*

基于身份的移动网动态可认证群组密钥协商协议

曹　帅，　张串绒，　宋程远
(空军工程大学电讯工程学院,陕西　西安　710077)

摘要　群组密钥协商是保证无线网络群组安全通信的重要工具之一。2007 年,Tseng 等提出一种适合无线移动网络的高效群组密钥协商协议。对 Tseng 协议安全性进行分析,发现 Tseng 协议不具备认证性,不能抵御主动攻击。因此,通过改进 Tseng 协议,提出一种新的动态可认证群组密钥协商协议。该协议基于身份的公钥密码体制,降低了建立和管理公钥基础设施的代价;同时,协议支持节点间的相互认证。分析结果表明:协议满足群组密钥所要求的安全准则,降低了普通节点的计算和通信成本。

关键词　群组密钥协商;基于身份的公钥密码体制;认证;双线性对
DOI　10.3969/j.issn.1009－3516.2011.05.014
中图分类号　TN918.1　　**文献标识码**　A　　**文章编号**　1009－3516(2011)05－0067－05

随着诸如视频会议等面向群组的应用在无线移动网络中的兴起,与之紧密相关的安全性便成为了人们关注的热点问题。群组密钥协商协议是解决其安全问题的一个很重要的工具。近年来许多应用于无线移动网络环境的群组密钥协商协议相继提出。文献[1－4]分别给出了成员静态和动态下的群组密钥协商方案,文献[5－7]给出了基于身份的群组密钥协商方案。但以上群组密钥协商方案都是针对一般对等群组的,它们不适合迅速发展的无线移动网络,因为在现在的无线移动网络中,尤其是军事战术无线移动网络,用户的处理能力千差万别,节点处理能力有高有低。Boyd 等[8]在这种网络环境下提出了一种较高效率的群组密钥协商协议,而且在随机预言模型下被证明是安全的,但是当用户的长期私钥泄露时,该方案不提供完善前向安全性。张串绒等[9]将签密技术应用到密钥协商方案中,提高了协议的效率和安全性。Tseng 等[10]基于计算离散对数难题提出了一种高效的群组密钥协商方案,该方案在被动攻击下是安全的。但是该方案不能抵御主动攻击,敌手可以冒充任意合法成员参与到密钥协商中获取群组密钥。本文基于身份的公钥密码体制改进 Tseng 协议,提出一种更加安全高效的可认证群组密钥协商协议,并给出了成员动态变化的相关协议。

1　双线性对

令 G_1 为由 p 生成的循环加法群,阶为 q,G_2 是具有相同阶 q 的循环乘法群,双线性对是指满足下列性质的一个映射 $e:G_1\times G_1\rightarrow G_2$:

1)双线性:对所有的 $P,Q\in G_1$,$e(aP,bQ)=e(P,Q)^{ab}$。

2)非退化性:存在 $P,Q\in G_1$,使 $e(P,Q)\neq 1$。

3)可计算性:对所有的 $P,Q\in G_1$,存在有效的算法计算 $e(P,Q)$。

本方案依赖以下难题假设:

定义 1　(Bilinear Discrete Logarithm Problem,记为 BDLP 问题):给定 2 个元素 $P\in G_1$ 和 $Q\in G_1$,计算 a

* **收稿日期**:2010－12－30
基金项目:国家自然科学基金资助项目(60873233)
作者简介:曹　帅(1987－),男,甘肃平凉人,硕士生,主要从事密码学与信息安全研究.
E－mail: shuaics187@163.com

$\in Z_q^*$,使其 $Q = aP$ 成立。

定义 2 (Bilinear Computational Diffie – Hellman Problem,记为 BCDHP 问题):给定 aP, bP,计算 abP,其中 $a, b \in Z_q^*$。

一般认为不存在多项式时间算法以不可忽略的优势来求解出 BDLP 和 BCDHP 问题。而且,椭圆曲线上的双线性对可以使用较短的密钥达到同等的安全强度,例如在同等安全前提下,160 bit 的椭圆曲线密码相当于 1 024 bit 的 RSA。

2 Tseng 群组密钥协商协议及其安全缺陷

2.1 Tseng 协议

参数设置:p, q 是 2 个大素数,其中 $p = 2q + 1$,g 是有限域 Z_p^* 上的生成元。U_i 为节点的唯一身份标识,$\{U_i, \cdots, U_{n-1}\}$ 为处理能力弱的普通节点,U_n 为处理能力较强,且在其一跳步通信范围内集中了大多数普通节点的中心节点。

步骤 1 每一个节点 $U_i (1 \leqslant i \leqslant n-1)$ 选择一个随机数 $r_i \in Z_q^*$ 并且计算 r_i^{-1} 和 $z_i = g^{r_i} \bmod p$,发送 (U_i, z_i) 给中心节点 U_n。这里的 r_i^{-1} 和 z_i 可以离线预计算,并存放在他们自己的存储卡中以节约计算资源。

步骤 2 收到每一个用户的 $(U_i, z_i) (1 \leqslant i \leqslant n-1)$ 之后,U_n 选择一个随机数 $r_n \in Z_q^*$,计算 $z_n = g^{r_n} \bmod p$ 和 $x_i = z_i^{r_n} \bmod p$。U_n 能计算得到组密钥 $K = z_n \prod_{i=1}^{n-1} x_i \bmod p$,并广播 $(U_n, x_1, x_2, \cdots, x_{n-1})$ 给其他的用户。

组密钥的生成:每个 U_i 收到广播消息后,计算组密钥 $K = z_n \prod_{i=1}^{n-1} x_i \bmod p = g^{r_n + r_1 r_n + r_2 r_n + \cdots + r_{n-1} r_n} \bmod p$。

2.2 Tseng 协议的安全缺陷

容易看到,在 Tseng 协议**步骤** 2 中,节点 U_n 无法确信收到的消息 (U_i, z_i) 是由合法节点 U_i 发送的。攻击者只需获得节点的身份标识 U_i,选择随机数 $r_i' \in Z_q^*$,计算 $r_i'^{-1}$ 和 $z'_i = g^{r'_i} \bmod p$。发送 (U_i, z'_i) 给节点 U_n,就可以冒充任意合法节点 U_i 参与到群组密钥协商中来获取群组密钥。同理在**步骤** 3 中,节点 U_i 也无法确信收到的消息是真正节点 U_n 发送的。因此,该协议不能提供节点身份认证,导致攻击者可以参与到密钥协商中获取群组密钥。

3 新的可认证群组密钥协商协议

3.1 初始化阶段

在该协议中,我们假定存在一个可信的密钥生成中心(Key Generation Center,KGC)。KGC 生成以下系统参数:G_1 是阶为 q 的循环加法群,G_2 是具有相同阶 q 的循环乘法群,双线性映射:$e: G_1 \times G_1 \to G_2$:$P, P_{\text{pub}} \in G_1$,随机选取 $s \in Z_q^*$ 作为系统的私钥,计算 $P_{\text{pub}} = sP$ 作为系统的公钥;安全的 Hash 函数:$H: \{0,1\}^* \to G_1$。公开系统参数 $\text{parmas} = \langle P, P_{\text{pub}}, e, q, G_1, G_2, H \rangle$。$\text{ID}_i$ 为节点的唯一身份标识,$Q_i = H(\text{ID}_i)$ 为节点的长期公钥,$s_i = sQ_i$ 为节点的长期私钥由 KGC 计算并从安全信道发送给节点。$\{U_1, U_2, \cdots, U_n\}$ 表示网络中的群组成员,其中 $\{U_1, U_2, \cdots, U_{n-1}\}$ 为处理能力较弱的普通节点,U_n 为处理能力较强的中心节点。

3.2 初始组密钥协商阶段

步骤 1 每一个节点 $U_i (1 \leqslant i \leqslant n-1)$ 选择一个随机数 $a_i \in Z_q^*$,并计算 a_i^{-1}, s_i^{-1} 和 $A_i = a_i P, V_i = s_i A_i$,将 (ID_i, A_i, V_i) 发送给 U_n,每个节点 $U_i (1 \leqslant i \leqslant n-1)$ 都可以在离线的状态下计算 $(a_i^{-1}, s_i^{-1} A_i, V_i)$ 并且存储在自己的存储卡中以节省计算资源。

步骤 2 接收到每个普通节点 U_i 发送过来的消息 (ID_i, A_i, V_i) 之后,U_n 首先验证等式 $e(V_i, P) = e(Q_i A_i, P_{\text{pub}})$ 是否成立,若等式成立,则 U_n 能够确信 (ID_i, A_i, V_i) 由合法的 U_i 发送。然后,U_n 随机选择 $a_n \in Z_q^*$,计算 $x_i = a_n s_n V_i, B = H(\text{ID}_n, x_1, x_2, \cdots, x_{n-1})$ 和 $V_n = s_n B$,广播 $(\text{ID}_n, x_1, x_2, \cdots, x_{n-1}, V_n)$ 给所有的节点。并计算群组

密钥 $K = e\left(a_n s_n P, \sum_{i=1}^{n-1} x_i\right)$。

组密钥生成:收到 U_n 的广播数据之后,每一个 U_i 先计算 $B = H(\mathrm{ID}_n, x_1, x_2, \cdots, x_{n-1})$,并验证等式 $e(V_n, P) = e(Q_n B, P_{\mathrm{pub}})$ 是否成立,若等式成立,则每一个 U_i 可以确定 $(\mathrm{ID}_n, x_1, x_2, \cdots, x_{n-1}, V_n)$ 是由合法的 U_n 发送的。之后 U_i 能够计算出群组密钥 $K = e\left(x_i a_i^{-1} s_i^{-1}, \sum_{i=1}^{n-1} x_i\right)$。

根据双线性对的性质可知,中心节点 U_n 和普通节点 U_i 所计算得到的组密钥 $K = e\left(x_i a_i^{-1} s_i^{-1}, \sum_{i=1}^{n-1} x_i\right) = e\left(a_n s_n P, \sum_{i=1}^{n-1} x_i\right) = e(P,P)^{a_n^2 s_n^2 (a_1 s_1 + a_2 s_2 + \cdots + a_{n-1} s_{n-1} + a_{n+1} s_{n+1})}$ 是一致的。

3.3　成员动态变化

这里仅以单个节点为例进行说明。

3.3.1 节点的加入算法

1) 新节点 U_{n+1} 选择随机数 $a_{n+1} \in Z_q^*$,并计算 $a_{n+1}^{-1}, s_{n+1}^{-1}$ 和 $A_{n+1} = a_{n+1} P, V_{n+1} = s_{n+1} A_{n+1}$,广播一个加入请求消息,其中包含 $(\mathrm{ID}_{n+1}, A_{n+1}, V_{n+1})$。

2) U_n 接受到请求消息后首先验证消息是否是合法的 U_{n+1} 发送,若是,则计算 $x_{n+1} = a_n s_n V_{n+1}, B' = H(\mathrm{ID}_n, x_1, x_2, \cdots, x_{n-1}, x_{n+1})$ 和 $V_n = s_n B'$,并广播 $(\mathrm{ID}_n, x_1, x_2, \cdots, x_{n-1}, x_{n+1}, V_n)$,计算得到新的群组密钥 $K' = e\left(a_n s_n P, \sum_{\substack{i=1 \\ i \neq n}}^{n+1} x_i\right) = e(P,P)^{a_n^2 s_n^2 (a_1 s_1 + a_2 s_2 + \cdots + a_{n-1} s_{n-1} + a_{n+1} s_{n+1})}$。

3) 对于 $(U_1, U_2, \cdots, U_{n-1})$ 这些节点,U_n 可以用原组密钥 K 加密新组密钥 K' 安全组播给他们,也可以自己通过广播信息计算出新的群组密钥 $K' = e\left(x_i a_i^{-1} s_i^{-1}, \sum_{\substack{i=1 \\ i \neq n}}^{n+1} x_i\right) = e(P,P)^{a_n^2 s_n^2 (a_1 s_1 + a_2 s_2 + \cdots + a_{n-1} s_{n-1} + a_{n+1} s_{n+1})}$。

4) 对于新节点 U_{n+1},收到广播信息后计算 $B' = H(\mathrm{ID}_n, x_1, x_2, \cdots, x_{n-1}, x_{n+1})$,验证 $e(V_n, P) = e(Q_n B', P_{\mathrm{pub}})$ 等式是否成立,确定消息合法性后,计算新的群组密钥:

$$K' = e\left(x_{n+1} a_{n+1}^{-1} s_{i+1}^{-1}, \sum_{\substack{i=1 \\ i \neq n}}^{n+1} x_i\right) = e(P,P)^{a_n^2 s_n^2 (a_1 s_1 + a_2 s_2 + \cdots + a_{n-1} s_{n-1} + a_{n+1} s_{n+1})}$$

3.3.2 节点离开算法

节点的离开分为 2 种情况:

1) 中心节点 U_n 离开。当其它节点 U_i 接受到中心节点 U_n 的离开通知后,重新选择它们中计算能力较强和在其一跳步通信范围内覆盖大多数普通节点的用户为中心节点,假设为 U_d。然后,每一个用户重新选择随机数 a'_i,重新执行初始群组密钥协商协议来更新群组密钥。

2) 普通节点 U_j 离开。当收到节点 U_j 的离开通知后,中心节点 U_n 重新选择随机数 $a'_n \in Z_q^* \neq a_n$,计算 $x'_i = a'_n V_i, (i \neq j), B' = H(\mathrm{ID}_n, x'_1, x'_2, \cdots, x'_{j-1}, x'_{j+1}, \cdots, x'_{n-1})$ 和 $V_n = s_n B_。$并广播 $(\mathrm{ID}_n, x'_1, x'_2, \cdots, x'_{j-1}, x'_{j+1}, \cdots, x'_{n-1}, V_n)$,计算 $K' = e\left(a'_n s_n P, \sum_{\substack{i=1 \\ i \neq j}}^{n-1} x'_i\right)$ 为新的群组密钥。其它节点 U_i 收到 U_n 的广播数据之后,首先计算 $B' = H(\mathrm{ID}_n, x'_1, x'_2, \cdots, x'_{j-1}, x'_{j+1}, \cdots, x'_{n-1})$,然后通过等式 $e(V_n, P) = e(Q_n B', P_{\mathrm{pub}})$ 验证消息来源的合法性后,能够计算得到新的群组密钥:

$$K' = e\left(x'_i a_i^{-1} s_i^{-1}, \sum_{\substack{i=1 \\ i \neq j}}^{n-1} x'_i\right) = e(P,P)^{a'^2_n s_n^2 (a_1 s_1 + a_2 s_2 + \cdots + a_{j-1} s_{j-1} + \cdots + a_{j+1} s_{j+1} + \cdots + a_{n-1} s_{n-1})}$$

4　协议分析

4.1　安全性分析

定理 1　本文的密钥协商协议是双向认证的。

证明:在初始密钥协商的3.2节**步骤**2中 U_n 通过计算等式 $e(V_i,P)=e(Q_iA_i,P_{pub})$ 是否成立来验证消息的来源,若是合法的节点 U_i 发送的消息就能通过验证,否则根据 BDLP 和 BCDHP 难题假设,很难成功找到一个合法的 s_i 来伪造 V_i 通过上述测试而欺骗到 U_n。因此在本文协议中,U_n 正确认证了节点($U_1,U_2,\cdots,U_{n-1}$)。同理,在协议的组密钥生成中 U_i 也可以认证收到的消息是不是合法节点 U_n 发送的。因此我们的协议是双向认证的。

1)密钥的保密性。在本方案中群组密钥 $K=e(P,P)^{a_n^2s_n^2(a_1s_1+a_2s_2+\cdots+a_{n-1}s_{n-1})}$。可以看出,组密钥是由群组中的所有节点协商得到,包含任意节点的临时秘密信息 a_i 和长期私钥 s_i。攻击者在仅知道公共信道传输的(U_i,A_i,V_i,x_i)和公共参数 parmas 的情况下,计算获得组密钥,就必须能够解决 BCDHP 和 BDLP 难题获得临时秘密信息 a_i 和节点的长期私钥 s_i,而一般认为这2个难题是无法在多项式时间内以不可忽略的概率求解。因此该协议实现了组密钥的保密性。

2)前后向安全性。对于加入协议,如果新加入节点想获取以前的组密钥,就必须知道其它节点的秘密随机数 a_i 和长期私钥 s_i。显然新加入节点无法从公共信道传输的信息中计算得到这2个秘密值,因此新加入节点无法计算出旧的组密钥,从而加入协议满足前向安全性;同理:对于离开协议,离去后的节点也同样无法计算出新的组密钥值,从而协议实现了后向安全性。

3)密钥的独立性。当节点加入群组或离开群组时,新的组密钥中都包含了随机生成的新信息,这就保证了更新后的新密钥和更新之前的密钥相互独立,即使节点的长期密钥丢失了,也不会引起旧组密钥的泄漏,即该协议提供了密钥独立性。

4.2 效率分析

本文选取两种基于身份的群组密钥协商协议和本文协议进行计算量,通信量,以及是否满足认证性比较。结果如表1所示,在总计算量中,我们未将节点预计算量和 Hash 运算包含在内。表1中 M 为椭圆曲线上的点乘运算;A 为椭圆曲线上的加法运算;P 为椭圆曲线上的对运算;R 为协议的轮数;C 为协议中的总计算量;B 为协议中的总消息数;AP 为协议是否提供认证性。

表1 本文提出的协议与已有的协议比较

Tab. 1 Comparisons among the ID base group key agreement protocols

Protocol	AP	R	C	B
Choi[5]	NO	2	$2nP+n^2M+nA$	$2n$
Tang[7]	YES	2	$3Np+(2n^2-2n)M+nA$	$2n$
Our	YES	2	$3(n-1)P+3(n-1)M+(n-1)^2A$	n

可以看出该协议比起其他2种基于身份的群组密钥协商协议的计算和通信消耗有所下降。而且该协议中大部分计算消耗都在处理能力较强的中心节点 U_n 上,普通节点的计算量只有3次对运算,2次点乘运算,$n-1$ 次椭圆曲线上的加法运算和1次 Hash 运算。

5 结束语

通过分析看出,本文协议具备双向认证性,解决了 Tseng 协议的安全缺陷;同时,能够抵御中间人等主动攻击,满足了群组密钥所要求的安全需求,降低了处理能力较弱节点的运行代价。对于节点处理能力差别大的无线移动网来说,我们的方案是实际可行的。给出协议的安全性证明和实验验证将是下一步的工作重点。

参考文献:

[1] Asokan N, Ginzboorg P. Key agreement in ad hoc networks[J]. Computer communication, 2000, 23(17): 1627-1637.

[2] Hwang M S, Yang W P. Conference key distribution protocols for digital mobile communication systems[J]. IEEE selected areas communication, 1995, 13: 416-420.

[3] Dutta R, Barua R. Provably secure constant round contributory group key agreement in dynamic setting[J]. IEEE trans on Information theory, 2008, 54(5): 2007-2025.

[4] KIM Y, Perrig A, Tsudik G. Tree based group key agreement[J]. ACM trans on information system security, 2004, 7(1):

60 – 96.

[5] Choi K Y, Hwang J Y, Lee D H. Efficient ID – based group key agreement with bilinear maps[C]//Proceeding of 2004 international workshop on practice and theory in public key cryptography(PKC04)(LNCS2947). Berlin: Springer – verlag, 2004: 130 – 144.

[6] 钟欢, 许春香, 基于身份的多方认证组密钥协商协议[J]. 电子学报,2008, 36(10): 1868 – 1872.
ZHANG Huan, XU Chunxiang. ID – based multi – party authenticated key agreement protocols using multilinear forms[J]. Acta electronica sinica, 2008, 36(10): 1868 – 1872. (in Chinese)

[7] Tang H, Zhu L, Zhang Z. Efficient ID – based two round authenticated group key agreement protocol[C]//WiCOM'08:4th international conference on wireless communication, networking and mobile computering. New York: IEEE press, 2008: 1 – 4.

[8] Boyd C, Nieto JMG. Round – optimal contributory conference key agreement[C]//Proceedings of public – key cryptography (LNCS2567). Berlin: Springer – verlag, 2003: 161 – 174.

[9] 张串绒,肖国镇. 基于签密技术的可认证密钥协商协议[J]. 空军工程大学学报:自然科学版,2006,7(6):65 – 68.
ZHANG Chuanrong, XIAO Guozhen. Sign – cryptic technique based on authenticated key agreement protocol[J]. Journal of air force engineering university:natural science edition,2006,7(6):65 – 68. (in Chinese)

[10] Tseng YM. A resource – constrained group key agreement protocol for imbalanced wireless networks[J]. Computer security, 2007, 26(4): 331 – 333.

(编辑:徐楠楠)

Identity – based Dynamic Authenticated Group Key Agreement Protocol for Mobile Networks

CAO Shuai ,ZHANG Chuan – rong,SONG Cheng – yuan
(Telecommunication Engineering Institute, Air Force Engineering University, Xi′an 710077, China)

Abstract:Group key agreement is one of the important means to ensure group secure communication for wireless networks. In 2007, Tseng et al. proposed an efficient group key agreement protocol in wireless mobile environment. In this paper, by analyzing the security of the Tseng's protocol, the authors have found that the Tseng's protocol is not an authenticated protocol and cannot resist active attacks. By improving the Tseng's protocol, the authors propose a new dynamic authenticated group key agreement protocol. Due to using ID – based public key, the expense of building and managing public key infrastructure is decreased, and the protocol supports mutual authentication between nodes. The analysis results show that this protocol can satisfy the security rules of group key, meanwhile, reduce the computation and communication cost of the ordinary nodes.

Key words:group key agreement protocol; ID – base public key; authentication; bilinear pairing