P, K_{i+1}^{2j}(Q_{i+1}^{2j-1} + s_v)P)^{K_{i+1}^{2j-1}}) = H_3(\hat{e}(P,P)^{K_{i+1}^{2j}K_{i+1}^{2j-1}}) \quad (1)$$

对于右孩子节点 N_{i+1}^{2j}:

$$K_i^j = H_3(\hat{e}(P_{i+1}^{2j}, BK_{i+1}^{2j-1})^{K_{i+1}^{2j}}) = H_3(\hat{e}((Q_{i+1}^{2j} + s_w)^{-1}P, K_{i+1}^{2j-1}(Q_{i+} + s_w)P)^{K_{i+1}^{2j}}) = H_3(\hat{e}(P,P)^{K_{i+1}^{2j}K_{i+1}^{2j-1}}) \quad (2)$$

如此逐层向上,最终每个组成员都可计算出根节点的生成密钥 K_1^1。注意式(1)和(2)中,s_v 区别于 s_w 表明了一组 KGCs 的作用所在,即每个组成员都随机地与任意一个 KGC 联系,注册并获得相应的密钥,却不影响子组成员最后可以协商出同一个密钥,从而实现了分布式管理,大大减轻了单个 KGC 的工作负担,提高了 DPG 组播系统的可扩展性。

仍以图 2 为例,U_2 从 KGCs 处获得了 K_3^2 以及 P_3^2、P_2^1,所有节点的盲密钥为公共信息。则 U_2 计算 K_1^1 的过程如下:

首先计算 K_2^1

$$K_2^1 = H_3(\hat{e}(P_3^2, BK_3^1)^{K_3^2}) = H_3(\hat{e}((Q_3^2 + s_v)^{-1}P, K_3^1(Q_3^2 + s_v)P)^{K_3^2}) = H_3(\hat{e}(P,P)^{K_3^1K_3^2}) \quad (3)$$

然后再计算 K_1^1

$$K_1^1 = H_3(\hat{e}(P_2^1, BK_2^2)^{K_2^1}) = H_3(\hat{e}((Q_2^1 + s_w)^{-1}P, K_2^2(Q_2^1 + s_w)P)^{K_2^1}) = H_3(\hat{e}(P,P)^{K_2^1K_2^2}) \quad (4)$$

若从 U_3 或 U_4 的角度出发,计算 K_2^2,可得

$$K_2^2 = H_3(\hat{e}(P,P)^{K_3^3K_4^3}) \quad (5)$$

将式(3)和(5)代入式(4),可进一步将 K_1^1 转换为如下形式:

$$K_1^1 = H_3(\hat{e}(P,P)^{H_3(\hat{e}(P,P)^{K_3^1K_3^2})H_3(\hat{e}(P,P)^{K_3^3K_3^4})}) \quad (6)$$

由式(6)显见,子组成员最终协商出的根节点的生成密钥仅与子组成员所关联的叶子节点的生成密钥有关。

2.3 DPG 组播通信过程

2.3.1 发送者在组内

假定图2中子组的身份标志为 SG_A,则 $Q_A = H_4(SG_A)$。采用文献[7]中的安全性要求更高的基于身份的加密方案 Full Ident。则子组 SG_A 的公钥参数 $P_{\text{pub}_A} = K_1^1 P$,私钥 $D_A = K_1^1 Q_A$。其中:K_1^1 为子组 SG_A 中成员协商出的根节点的生成密钥;P 为 G_1 的生成元。KGCs 处公开所有子组的身份标志以及对应的公钥。

子组 SG_B 中的某个成员给子组 SG_A 发送消息的过程为,从 KGCs 处公布的信息中获得 Q_A 和 P_{pub_A},然后随机选择 $\sigma \in \{0,1\}^n$,计算 $r = H_6(\sigma, M)$。对于 $M \in M$,加密后的密文为

$$C = \langle U, V, W \rangle = \langle rP, \sigma \oplus H_5(\hat{e}(Q_A, P_{\text{pub}_A})^r), M \oplus H_7(\sigma) \rangle$$

子组 SG_A 中成员解密过程如下:

a)首先计算 $V \oplus H_5(\hat{e}(D_A, U))$,

$$V \oplus H_5(\hat{e}(D_A, U)) = V \oplus H_5(\hat{e}(K_1^1 Q_A, rP)) =$$

$$V \oplus H_5(\hat{e}(Q_A, K_1^1 P)^r) = V \oplus H_5(\hat{e}(Q_A, P_{\text{pub}_A})^r) = \sigma'$$

b)再计算 $W \oplus H_7(\sigma') = M'$,

c)最后令 $r' = H_6(\sigma', M')$,若 $U \neq r'P$,则拒绝接收此密文;否则,M' 即为解密后的明文。

2.3.2 发送者在组外

以上通信过程考虑的是组内成员相互通信的应用场景,如视频电话会议。实际上,对于发送者在组外的一般意义的组播应用,如视频点播,此方案同样适合。具体过程是,外部发送者首先将会话密钥通过上述方案加密发送给各子组,从而所有的合法组成员便可解密获得会话密钥;然后发送者用会话密钥加密真正的组播通信数据,发送到组播组。

2.4 新成员加入过程

仍以图2所示的子组为例,假设有新成员 U_5 要求加入,则 KGCs 更新子组 Merkle 身份树,如图3所示。

显见,图中虚线部分为 U_5 加入后受到影响的节点。U_4 被关联到新的叶子节点 ID_4^1 上,U_5 则在其兄弟节点 ID_4^2 上。更新子组 Merkle 身份树的一个基本原则是确保每个节点(除根节点)都有兄弟节点。KGCs 为受影响的节点重新计算 hash 值、私钥和盲密钥,并选择 $K_4^2 \in Z_q^*$,连同 P_4^2、P_3^4 和 P_2^2 一起安全单播给 U_5。需要注意的是,KGCs 应将更新后的 P_2^2 发送给 U_3,以及更新后的 P_2^2、P_3^4 和 P_4^1 发送给 U_4,而 U_5 加入前的 K_3^4 仍可作为 K_4^1 使用。

子组 Merkle 身份树更新后,$U_1 \sim U_5$ 协商更新后的 K_1^1 的过程与2.2节类似,不再详述。由于根节点到 U_5 所在叶子节点这条路径所有节点的私钥和盲密钥都已更新,U_5 便无法计算出其加入之前子组的 K_1^1,也就无法获得子组以前的私钥,自然也无法解密组之前的通信内容,从而保证了组播的前向安全要求。

需要说明的是,此例考虑的是单个或少量成员加入的情形,当有大量成员同时要求加入组播组时,KGCs 为之创建一个新子组的计算和通信代价要远小于逐个更新各子组的代价。

2.5 组成员退出过程

以图3所示的变化后的子组为例,假设成员 U_4 和 U_5 同时退出子组,则更新后的子组 Merkle 身份树如图4所示。

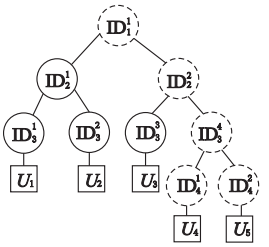

图3 子组增加新成员 U_5

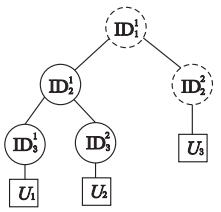

图4 成员 U_4 和 U_5 退出子组

为确保更新后的子组 Merkle 身份树中每个节点(除根节点)都有兄弟节点,U_3 被提升关联到节点 ID_2^2 上。与加入过程类似,KGCs 为受影响的节点重新计算 hash 值、私钥和盲密钥。此例中,即 KGCs 需要将更新后的 P_2^2 发送给 U_3。U_1 到 U_3 重新协商出一个新的 K_1^1。退出的 U_4 和 U_5 由于不掌握更新的 P_2^2,便无法计算出更新的 K_1^1,从而保证了组播的后向安全要求。

3 安全性分析

从密钥协商安全性要求的角度来看,本方案可满足其要求:

a)组会话密钥安全。每轮密钥协商过程中都有一个随机数 $\sigma \in \{0,1\}^n$,基于 DLP、CDHP 和 BIDHP 困难问题假设,被动攻击者通过窃听组广播消息获取组会话密钥在计算上是不可行的。

b)前向安全。当有新成员 U_j 加入组播组时,子组身份树的根节点到 U_j 所在节点这条路径上所有的私钥和盲密钥都将更新,U_j 则无法计算其加入组之前所在子组 K_1^1 的及私钥,保证了前向安全。

c)后向安全。对于退出组播组的成员 U_l,同样由于其所在子组身份树信息的更新,也无法计算出其退出后的 K_1^1,从而保证了后向安全。

d)抗合谋攻击。对于退出组播组的一组成员,即使其合谋也无法计算出所在子组的 K_1^1。

4 计算与通信代价分析

从上述过程可知,在整个安全组播生命期内,KGCs 只负责系统初始化、成员注册以及运行过程中组成员动态变化时公共信息的更新工作。具体地说,其需要维护并公开发布两张表,即各子组 Merkle 身份树信息表 $\{SG_{\text{ID}}, \text{ID}_i^j, Q_i^j, BK_i^j, \text{ID}_{\text{Lchild}}, \text{ID}_{\text{Rchild}}\}$ 和各子组公钥信息表 $\{SG_{\text{ID}}, Q_{\text{ID}}, P_{\text{pub}_{\text{ID}}}, U_{\text{Users}}\}$。其中:$\text{ID}_{\text{Lchild}}$、$\text{ID}_{\text{Rchild}}$ 分别指节点 N_i^j 的左、右孩子节点的身份信息,若 N_i^j 为叶子节点,则其 $\text{ID}_{\text{Lchild}}$ 和 $\text{ID}_{\text{Rchild}}$ 记为"-",N_{users} 指子组 SG_{ID} 当前的成员数,$N_{\text{Users}} \leqslant 2^{h-1}$。

对于各子组中的每个成员,则需要在本地保密并维护表 $\{\text{ID}_i^j, Q_i^j, P_i^j\}$,以保存和更新 KGCs 发来的从其所在叶子节点到子组根节点(根节点除外)这条路径上所有节点的私钥。

前文已定义每棵子组 Merkle 身份树的最大高度为 h,则每个成员最多需要在本地保存 $(h-1)$ 条相关节点私钥信息。

子组成员协商密钥时,每个成员最多需要作 $(h-1)$ 次 pairing 运算。

当某个成员需要与 t 个子组进行通信时, (下转第 688 页)

和三次椭圆曲线加法运算;新方案需两次哈希、三次椭圆曲线乘法和两次椭圆曲线加法运算。显然,新方案的效率要高于 ZL 方案。

5　结束语

本文首先介绍了文献[14]提出的基于椭圆曲线的代理签名方案并构造了针对该方案的原始签名人伪造攻击;然后提出新的方案,并验证了新的安全代理签名方案避免了以往方案所存在的安全问题,满足引言中所列出的典型代理签名方案应具备的六个方面的安全特性。新方案具有椭圆曲线密码体制安全性高、密钥短小、运算速度快等优点,具备强代理签名方案所应有的性质,且无须安全信道,具有更强的抗攻击性和更高的实用价值。

参考文献:

[1] MAMBO M, USUDA K, OKAMOTO E. Proxy signature: delegation of the power to sign messages[J]. IEICE Trans on Fundamentals of Electronics Communications and Computer Sciences, 1996, E79A(9): 1338-1354.

[2] 祁明, HARN L. 基于离散对数的若干新型代理签名方案[J]. 电子学报, 2000,28(11):114-115.

[3] SHAO Zu-hua. Proxy signature schemes based on factoring[J]. Information Processing Letters, 2003,85(3): 137-143.

[4] LEE B, KIM H, KIM K. Strong proxy signature and its applications [C]//Proc of Symposium on Cryptography and Information Security. Oiso, Japan :[s. n.], 2001:603-608.

[5] 杨伟强, 徐秋亮. 典型代理签名方案的分析与改进[J]. 计算机工程与应用, 2004,40(9): 152-154.

[6] KOBLITZ N. Elliptic curve cryptosystems[J]. Mathematics of Computation,1987,48(1): 203-209.

[7] MILLER V S. Use of elliptic curve in cryptography[C]//Proc of Advances in Cryptology-Crypto'85. New York: Springer-Verlag,1986: 417-426.

[8] CAELLI W J, DAWSON E P, REA S A. PKI, elliptic curve cryptography, and digital signatures [J]. Computers and Security, 1999, 18(1): 47-66.

[9] CHEN T S, LIU T P, HWANG G S, *et al*. An improvement of proxy-protected proxy multi-signature scheme[C]//Proc of the 13th International Conference on Information Management. 2002:33-40.

[10] CHEN T S, CHUNG Y F, HWANG G S. Efficient proxy multi-signature schemes based on the elliptic curve cryptosystem[J]. Computers & Security,2003,22(6):527-534.

[11] 曹天杰,林东岱,薛锐. 基于椭圆曲线的代理多签名方案的安全性分析[J]. 小型微型计算机系统,2006,27(5):798-801.

[12] 纪家慧,李大兴.新的代理多签名体制[J].计算机研究与发展, 2004,141(14):715-719.

[13] 吴旭辉,沈庆浩.一种代理多签名体制的安全性分析[J].通信学报, 2005,26(7):119-122.

[14] 左为平, 李海峰. 一种安全的椭圆曲线代理签名方案[J]. 佳木斯大学学报:自然科学版, 2007,25(4): 495-497.

[15] CHANG M H, CHEN I T, CHEN M T. Design of proxy signature in ECDSA[C]//Proc of the 8th International Conference on Intelligent Systems Design and Applications. Kaohsiung City, Taiwan:[s. n.], 2008: 17-22.

(上接第 684 页)其需要将欲发送的消息分别用各子组的公钥进行加密后连接起来广播出去,消息总长度大约为 2 tn。

5　结束语

设计动态高效的分布式组密钥管理协议是 DPG 组播通信需要重点考虑的问题。本文在文献[6]的基础上,提出了一个新的基于 Merkle 身份树的 DPG 密钥协商方案,实现了任意多个子组之间的保密通信,而无须经过 KGCs 的转发,避免了其翻译组播消息时所引起的延迟,具有较高的灵活性。子组成员之间以及子组与子组之间,在协商密钥或通信时都是相互独立的,充分体现了分布式的特点。使用一组并行工作的 KGCs,也大大降低了单个 KGC 的工作负担,避免了单点故障的产生,提高了组播系统的健壮性。

密钥托管(key escrow)是基于身份的密码系统所固有的缺点,本文方案同样存在这个问题,即 KGCs 可以计算出所有子组的公、私钥。近年来提出的无证书密码系统[7,8]在传统的基于证书的公钥密码系统和基于身份的公钥密码系统之间进行了适当的折中,取得了较好的效果。下一步的工作将考虑应用无证书的密码系统,以期构造一个更安全的密钥协商方案。

参考文献:

[1] MA Chun-bo, AO Jun, LI Jian-hua. A novel verifier-based authenticated key agreement protocol[C]//Proc of International Conference on Intelligent Computing. Heidelberg: Springer, 2007: 1044-1050.

[2] YOON E J, YOO K Y. A new key agreement protocol based on chaotic maps[C]//Proc of the 2nd International Symposium on Agents and Multi-agent Systems: Technologies and Applications. Heidelberg: Springer, 2008: 897-906.

[3] SVEN L, SYLVAIN P. SAS-based group authentication and key agreement protocols[C]//Proc of International Conference on Theory and Practice of Public-Key Cryptography. Heidelberg: Springer, 2008: 197-213.

[4] CHEN L, CHENG Z, SMART N P. Identity-based key agreement protocols from pairings[J]. International Journal of Information Security,2007,6(4): 213-241.

[5] CHIEN Hung-yu. ID-based key agreement with anonymity for Ad hoc networks[C]//Proc of IFIP International Conference on Embedded and Ubiquitous Computing. Heidelberg: Springer, 2007: 333-345.

[6] WANG Li-ming, WU Chuan-kun. Efficient key agreement for large and dynamic multicast groups[J]. International Journal of Network Security,2006, 3(1): 11-20.

[7] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Advances in Cryptology. Heidelberg: Springer, 2003: 452-473.

[8] MANDT T K, TAN C H. Certificateless authenticated two-party key agreement protocols[M]. Heidelberg: Springer, 2007: 37-44.

[9] BONEH D, FRANKLIN M K. Identity-based encryption from the Weil pairing[C]//Proc of the 21st Annual International Cryptology Conference on Advances in Cryptology. London, UK: Springer, 2001: 213-229.