基于身份的多方认证组密钥协商协议

钟 欢,许春香
(电子科技大学计算机学院,四川成都 610054)

摘 要: 2002 年,Boneh 和 Silverberg 提出了多线性表理论和基于多线性表的多方 Diffe-Hellman 密钥交换协议,H. K. Lee 等人在该协议基础上利用证书对参与者进行身份认证,解决了该协议容易遭受中间人攻击的问题,H. M. Lee 等人进一步引入基于身份的公钥密码技术替代数字证书,提高了密钥协商的效率,形成了 ID-MAK 协议. 在本文中,我们对 ID-MAK 协议进行了安全性分析,发现 ID-MAK 协议没有真正实现它所宣称的身份认证,不能抵御主动攻击,敌手可冒充任意合法成员参与到密钥协商中获取组密钥. 本文在计算多线性 D-H 问题假设下提出了两个 ID-MAK 协议改进方案,两个改进协议只需一轮即可协商一个组密钥,本文还给出了相应的成员动态变化和组密钥更新协议. 本文最后对我们改进的协议进行了安全性分析.

关键词: 多方密钥协商; 认证; 基于身份的公钥; 多线性表
中图分类号: TN914 **文献标识码**: A **文章编号**: 0372-2112 (2008) 10-1869-04

ID-based Multi-Party Authenticated Key Agreement Protocols Using Multilinear Forms

ZHONG Huan, XU Chun-xiang
(*School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan* 610054, *China*)

Abstract: In 2002, Boneh and Silverberg presented theory of multilinear forms and a multi-party Diffe-Hellman key agreement protocol using multilinear forms. H. K. Lee et al adopted certificates to authenticate group members and protect against middle-man attacks in this protocol. Subsequently, H. M. Lee et al deployed ID-base public keys other than certificates in the MAK protocol, and presented the ID-MAK protocol. Owing to simplicity of ID-base public keys, the ID-MAK Protocol is more efficient. In this paper, we analyze the security of the ID-MAK protocol, and have found that the ID-MAK protocol doesn't really authenticate group members as claimed. Thus it cannot resist active attacks, and an adversary can pretend to be a legal member to obtain the group key. Based on the computational multilinear Diffe-Hellman assumption, we present two improved schemes to the ID-MAK protocol to remove this security defect. Both our improved protocols need only one round agreement. They support dynamic member change and key refresh. Our security analysis shows that they are secure.

Key words: multi-party key agreement; authentication; ID-base public keys; multilinear forms

1 引言

随着诸如视频会议,网络游戏等面向群组的应用的兴起,与之紧密相关的安全性便成为了人们关注的问题,组密钥协商协议是解决其安全问题的一个很重要的基本工具.

目前大多数组密钥协商协议都是基于多方 Diffie-Hellamn 密钥交换协议[1~4]以及 Weil 双线性对[5~7]. 最初组密钥协商协议为实现认证性通常采用 PKI 机制,为了解决该机制带来的证书认证需要的大量计算和存储空间,Boneh and Franklin[8]和 Cocks[9]分别提出了基于身份的加密体制,接着文献[6]和[10]在双线性 DH 问题假设下提出了基于身份的认证三方密钥协商协议.

2002 年,Boneh 和 Silverberg 提出了多线性表的概念,并利用此概念提出了一轮多方 D-H 密钥交换协议[11],然而由于该协议缺乏对参与者的身份认证,因此容易遭受中间人攻击. 文献[12]克服了该问题,并提出了 MAK 协议,该协议将 MTI 协议[14]和 MQV 协议[15]扩展到多线性表的应用中来,然而它需要结合证书提供对参与者的身份认证. 文献[13]在此基础上提出 ID-MAK

收稿日期:2007-05-28;修回日期:2008-07-23
基金项目:现代通信国家重点实验室基金(No. 9140C1107010604);华为公司科技基金(No. YJCB2006053DC);计算机网络与信息安全教育部重点实验室基金

协议,旨在通过引入基于身份的公钥密码体制来撤消对数字证书的使用,以及提供隐、显式密钥认证,然而该协议并未达到预期的目的,它仍存在明显不足.本文对其缺陷进行分析后,在多线性 D-H 问题假设下提出了两个基于身份的组密钥协商协议,并给出了对应的成员动态变化和组密钥更新的相关协议,弥补了 ID-MAK 协议的不足,同时对协议进行了安全性分析.

2 多线性表及难解假设

2.1 多线性表

Boneh 和 Silverberg 在文献[11]中提出了多线性表的概念,本文在此使用与该文献相同的定义.如果映射 $e_n: G_1^n \rightarrow G_2$ 满足如下性质,那么我们说它是一个 n 线性映射:

(1) G_1 和 G_2 是阶同为素数 p 的有限循环群;

(2) 如果 $a_1, a_2, \cdots, a_n \in Z_p$,且 $x_1, x_2, \cdots, x_n \in G_1$,则有 $e_n(x_1^{a_1}, \cdots, x_n^{a_n}) = e_n(x_1, \cdots, x_n)^{a_1 \cdots a_n}$;

(3) 映射 e_n 是非退化的,如果它有下面的特性:即如果 $g \in G_1$ 是 G_1 的一个生成元,则 $e_n(g, \cdots, g)$ 是 G_2 的生成元.

2.2 计算多线性 D-H 假设(CMDH 假设)

计算多线性 D-H 问题(CMDH 问题):对于 n 线性映射 $e_n: G_1^n \rightarrow G_2$,给定 G_1 中的元素 $(g, g^{a_1}, \cdots, g^{a_{n+1}})$,其中 $a_1, \cdots, a_{n+1} \in Z_p$,计算 G_2 中的 $e_n(g, \cdots, g)^{a_1 \cdots a_{n+1}}$.

可计算多线性 D-H 假设(CMDH 假设):一般认为 CMDH 问题是难解的,也就是不存在多项式时间算法以不可忽略的优势在$\langle G_1, G_2, e_n\rangle$中求解出 CMDH 问题.

本文提出的协议的安全性正是基于 CMDH 假设.

3 ID-MAK 协议及其缺陷

本文首先回顾 ID-MAK 协议[13],然后指出该协议的缺陷,并详细分析缺陷存在的原因.

3.1 ID-MAK 协议

初始化阶段:设 G_1 和 G_2 是阶同为素数 p 的有限循环群,g 是 G_1 的生成元,$e_{n-1}: G_1^{n-1} \rightarrow G_2$ 为 $n-1$ 线性映射.令 $V: G_2 \rightarrow \{0,1\}^*$ 和 $H: \{0,1\}^* \rightarrow G_1$ 表示哈希函数.组成员分别用 $A_1, \cdots, A_n$ 来表示,其中任意成员 A_i 的身份为 ID_i.假设存在一个离线的密钥生成中心(KGC),它负责产生系统参数并根据组成员的身份为其产生私钥.KGC 在$[1, p-1]$中随机选择一个私钥 s,计算 $P_{KGC} = g^s$ 并公布(g, P_{KGC}).组成员 A_i 的公/私钥对 (Q_{A_i}, S_{A_i}) 由 KGC 计算得出,其中 $Q_{A_i} = H(ID_{A_i})$,$S_{A_i} = Q_{A_i}^s$.

密钥协商阶段:每个参与者随机选取 $k_i \in [1, p-1]$,并执行如下计算:

(1) ID-MAK-1 协议:

①成员 A_i 计算并广播 $g^{k_i S_{A_i}} \in G_1$ 给网络内其它成员;

②成员 A_i 收到其他成员发来的消息后,计算密钥如下:

$$K_{A_i} = e_{n-1}(g^{k_1 S_1}, \cdots, g^{k_{i-1} S_{i-1}}, g^{k_{i+1} S_{i+1}}, \cdots, g^{k_n S_n})^{k_i S_i} = e_{n-1}(g, g \cdots, g)^{k_1 \cdots k_n S_1 \cdots S_n}.$$

(2) ID-MAK-2 协议:

①成员 A_i 计算并广播 $P_{KGC}^{k_i} \in G_1$ 给网络内其它成员;

②成员 A_i 收到其他成员发来的消息后,计算密钥如下:

$$K_{A_i} = e_{n-1}(S_{A_i}, g, \cdots, g)^{k_i} \cdot \prod_{j=1, j \neq i}^{n} e_{n-1}(Q_{A_j}, P_{KGC}^{k_j}, g, \cdots, g) = \prod_{i=1}^{n} e_{n-1}(Q_{A_i}, g, \cdots, g)^{k_i s}.$$

(3) ID-MAK-3 协议:

①成员 A_i 计算并广播 g^{k_i}、$g^{S_{A_i}} \in G_1$ 给网络内其它成员;

②成员 A_i 收到其他成员发来的消息后,计算密钥如下:

$$K_{A_i} = e_{n-1}\left(g^{k_1 + H(g^{k_1} \| g^{S_{A_1}}) \cdot S_{A_1}}, \cdots, g^{k_{i-1} + H(g^{k_{i-1}} \| g^{S_{A_{i-1}}}) \cdot S_{A_{i-1}}}, g^{k_{i+1} + H(g^{k_{i+1}} \| g^{S_{A_{i+1}}}) \cdot S_{A_{i+1}}}, \cdots, g^{k_n + H(g^{k_n} \| g^{S_{A_n}}) \cdot S_{A_n}}\right)^{k_i + H(g^{k_i} \| g^{S_{A_i}}) \cdot S_{A_i}}$$
$$= e_{n-1}(g, \cdots, g)^{(k_1 + H(g^{k_1} \| g^{S_{A_1}}) \cdot S_{A_1}) \cdots (k_n + H(g^{k_n} \| g^{S_{A_n}}) \cdot S_{A_n})}。$$

因此所有成员可以得到共享密钥 $V(K)$.

3.2 协议缺陷

ID-MAK 协议虽然能共享会话密钥并能抵抗被动攻击,但是它并没有象文献[13]所描述的实现在真正的身份认证,不能抵抗主动攻击.

对于 ID-MAK-1 和 ID-MAK-3 协议,攻击者只需获得任意成员 A_i 的身份 Q_{A_i},便可以冒充 A_i 参与到密钥协商过程中来.M 随机选取任意 $S_M \in [1, p-1]$作为长期私钥,以及 $k_M \in [1, p-1]$作为临时私钥,然后计算并广播 $g^{k_M S_M} \in G_1$ 给网络内其它成员(ID-MAK-3 协议中 M 计算 g^{k_M}、$g^{S_M} \in G_1$),M 收到其它成员发来的消息后可计算得出组密钥为 $K_M = e_{n-1}(g, g \cdots, g)^{k_1 \cdots k_M \cdots k_n \cdot S_1 \cdots S_M \cdots S_n}$(ID-MAK-3 协议中 M 计算得出组密钥为 $K_M = e_{n-1}(g, \cdots, g)^{(k_1 + H(g^{k_1} \| g^{S_{A_1}}) \cdot S_{A_1}) \cdots (k_M + H(g^{k_M} \| g^{S_M}) \cdot S_M) \cdots (k_n + H(g^{k_n} \| g^{S_{A_n}}) \cdot S_{A_n})}$).$M$ 之所以可以如此轻易的冒充 A_i 实施攻击,是因为在最终计算得出的组共享密钥中并未验证攻击者 M 是否知道与身份 Q_i 相对应的长期密钥 S_i.

对于 ID-MAK-2 协议,攻击者同样只需获得任意成员 A_i 的身份 Q_{A_i} 便可轻易冒充 A_i 参与密钥协商.M 随机

选取任意 $k_M \in [1, p-1]$作为临时私钥,然后计算并广播 $P_{KGC}^{k_M} \in G_1$ 给网络内其它成员. 尽管 M 不知道 S_{A_i}的值,但由于 $e_{n-1}(S_{A_i}, g, \cdots, g)^{k_M} = e_{n-1}(Q_{A_i}, g, \cdots, g)^{s \cdot k_M} = e_{n-1}(Q_{A_i}, g^s, \cdots, g)^{k_M} = e_{n-1}(Q_{A_i}, P_{KGC}, \cdots, g)^{k_M}$,因此 M 可计算得出组密钥为 $K_M = e_{n-1}(Q_i, P_{KGC}, \cdots, g)^{k_M} \cdot \prod_{j=1, j\neq i}^{n} e_{n-1}(Q_j, P_{KGC}^{k_i}, g, \cdots, g)$.

由上分析可知,ID-MAK 协议并未能实现对参与者的身份认证,攻击者 M 可以冒充网络中的任意成员参与到密钥协商过程中来. 攻击者在计算得到 K_M 后可以计算得到共享密钥 $V(K)$ 并顺利完成密钥确认过程.

4　新的协议

4.1　基本协议

本文提出的协议由两个阶段组成:初始化阶段和密钥协商阶段.

初始化阶段:设 G_1 和 G_2 是阶同为素数 p 的有限循环群, g 是 G_1 的生成元,设 m 为参与密钥协商的最大成员数量. 我们选择: $e_m: G_1^m \rightarrow G_2$ 为 m 线性映射. $V: G_2 \rightarrow \{0,1\}^*$ 和 $H: \{0,1\}^* \rightarrow G_1$ 表示哈希函数. 组成员分别用 $A_1, \cdots, A_n$ 来表示,其中 $n < m$. 密钥生成中心(KGC)在 $[1, p-1]$中随机选择一个私钥 s,计算 $P_{KGC} = g^s$ 并公布系统参数 (g, P_{KGC}). 每个组成员 A_i 都拥有系统产生的长期公/私钥对 (Q_i / S_i),其中 $Q_i = H(ID_i)$, $S_i = Q_i^s$,且 $Q_i \neq P_{KGC}$.

密钥协商阶段:每个参与者随机选取秘密指数 $k_i \in [1, p-1]$,并执行如下计算:

(1) 协议 1:

①成员 A_i 计算并广播 $g^{k_i} \in G_1$ 给网络内其它成员;

②成员 A_i 收到其他成员发来的消息后,计算密钥如下:

$$\begin{aligned} K_i &= e_m(Q_{i+1(\mathrm{mod}\ n)}^{k_i}, Q_1, \cdots, Q_{i-1}, Q_{i+2}, \cdots, Q_n, P_{KGC}, \cdots, P_{KGC}) \\ &\quad \cdot \prod_{j=1, j\neq i}^{n} e_m(S_i, {}_{j\text{遍取}1\sim n, \text{且} t\neq i, j} \cup Q_t, g^{k_i}, P_{KGC}, \cdots, P_{KGC}) \\ &= e_m(Q_{i+1(\mathrm{mod}\ n)}^{k_i}, Q_1, \cdots, Q_{i-1}, Q_{i+2}, \cdots, Q_n, g^s, \cdots, g^s) \\ &\quad \cdot \prod_{j=1, j\neq i}^{n} e_m(Q_i^s, {}_{j\text{遍取}1\sim n, \text{且} t\neq i, j} \cup Q_t, g^{k_j}, g^s, \cdots, g^s) \\ &= e_m(Q_{i+1(\mathrm{mod}\ n)}, Q_1, \cdots, Q_{i-1}, Q_{i+2}, \cdots, Q_n, g, \cdots, g)^{s^{m-n+1} \cdot k_i} \\ &\quad \cdot \prod_{j=1, j\neq i}^{n} e_m(Q_i, {}_{j\text{遍取}1\sim n, \text{且} t\neq i, j} \cup Q_t, g, \cdots, g)^{s^{m-n+1} \cdot k_j} \\ &= \prod_{i=1}^{n} e_m(Q_1, Q_2, \cdots, Q_{i-1}, Q_{i+1}, \cdots, Q_n, g, \cdots, g)^{s^{m-n+1} \cdot k_i} \end{aligned}$$

(2) 协议 2:

①成员 A_i 计算并广播 $Q_i^{k_i} \in G_1$ 给网络内其它成员;

②成员 A_i 收到其他成员发来的消息后,计算密钥如下:

$$\begin{aligned} K_i &= e_m(S_i^{k_i}, Q_1^{k_i}, \cdots, Q_{i-1}^{k_{i-1}}, Q_{i+1}^{k_{i+1}}, \cdots, Q_n^{k_n}, P_{KGC}, \cdots, P_{KGC}) \\ &= e_m(Q_1, Q_2, \cdots, Q_n, g, \cdots, g)^{s^{m-n+1} k_1 k_2 \cdots k_n} \end{aligned}$$

从而可以得到最终共享组密钥 $K = V(K_1) = V(K_2) = \cdots = V(K_n)$.

4.2　密钥确认

上述改善后的协议只能协商得到隐式认证的密钥,要建立显式认证的组密钥每个组成员 A_i 还需要执行密钥确认过程:

$$A_i \rightarrow A_j: M_{ij} = MAC_K(i, ID_1, \cdots, ID_n),\ j = 2, \cdots, n.$$

成员 A_j 在收到其他成员发来的信息后验证等式 $M_{ij} = MAC_K(i, ID_1, \cdots, ID_n)$ 是否成立,若对于所有 $i = 1, 2, \cdots, n$ 等式都成立,则说明组成员均获得了正确的共享组密钥值.

4.3　成员动态变化与组密钥更新

下面仅以单个成员为例进行说明,根据前面设定的网络规模 m,该网络在没有节点退出的情况下,最多只允许再有 $m-n$ 个成员加入,直到成员数达到 m.

(1) 成员加入

如果此前 n 个成员执行了协议 1,则当有新成员 A_{n+1}加入时,他向所有节点广播信息 $M' = \{Join\ Request, ID_{n+1}, g^{k_{n+1}}\}$;其中 *Join Request* 是指 A_{n+1}的加入请求(该加入请求需要经过 KGC 签名). 其他成员 A_i 在收到此消息后,将自己身份信息 ID_i 和 g^{k_i}发送给 A_{n+1},也可由指定的成员来发送所有成员的这些公开消息. 其中 k_i 与密钥协商阶段使用的相同,不需要重新选择. 这样所有成员在收到消息后,可以执行如下计算得到新的组密钥 K':

$$\begin{aligned} K' &= e_m(Q_{i+1(\mathrm{mod}\ n+1)}^{k_i}, Q_1, \cdots, Q_{i-1}, Q_{i+2}, \cdots, Q_{n+1}, P_{KGC}, \cdots, P_{KGC}) \\ &\quad \cdot \prod_{j=1, j\neq i}^{n+1} e_m(S_i, {}_{j\text{遍取}1\sim n+1, \text{且} t\neq i, j} \cup Q_t, g^{k_j}, P_{KGC}, \cdots, P_{KGC}) \\ &= \prod_{i=1}^{n+1} e_m(Q_1, \cdots, Q_{i-1}, Q_{i+1}, \cdots, Q_{n+1}, g, \cdots, g)^{s^{m-n} \cdot k_i} \end{aligned}$$

如果此前 n 个成员执行了协议 2,则当有新成员 A_{n+1}加入时,他向所有节点广播信息 $M' = \{Join\ Request, ID_{n+1}, Q_{n+1}^{k_{n+1}}\}$. 其他成员 A_i 在收到此消息后,将 ID_i 和 $Q_i^{k_i}$ 发送给 A_{n+1},其中 k_i 同样不需要重新选择. 这样所有成员可以执行如下计算得到新的组密钥 K':

$$\begin{aligned} K' &= e_m(S_i^{k_i}, Q_1^{k_1}, \cdots, Q_{i-1}^{k_{i-1}}, Q_{i+1}^{k_{i+1}}, \cdots, Q_{n+1}^{k_{n+1}}, P_{KGC}, \cdots \\ &\quad P_{KGC}) \\ &= e_m(Q_1, Q_2, \cdots, Q_{n+1}, g, \cdots, g)^{s^{m-n-1} k_1 k_2 \cdots k_{n+1}}。 \end{aligned}$$

(2) 成员退出

成员 A_n 退出时广播信息 $M'' = \{Quit\ Request, n, ID_n\}$,并用自己的私钥 S_n 对此消息进行签名. 其他成员 A_i 在收到此消息后,先用 A_n 的公钥 Q_n 验证此消息,验

证通过后执行下面的计算.

如果此前 n 个成员执行了协议 1,则 A_i 执行如下计算得到新的组密钥 K'':

$$K''=e_m(Q_{i+1(\mathrm{mod}\ n-1)}^{k_i},Q_1,\cdots,Q_{i-1},Q_{i+2},\cdots,Q_{n-1},P_{KGC},\cdots,P_{KGC})\cdot\prod_{j=1,j\neq i}^{n-1}e_m(S_i,\bigcup_{\text{遍取}1\sim n-1,\text{且}t\neq i,j}Q_t,g^{k_j},P_{KGC},\cdots,P_{KGC})$$
$$=\prod_{i=1}^{n-1}e_m(Q_1,\cdots,Q_{i-1},Q_{i+1},\cdots,Q_{n-1},g,\cdots,g)^{s^{m-n+1}\cdot k_i}$$

如果此前 n 个成员执行了协议 2,则 A_i 执行如下计算得到新的组密钥 K'':

$$K''=e_m(S_i^{k_i},Q_1^{k_1},\cdots,Q_{i-1}^{k_{i-1}},Q_{i+1}^{k_{i+1}},\cdots,Q_{n-1}^{k_{n-1}},P_{KGC},\cdots P_{KGC})$$
$$=e_m(Q_1,Q_2,\cdots,Q_{n-1},g,\cdots,g)^{s^{m-n+1}k_1k_2\cdots k_{n-1}}。$$

(3) 密钥更新

私钥的长期使用会增加私钥泄露的可能性,因此需要定期对各成员的临时公/私钥对和长期公/私钥对进行更新. 前者的更新操作可以通过指定的组成员来发起,该组成员在规定的时间间隔内向其他成员广播临时密钥更新信息,然后所有成员重新执行密钥协商协议即可;后者的更新操作由 KGC 发起,KGC 需要在更长的时间间隔内重新选择私钥 s',然后为所有组成员计算新的私钥 $S_i'=Q_i^{s'}$,并公布新的系统参数$(g,P'_{KGC}=g^{s'})$,所有成员根据新的公私钥对重新执行协议以获得新的组密钥.

5 协议安全性分析

下面用 $P_{initial}$ 表示我们的基本协议,P_{join} 表示成员加入协议,P_{leave} 表示成员退出协议. $P_{initial}$ 协议的安全性是基于 CMDH 假设的,通过协议协商得到的密钥不仅能够提供安全保密性和隐式密钥认证性,而且 P_{join}、P_{leave} 还能够分别实现前、后向安全性,另外协议可以检测出是否存在非组内成员的欺骗行为. 下面逐一分析.

安全保密性:由于任意 $Q_i\neq P_{KGC}$,即 $S_i\neq P_{KGC}^s$,因此对于协议 1 而言,只有两种情况下可以计算出共享密钥:一是拥有所有成员的秘密指数 $k_i(i\in[1,n])$,二是拥有任一成员的秘密指数值 k_i 和长期私钥信息 S_i;而对于协议 2 而言,只有拥有任一成员的秘密指数值 k_i 和长期私钥信息 S_i 才能求出共享密钥. 由此可知,任意非组内成员均无法获得上述信息,因此协议 1 和协议 2 均可以实现组密钥的安全保密性.

隐式密钥认证性:对于协议 1,在敌手不能获得所有成员的秘密指数 $k_i(i\in[1,n])$ 的情况下,由于需要使用长期私钥信息 S_i,故可实现隐式密钥认证;对于协议 2,成员必须使用长期私钥信息 S_i 才能够获得组密钥的值,因而可以实现隐式密钥认证. 如果协议运行得到共享组密钥后执行如上 4.2 节所示的密钥确认过程,则可实现显式密钥认证特性.

前、后向安全性:对于 P_{join} 协议,由于新加入的成员无法获得其他成员的秘密指数值 k_i 和长期私钥信息 S_i,因此新成员在加入组的前后所获得的关于旧的组密钥值的信息同样多,无法计算出旧的组密钥值,从而 P_{join} 协议实现了前向安全性;对于 P_{leave} 协议,新的组密钥信息中不包括离去成员的秘密值信息,因此离去后的成员也同样无法计算出新的组密钥值,从而 P_{leave} 协议实现了后向安全性. 另外,当协议参与者的长期私钥的泄漏后,由于成员会定期对秘密指数值进行更新,敌手无法计算出秘密指数值更新前协商得到的密钥.

欺骗行为检测:由于每个成员在获得组成员身份信息后,在计算密钥时将所有成员的长期公钥信息和秘密指数值都包含到密钥中来,因此如果有敌手冒充合法成员参与到协议中来,由于他不具有 k_i 和 S_i 的值,从而无法获得组密钥值,这样在密钥确认阶段就能检测出是否存在欺骗行为,并可以确定出是哪个成员被敌手冒充.

6 结束语

本文在分析 ID-MAK 协议存在的安全缺陷后,在多线性 D-H 问题假设下提出了改进的基于身份的组密钥协商协议,以及成员动态变化及组密钥更新的相关协议,并对协议的安全性进行了分析. 可以看出本文提出的协议解决了文献[13]存在的安全问题,同时成员只需要执行一轮消息交换即可.

作者简介:

钟 欢 男,1982 年生于广东梅州,电子科技大学计算机学院硕士研究生,主要研究方向为密码学.

许春香 女,1965 年生于湖南长沙,博士,电子科技大学计算机学院教授,博士生导师,主要研究方向为密码学.

E-mail:chxxu@uestc.edu.cn

参考文献:

[1] Steiner M, Tsudik G, Waidner M. Key agreement in dynamic peer groups [J]. IEEE Transactions on Parallel and Distribution System, 2000, 11(8): 769 - 780.

[2] Burmester M, Desmedt Y. A secure and efficient conference key distribution system[A]. In Advance in Cryptology EUROCRYPT'94[C]. Berlin: Springer-Verlag, 1994. 275 - 286.

[3] Becker K, Wille U. Communication complexity of group key distribution[A]. In ACM conference on Computer and Communication Security[C]. New York: ACM Press, 1998. 1 - 6.

(下转第 1890 页)

decentralized administration model for enterprise wide access control[J]. ACM Transactions on Information and System Security, 2005, 8(4): 388 - 423.

[19] S Oh, R Sandhu, X Zhang. An effective role administration model using organization structure[J]. ACM Transactions on Information and System Security, 2006, 9(2): 113 - 137.

[20] J Crampton. Understanding and developing role-based administrative models[A]. Proceedings of the 12th ACM Conference on Computer and Communications Security[C]. Alexandria, VA, USA: ACM Press, 2005. 158 - 167.

[21] Q Li, J Shi, S Qing. An administration model of DRBAC on the web[A]. Proceedings of the IEEE International Conference on e-Business Engineering[C]. Beijing, China: IEEE Computer Society, 2005. 364 - 367.

作者简介:

李凤华 男,1966 年 3 月出生于湖北省浠水县,西安电子科技大学博士生,北京电子科技学院教授,主要研究方向为网络安全与可信计算. E-mail: lfh@besti.edu.cn

王 巍 男,1980 年 2 月出生于河北省张家口市,西安电子科技大学博士生,主要研究方向为群组密钥管理、协议形式化证明.
E-mail: wei_wang@mail.xidian.edu.cn

马建峰 男,1963 年 10 月出生于陕西省西安市,西安电子科技大学计算机学院院长、博士、教授、博士生导师,主要研究方向为密码学与网络安全. E-mail: jfma@mail.xidian.edu.cn

梁晓艳 女,1985 年 4 月出生于湖南省益阳市,西安电子科技大学硕士生,主要研究方向为网络安全.

(上接第 1872 页)

[4] Ateniese G, Steiner M, Tsudik G. New multiparty authentication services and key agreement protocols[J]. IEEE Journal on Selected Areas in Communications, 2000, 18(4): 628 - 640.

[5] Boneh D, Franklin M. Identity-based Encryption from the weil Pairing[A]. In Proceedings of Crypto'2001[C]. Berlin: Springer-Verlag, 2001. 213 - 229.

[6] Joux A. One round protocol for tripartite Diffie-Hellman[A]. Proceedings of Algorithmic Number Theory Symposium[C]. Berlin: Springer-Verlag, 2000. 385 - 394.

[7] Smart N P. An Identity based authenticated Key Agreement protocol based on the Weil Pairing. Cryptography [R/OL]. eprint Archive, http://eprint.iacr.org/2001/111.

[8] Boneh D, Franklin M. Identity-based encryption from the Weil Pairing[A]. Advances in Cryptography-CRYPTO 2001[C]. Berlin: Springer-Verlag, 2001: 213 - 229.

[9] Cocks C. An Identity based encryption scheme based on quadratic residues[A]. Advances in Cryptography and Coding[C]. Berlin: Springer-Verlag, 2001. 360 - 363.

[10] Sattam S, Kenneth A. Parterson G. Authenticated Three Party Key Agreement Protocols from Pairings[OL]. http://eprint.iacr.org/2002/035.

[11] Boneh D, Silverberg A. Application of Multilinear forms to Cryptography[OL]. http://eprint.iacr.org/2002/080.

[12] H K Lee, H S Lee, Y R Lee. Multi-party Authenticated Key Agreement Protocols from Multilinear Forms[R/OL]. Cryptology ePrint Archive: http://eprint.iacr.org/2002/166.

[13] H M Lee, K J Ha, K M Ku. ID-based Multi-party Authenticated Key Agreement Protocols from Multilinear Forms[A]. Information Security, 8th International Conference, ISC 2005[C]. Berlin: Springer-Verlag, 2005. 104 - 117.