文章编号:1001-506X(2012)06-1258-08

基于身份的域间认证及密钥协商协议

庞辽军[1,2],徐银雨[2],裴庆祺[3],李慧贤[4],王育民[2]
(1. 西安电子科技大学生命科学技术学院,陕西 西安 710071;
2. 西安电子科技大学计算网络与信息安全教育部重点实验室,陕西 西安 710071;3. 西安电子科技大学通信工程学院,陕西 西安 710071;4. 西北工业大学 计算机学院,陕西 西安 710072)

摘 要:基于 Shamir 的秘密共享思想,提出了一种基于身份的域间认证及密钥协商协议。该协议要求域内节点共同参与共享密钥的生成,解决了现有的两方密钥协商方法用于域间认证,及密钥协商时不能保障代表节点可靠性和普通节点参与度的问题。协议的正确性和安全性分析说明,该协议不仅满足密钥协商的基本安全属性,而且还满足数据保密性、数据完整性、抵抗代表节点假冒和欺骗等安全性要求。与使用现有的两方密钥协商协议进行域间认证及密钥协商相比较,本协议具有更低的通信量和计算量,同时,提高了域内普通节点在密钥协商过程中的参与度。

关键词:域间认证;密钥协商;共享密钥
中图分类号:TP 309 **文献标志码**:A **DOI**:10.3969/j.issn.1001-506X.2012.06.32

Identity-based inter-domain authentication and key agreement protocol

PANG Liao-jun[1,2], XU Yin-yu[2], PEI Qing-qi[3], LI Hui-xian[4], WANG Yu-min[2]
(*1. School of Life Sciences and Technology, Xidian University, Xi'an 710071, China;*
2. Key Laboratory of Computer Network and Information Security, the Ministry of Education, Xidian University, Xi'an 710071, China;
3. School of Telecommunications Engineering, Xidian University, Xi'an 710071, China;
4. School of Computer Science and Technology, Northwestern Polytechnical University, Xi'an 710072, China)

Abstract: Derived from Shamir's secret sharing idea, an identity-based inter-domain authentication and key agreement protocol is proposed. The protocol requires all nodes of a domain to participate the generation of the shared key, thus two knotty problems that the reliability of the representative nodes of the domains cannot be guaranteed and the efficiency of key agreement is very low are solved when using the existing two-party key agreement protocols for inter-domain authentication and key agreement. The correctness and security analyses show that this protocol meets not only the basic security properties of the key agreement, but also data confidentiality, data integrity, resistance to impersonating the representative nodes and so on. Compared with the existing two-party key agreement protocols in inter-domain key agreement, the proposed protocol is less in communication and computation, and at the same time, it improves the participation of the common nodes of the domains in the process of key agreement.

Keywords: inter-domain authentication; key agreement; shared key

0 引 言

随着通信技术的快速发展,网络通信中的安全问题也不断出现,这些安全破坏给人们带来了不可估量的损失,所以在不安全的网络环境中实现安全通信就成为当前的迫切需求。密钥协商技术是实现开放网络中安全通信的关键技术之一,具有重要的基础性作用,已成为信息安全和密码学中应对安全问题的一个重要研究方向[1]。通过密钥协商协议,可在通信节点之间建立共享会话密钥。密钥协商协议的安全性要求每一个参与和使用共享会话密钥的用户对会

收稿日期:2011-06-20; **修回日期**:2012-01-09。
基金项目:国家自然科学基金(60803151, 60803150, 61103178);NSFC-广东联合基金重点项目(U0835004);高等学校博士学科点专项科研基金新教师基金(20096102120045)资助课题
作者简介:庞辽军(1978-),男,博士,副教授,主要研究方向为密码学、安全协议设计与分析。E-mail:ljpang@mail.xidian.edu.cn

话密钥的计算都有贡献[2]。两方认证密钥协商协议可以使双方确信彼此的真实身份，同时，协议协商结束之后使得想要进行通信的双方确信：它们共享了一个只有自己知道的秘密会话密钥，而且该密钥是新鲜的，不可能被预先计算。该秘密会话密钥可为此后的通信会话提供数据保密性和数据完整性等安全保护。

1976 年，文献[3]提出了第一个两方的密钥协商协议，其有效性是建立在计算离散对数很困难这一基础上的。随着研究的深入，出现了多种基于扩展的 Diffie-Hellman 问题的密钥交换协议[4]。1984 年，文献[5]提出了基于身份的公钥密码体制(identity-based public key cryptosystem，ID-PKC)概念，在 ID-PKC 中，终端用户的公钥是从其身份信息得到的，这一做法极大地降低了密码系统中密钥管理的复杂度[6]。2001 年，文献[7]提出了一个利用双线性对的真正意义上基于身份的加密 (identity-based encryption，IBE)方案。2002 年，文献[8]利用文献[7]基于身份加密方案的思想，设计了第一个利用双线性对的基于身份的认证密钥协商协议。此后，大量使用双线性对的基于身份认证密钥协商协议被许多学者陆续提出[1,8-10]。2003 年，文献[11]针对文献[8]方案的密钥托管问题给出了改进方案，并提出了效率更高的基于身份的两方认证密钥协商协议。2005 年，文献[6]又在文献[11]方案的基础上提出了更高效的协议。同年，文献[12]首次提出了基于模糊身份的加密体制，即基于属性的加密体制(attribute-based encryption，ABE)，用户的身份由一个属性集合给出，该集合中的属性可以是用户的基本信息，如姓名、年龄等，ABE 能够更加灵活地控制不同属性的用户对密文的解密权限。在此基础上，2009 年，文献[9－10]提出了一种基于属性的两方密钥交换协议，在随机预言模型中给出了完整的安全性证明，后来又在标准模型下对该协议进行了严格的安全性证明。在研究两方密钥协商协议的基础上以及网络通信中用户数目不断飙升的现实，我们将节点之间通信的物理网络转换为域与域之间通信的逻辑网络，所有域覆盖整个网络，将整个网络系统划分为一系列相邻的、内部成员地位平等的域单元，整个网络实现无缝通信[13]。基于域的通信[13]也是多基站安全广播、无缝切换的基本目标，如无线城域网(wireless metropolitan area network，WMAN)(IEEE802.16e)等。

研究发现对于不同域之间进行认证及协商共享密钥，采用现有的两方密钥协商协议只是在两个域的代表节点之间进行认证和协商，忽略了普通节点的参与，代表节点的可靠性得不到保障。这样，域内普通节点不参与协商，整个协商过程由代表节点“说了算”，这对于普通节点来说是很不公平的，容易导致代表节点欺骗普通节点的安全事件[13]。另外，如前文所述，由于只有域内节点真正参与密钥协商过程才能确保所协商的共享密钥的可靠性和新鲜性，采用两方密钥协商协议实现两个域中任意节点之间的认证和密钥协商，必然需要运行两个域中节点个数相乘次密钥协商协议，而且若有 N 个节点，每个节点就必须存储 $N-1$ 个共享密钥，这显然会降低系统整体效率，与网络分域管理的目标不符。为此，基于 Shamir 的秘密共享思想[14]，建立以域中代表节点为中心、普通节点共同参与的密钥协商机制。在整个认证和密钥协商过程中，不仅代表节点要参与，而且普通节点也必须实时参与整个过程。本文提出的基于身份的域间认证及密钥协商协议有效地克服了现有方法用于域间密钥协商时不能保障代表节点的可靠性和普通节点的参与度以及密钥协商效率低的问题。

1　背景知识

1.1　双线性映射

设 G_1 为阶数为 q 的加法群，G_2 为阶数同为 q 的乘法群，其中 q 为一个大素数，G_1、G_2 上的双线性映射 e：$G_1\times G_1\to G_2$ 满足以下性质：

(1) 双线性：$e(aP,bQ)=e(P,Q)^{ab}$，其中，$P,Q\in G_1$；$a,b\in N$；

(2) 非退化性：若 g 为 G_1 的生成元，则有 $e(g,g)\neq 1$；

(3) 可计算性：对于任意的 $P,Q\in G_1$，存在有效的概率多项式时间算法可以计算出 $e(P,Q)$。

1.2　Shamir 秘密共享方案

秘密共享[14]是指将一个密钥分解成 n 份，只有知道其中至少 $d(d\leqslant n)$份才能恢复出原来的秘密信息 K。下面介绍 Shamir 的基于 Lagrange 插值公式的密钥共享方案。

设 $GP(q)$是一个有限域，q 是素数且 $q>n$，现在将秘密信息 K 分成 n 份，交给 n 个人保管，且要使得其中任意 $d(d\leqslant n)$个或 d 个以上人合作才能恢复出原来的秘密信息 K，任取 $a_1,a_2,\cdots,a_{d-1}\in GP(q)$ 构造一个多项式：$f(x)=K+a_1x+a_2x^2+\cdots+a_{d-1}x^{d-1}$，其中 K 为密钥。

令 g 是 $GP(q)$域的本原元素，作 $k_i=f(g^i)$ $(i=1,2,\cdots,n)$，称 $k_i(i=1,2,\cdots,n)$为子密钥，将 k_i 及各自的序号 1，2，…，n 分别交给分享者 $S_i(i=1,2,\cdots,n)$。若有 d 个分享者想恢复秘密信息 K，则利用 Lagrange 插值公式：

$$h(x)=\sum_{i=1}^{d}k_i\prod_{\substack{j=1\\ j\neq i}}^{d}\frac{(x-g^j)}{(g^i-g^j)} \tag{1}$$

将 Lagrange 插值系数记为 $\Delta_{i,s}(x)$，即 $\Delta_{i,s}(x)=\prod_{\substack{j=1\\ j\neq i}}^{d}\frac{(x-g^j)}{(g^i-g^j)}$，其中 S 为恢复秘密信息的秘密分享者集合，由式(2) 可得秘密信息 K。

$$K=h(0)=f(0) \tag{2}$$

1.3　判定性 Diffie-Hellman 假定

令 G 为阶数为素数 q 的有限循环群，生成元为 g，且 a、

$b\in Z_q^*$，$C\in G$。对于任意的概率多项式时间算法 F 均有：概率$|\Pr[F(q, g, g^a, g^b, C)=1]-\Pr[F(q, g, g^a, g^b, g^{ab})=1]|$可忽略。

1.4 协议基本安全目标

文献[15]中总结了一个安全的密钥协商协议应满足以下基本的安全属性：

(1) 已知密钥安全：当两个协议参与者之间共享的某个会话密钥泄露之后，要求获得该密钥的攻击者无法根据已获得的会话密钥求出其他会话密钥，每次协商的会话密钥具有唯一性。

(2) 完美前向保密安全：若两个协议参与者的长期私钥都泄露，攻击者不能由此求出它们在私钥泄露之前协商获得的会话密钥。

(3) 密钥生成中心(public key generator, PKG)前向保密安全：对于基于身份的密钥协商协议，若在某一时刻，PKG 的主密钥泄漏，获得该主密钥的攻击者仍然不能求出该 PKG 的用户之前协商获得的会话密钥。PKG 前向安全性同时意味着 PKG 不能被动地托管其用户之间协商达成的会话密钥。

(4) 抗未知共享密钥安全：实体 A 不会在不了解实体 B 身份的情况下，与实体 B 协商达成一个共享会话密钥。也就是说，当实体 A 与 B 之间协商达成一个共享会话密钥之后，要求 A 不会错误地认为该密钥是和另外某个实体 E 共享的。

(5) 抗密钥泄漏伪装攻击安全：假设攻击者获得了通信实体 A 的私钥，可以假冒 A 的身份与其他实体进行通信，但不能假冒其他实体与 A 进行通信。

(6) 无密钥控制安全：会话密钥的协商需要通信双方的共同参与，任何一方不能将正在协商的会话密钥的全部或部分设置成某个预先设定的参数。

2 方案介绍

本文提出的基于身份的域间认证及密钥协商协议解决了图 1 所示的两个域之间的认证与密钥协商问题。系统初始化时，由注册于同一个可信第三方(trusted third party, TTP)的节点所构成的每个域采用与传统单个节点向 TTP 注册的类似方式在 TTP 处进行域注册，并获取域内每个节点与该域相关的私钥。在注册过程中，每个域选举代表节点，并由代表节点代表所在域向 TTP 提交申请注册信息。在认证及密钥协商过程中，代表节点与其他域的代表节点进行交互，而普通节点必须实时参与整个密钥协商协议运行过程。只有得到一定数目普通节点的支持后，代表节点才能成功完成认证和密钥协商。

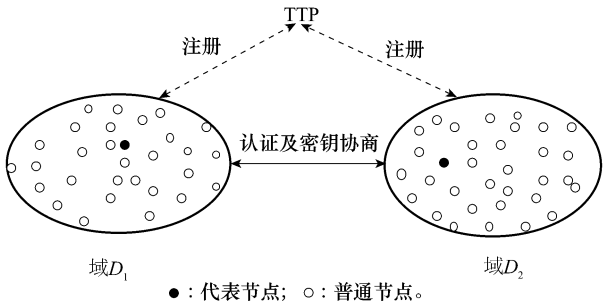

图 1 方案拓扑图

假设在每个域中选举代表节点时，每个普通节点和代表节点之间已经建立了共享密钥，即它们之间具有安全通道。在此基础上，本文提出的基于身份的域间认证及密钥协商协议的流程图如图 2 所示。具体步骤如下：

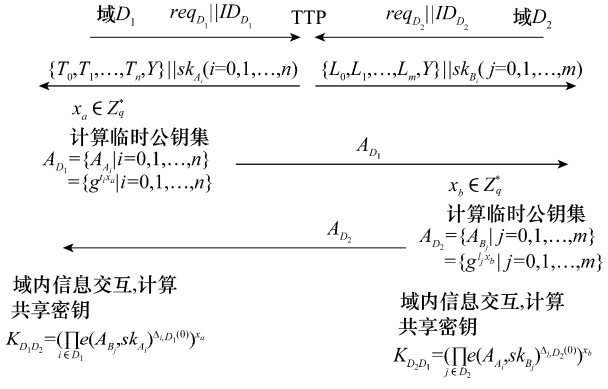

图 2 本协议的流程图

步骤 1 注册过程

(1) 域 D_1 中的所有节点向可信第三方 TTP 进行注册，具体步骤如下：

① 域 D_1 中的所有节点随机选取代表节点 A_0，然后 A_0 收集域 D_1 中所有节点的信息，构造密钥申请信息集合 req_{D_1} 和身份信息集合 ID_{D_1}，并发送消息 $req_{D_1}\parallel ID_{D_1}$ 给 TTP，其中“$\parallel$”为消息链接操作；

② TTP 收到域 D_1 发来的消息 $req_{D_1}\parallel ID_{D_1}$ 后，随机选取一组随机数 $t_0, t_1, \cdots, t_i, \cdots, t_n\in Z_q^*$ 和满足 $f_1(0)=y$ 的 $(d-1)$次(d 是一个整数，是预先设置的安全参数，满足 $d-1<n$)多项式 $f_1(x)$，并计算公开参数 $T_0=g^{t_0}$，$T_1=g^{t_1}$，$\cdots$，$T_i=g^{t_i}$，$\cdots$，$T_n=g^{t_n}$，$Y=e(g,g)^y$(y 是 TTP 的私钥)和各节点的私钥 $sk_{A_0}=g^{f_1(1)/t_0}$，$sk_{A_1}=g^{f_1(2)/t_1}$，$\cdots$，$sk_{A_i}=g^{f_1(i+1)/t_i}$，$\cdots$，$sk_{A_n}=g^{f_1(n+1)/t_n}$，然后通过安全信道发送消息 $\{T_0, T_1, \cdots, T_n, Y\}\parallel sk_{A_i}$ 给域 D_1 中对应的节点 $A_i(i=0,1,\cdots,n)$。

(2) 同理，域 D_2 中的所有节点向可信第三方 TTP 进行注册，具体步骤如下：

① 域 D_2 中的所有节点随机选举代表节点 B_0，然后 B_0

收集域 D_2 中所有节点的信息，构造密钥申请信息集合 req_{D_2} 和身份信息集合 ID_{D_2}，并发送消息 $req_{D_2} \| \mathrm{ID}_{D_2}$ 给 TTP；

② TTP 收到域 D_2 发来的信息 $req_{D_2} \| ID_{D_2}$ 后，随机选取一组随机数 $l_0, l_1, \cdots, l_j, \cdots, l_m \in Z_q^*$ 和满足 $f_2(0)=y$ 的 $(d-1)$ 次（d 是一个整数，是预先设置的安全参数，满足 $d-1<m$）多项式 $f_2(x)$，并计算公开参数 $L_0=g^{l_0}$，$L_1=g^{l_1}$，$\cdots$，$L_j=g^{l_j}$，$\cdots$，$L_m=g^{l_m}$，$Y=e(g,g)^y$（y 是 TTP 的私钥）和各节点的私钥 $sk_{B_0}=g^{f_2(1)/l_0}$，$sk_{B_1}=g^{f_2(2)/l_1}$，$\cdots$，$sk_{B_j}=g^{f_2(j+1)/l_j}$，$\cdots$，$sk_{B_m}=g^{f_2(m+1)/l_m}$，然后通过安全信道发送消息 $\{L_0, L_1, \cdots, L_m, Y\} \| sk_{B_j}$ 给域 D_2 中对应的节点 B_j（$j=0, 1, \cdots, m$）。

注：TTP 在参数设置时会比较两个域中的节点数。若 $n=m$，则令 $\{t_0, t_1, \cdots, t_i, \cdots, t_n\}=\{l_0, l_1, \cdots, l_j, \cdots, l_m\}$；若 $n>m$，则令 $\{l_0, l_1, \cdots, l_j, \cdots, l_m\} \subset \{t_0, t_1, \cdots, t_i, \cdots, t_n\}$；若 $n<m$，则令 $\{t_0, t_1, \cdots, t_i, \cdots, t_n\} \subset \{l_0, l_1, \cdots, l_j, \cdots, l_m\}$，故有不少于 d 个 $t_i=l_j$。

步骤 2　通信过程

域 D_1 中的代表节点 A_0 随机选取一个随机数 $x_a \in Z_q^*$，计算域 D_1 的临时公钥集 $A_{D_1}=\{A_{A_i} \mid i=0, 1, \cdots, n\}=\{T_i^{x_a} \mid i=0, 1, \cdots, n\}=\{g^{t_i x_a} \mid i=0, 1, \cdots, n\}$，然后将域 D_1 的临时公钥集 A_{D_1} 发送给域 D_2 中的代表节点 B_0。

同理，域 D_2 中的代表节点 B_0 随机选取一个随机数 $x_b \in Z_q^*$，计算域 D_2 的临时公钥集 $A_{D_2}=\{A_{B_j} \mid j=0, 1, \cdots, m\}=\{L_j^{x_b} \mid j=0, 1, \cdots, m\}=\{g^{l_j x_b} \mid j=0, 1, \cdots, m\}$，然后将域 D_2 的临时公钥集 A_{D_2} 发送给域 D_2 的代表节点 A_0。

步骤 3　计算过程

(1) 域 D_1 内代表节点与域内其他节点执行以下过程：

① 域 D_1 中的代表节点 A_0 收到域 D_2 中的代表节点 B_0 发来的临时公钥集 A_{D_2} 后，向域内其他节点广播临时公钥集 A_{D_2}；

② 域 D_1 内第 $i(i=1, 2, \cdots, n)$ 个节点 A_i 收到代表节点 A_0 发送的域 D_2 的临时公钥集 A_{D_2} 后，利用自己的私钥 sk_{A_i} 计算共享子密钥 $e(A_{B_j}, sk_{A_i})^{\Delta_{i,D_1}(0)}$，并从节点 A_i 与节点 A_0 的共享密钥 $K_{A_i \cdot A_0}$ 导出加密密钥 $KE_{A_{i,}A_0}$ 和完整性校验密钥 $KI_{A_{i,}A_0}$；

③ 节点 A_i 用加密密钥 $KE_{A_{i,}A_0}$ 加密共享子密钥 $e(A_{B_j}, sk_{A_i})^{\Delta_{i,D_1}(0)}$ 得到密文 $C_{KE_{A_{i,}A_0}}=E_{KE_{A_{i,}A_0}}(e(A_{B_j}, sk_{A_i})^{\Delta_{i,D_1}(0)})$，并用完整性校验密钥 $KI_{A_{i,}A_0}$ 计算消息 $C_{KE_{A_{i,}A_0}}$ 的完整性校验码 $MIC1_{A_i \cdot A_0}$，然后将消息 $C_{KE_{A_{i,}A_0}} \| MIC1_{A_i \cdot A_0}$ 发送给代表节点 A_0；

④ 代表节点 A_0 收到节点 A_i 发来的消息 $C_{KE_{A_{i,}A_0}} \| MIC1_{A_i \cdot A_0}$ 后，从节点 A_0 与节点 A_i 的共享密钥 $K_{A_0 \cdot A_i}$ 导出解密密钥 $KE_{A_0 A_i}$ 和完整性校验密钥 $KI_{A_0 A_i}$；

⑤ 代表节点 A_0 用完整性校验密钥 $KI_{A_0 A_i}$ 对接收到的消息 $C_{KE_{A_{i,}A_0}}$ 重新计算消息完整性校验码 $MIC1_{A_0 \cdot A_i}$，并比较接收到的消息完整性校验码 $MIC1_{A_i \cdot A_0}$ 和计算得到的 $MIC1_{A_0 \cdot A_i}$ 是否相等。如果不相等，则丢弃该消息；若相等，则用解密密钥 $KE_{A_0 \cdot A_i}$ 对密文信息 $C_{KE_{A_{i,}A_0}}$ 进行解密得到节点 A_i 计算的共享子密钥 $e(A_{B_j}, sk_{A_i})^{\Delta_{i,D_1}(0)}=D_{KE_{A_0 A_i}}(C_{KE_{A_{i,}A_0}})$；

⑥ 代表节点 A_0 收到域内各节点发来的消息成功获得 $(d-1)$ 个共享子密钥，并计算共享子密钥 $e(A_{B_0}, sk_{A_0})^{\Delta_{0,D_1}(0)}$，然后由这 d 个共享子密钥计算域 D_1 与域 D_2 的共享密钥，即 $K_{D_1 \cdot D_2}=(\prod_{i \in D_1} e(A_{B_j}, sk_{A_i})^{\Delta_{i,D_1}(0)})^{x_a}=(e(g,g))^{f_1(0)x_a x_b}=Y^{x_a x_b}$。

(2) 同理，域 D_2 内代表节点与域内其他节点执行以下过程：

① 域 D_2 中的代表节点 B_0 收到域 D_1 中的代表节点 A_0 发来的临时公钥集 A_{D_1} 后，向域内其他节点广播临时公钥集 A_{D_1}；

② 域 D_2 内第 $j(j=1, 2, \cdots, m)$ 个节点 B_j 收到代表节点 B_0 发送的域 D_1 的公钥集 A_{D_1} 后，利用自己的私钥 sk_{B_j} 计算共享子密钥 $e(A_{A_i}, sk_{B_j})^{\Delta_{j,D_2}(0)}$；并从节点 B_j 与节点 B_0 的共享密钥 $K_{B_j \cdot B_0}$ 导出加密密钥 $KE_{B_{j,}B_0}$ 和完整性校验密钥 $KI_{B_{j,}B_0}$；

③ 节点 B_j 用加密密钥 $KE_{B_j B_0}$ 加密共享子密钥 $e(A_{A_i}, sk_{B_j})^{\Delta_{j,D_2}(0)}$ 得到密文 $C_{KE_{B_j B_0}}=E_{KE_{B_{j,}B_0}}(e(A_{A_i}, sk_{B_j})^{\Delta_{j,D_2}(0)})$，并用完整性校验密钥 $KI_{B_j B_0}$ 计算消息 $C_{KE_{B_j B_0}}$ 的完整性校验码 $MIC1_{B_j B_0}$，然后将消息 $C_{KE_{B_j B_0}} \| MIC1_{B_j B_0}$ 发送给代表节点 B_0；

④ 代表节点 B_0 收到节点 B_j 发来的消息 $C_{KE_{B_{j,}B_0}} \| MIC1_{B_j \cdot B_0}$ 后，从节点 B_0 与节点 B_j 的共享密钥 $K_{B_0 \cdot B_j}$ 导出解密密钥 $KE_{B_0 \cdot B_j}$ 和完整性校验密钥 $KI_{B_0 \cdot B_j}$；

⑤ 代表节点 B_0 用完整性校验密钥 $KI_{B_0 \cdot B_j}$ 对接收到的消息 $C_{KE_{B_{j,}B_0}}$ 重新计算消息完整性校验码 $MIC1_{B_0 \cdot B_j}$，并比较接收到的消息完整性校验码 $MIC1_{B_j B_0}$ 和计算得到的 $MIC1_{B_0 \cdot B_j}$ 是否相等。如果不相等，则丢弃该消息；若相等，则用解密密钥 $KE_{B_0 \cdot B_j}$ 对密文信息 $C_{KE_{B_{j,}B_0}}$ 进行解密得到节点 B_j 计算的共享子密钥 $e(A_{A_i}, sk_{B_j})^{\Delta_{j,D_2}(0)}=D_{KE_{B_0 B_j}}(C_{KE_{B_{j,}B_0}})$；

⑥ 代表节点 B_0 收到域内节点发来的消息成功获得 $d-1$ 个共享子密钥，并计算共享子密钥 $e(A_{A_0}, sk_{B_0})^{\Delta_{0,D_2}(0)}$，然后由这 d 个共享子密钥计算域 D_1 与域 D_2 的共享密钥，即 $K_{D_2 \cdot D_1}=(\prod_{j \in D_2} e(A_{A_i}, sk_{B_j})^{\Delta_{j,D_2}(0)})^{x_b}=(e(g,g))^{f_2(0)x_a x_b}=Y^{x_a x_b}$。

步骤 4　域内共享密钥分发过程

(1) 域 D_1 的代表节点 A_0 计算获得域 D_1 与域 D_2 的共享密钥 $K_{D_1 \cdot D_2}$ 后，执行以下步骤：

① 域 D_1 的代表节点 A_0 利用与节点 $A_i(i=1,2,\cdots,n)$ 之间的共享密钥推导出的加密密钥 KE_{A_0,A_i} 加密共享密钥 K_{D_1,D_2} 得到密文消息 $C^*_{KE_{A_0,A_i}}=E_{KE_{A_0,A_i}}(K_{D_1,D_2})$，并用完整性校验密钥 KI_{A_0,A_i} 计算消息 $C^*_{KE_{A_0,A_i}}$ 的完整性校验码 $MIC2_{A_0,A_i}$，然后将消息 $C^*_{KE_{A_0,A_i}}\|MIC2_{A_0,A_i}$ 发送给域内的第 i 个节点 A_i；

② 域内节点 A_i 收到消息 $C^*_{KE_{A_0,A_i}}$ 后重新计算消息完整性校验码 $MIC2_{A_i,A_0}$，并比较接收到的消息完整性校验码 $MIC2_{A_0,A_i}$ 和计算得到的 $MIC2_{A_i,A_0}$ 是否相等。如果不相等，则丢弃该消息；若相等，则用节点 A_i 与代表节点 A_0 之间的共享密钥推导出的解密密钥 KE_{A_i,A_0} 解密 $C^*_{KE_{A_0,A_i}}$ 得到域 D_1 与域 D_2 的共享密钥 $K=K_{D_1,D_2}=D_{KE_{A_i,A_0}}(C_{KE_{A_0,A_i}})$。

(2) 同理，域 D_2 的代表节点 B_0 计算获得域 D_2 与域 D_1 的共享密钥 K_{D_2,D_1} 后，执行以下步骤：

① 代表节点 B_0 利用与节点 $B_j(j=1,2,\cdots,n)$ 之间的共享密钥推导出的加密密钥 KE_{B_0,B_j} 加密共享密钥 K_{D_2,D_1} 得到密文消息 $C^*_{KE_{B_0,B_j}}=E_{KE_{B_0,B_j}}(K_{D_2,D_1})$，并用完整性校验密钥 KI_{B_0,B_j} 计算消息 $C^*_{KE_{B_0,B_j}}$ 的完整性校验码 $MIC2_{B_0,B_j}$，然后将消息 $C^*_{KE_{B_0,B_j}}\|MIC2_{B_0,B_j}$ 发送给域内的第 j 个节点 B_j；

② 域内节点 B_j 收到消息 $C^*_{KE_{B_0,B_j}}$ 后重新计算消息完整性校验码 $MIC2_{B_j,B_0}$，并比较接收到的消息完整性检验码 $MIC2_{B_0,B_j}$ 和计算得到的 $MIC2_{B_j,B_0}$ 是否相等。如果不相等，则丢弃该消息；若相等，则用节点 B_j 与代表节点 B_0 之间的共享密钥推导出的解密密钥 KE_{B_j,B_0} 解密 $C^*_{KE_{B_0,B_j}}$ 得到域 D_1 与域 D_2 的共享密钥 $K=K_{D_2,D_1}=D_{KE_{B_j,B_0}}(C_{KE_{B_0,B_j}})$。

通过执行本协议，想要通信的域 D_1 与域 D_2 中的所有节点都获得了共享密钥 K。

步骤 5 共享密钥验证过程

(1) 域 D_1 中任意 d 个普通节点，例如 $A_i(i=1,2,\cdots,d)$，合作验证代表节点 A_0 分发的共享密钥过程如下：

① d 个普通节点中的任意一个节点计算：

$$Y^{x_b}=\prod_{i\in D_1}^{d}e(g^{l_jx_b},g^{f_1(i+1)/t_i})^{\Delta_{i,D_1}(0)}=$$

$$e(g,g)^{x_b\sum_{i\in D_1}^{d-1}f_1(i+1)\Delta_{i,D_1}(0)}=e(g,g)^{f_1(0)x_b}$$

② 节点 $A_i(i=1,2,\cdots,d)$ 通过安全信道向代表节点 A_0 索取临时私钥 x_a，验证等式 $K'\overset{?}{=}(Y^{x_b})^{x_a}$ 是否成立。若相等，则接受代表节点分发的共享密钥，否则说明域间密钥不正确，同时，向域内其他节点广播验证结果。

(2) 同理，域 D_2 中任意 d 个普通节点，例如 $B_j(j=1,2,\cdots,d)$，可以合作验证代表节点 B_0 分发的共享密钥：

① d 个普通节点中的任意一个节点计算：

$$Y^{x_a}=\prod_{j\in D_2}^{d}e(g^{t_ix_a},g^{f_2(j+1)/l_j})^{\Delta_{j,D_2}(0)}=$$

$$e(g,g)^{x_a\sum_{j\in D_2}^{d-1}f_2(j+1)\Delta_{j,D_2}(0)}=e(g,g)^{f_2(0)x_a}$$

② 节点 $B_j(j=1,2,\cdots,d)$ 通过安全信道向代表节点 B_0 索取临时私钥 x_b，验证等式 $K'\overset{?}{=}(Y^{x_a})^{x_b}$ 是否成立。若相等，则接受代表节点分发的共享密钥，否则说明域间密钥不正确，同时，向域内其他节点广播验证结果。

3 协议分析

3.1 正确性分析

根据注册过程及其附加说明可知，域 D_1 中第 $i(i=1,2,\cdots,n)$ 个节点 A_i(以域 D_1 为例)计算的子密钥为 $e(A_{B_j},sk_{A_i})^{\Delta_{i,D_1}(0)}=e(g^{l_jx_b},g^{f_1(i+1)/t_i})^{\Delta_{i,D_1}(0)}=e(g,g)^{l_jx_bf_1(i+1)/t_i\cdot\Delta_{i,D_1}(0)}=e(g,g)^{x_bf_1(i+1)\Delta_{i,D_1}(0)}$。

则域 D_1 的代表节点 A_0 利用来自域内节点的 $d-1$ 个子密钥和自己计算的子密钥计算域 D_1 与域 D_2 的共享密钥为

$$K_{D_1,D_2}=(\prod_{i\in D_i}e(A_{B_j},sk_{A_i})^{\Delta_{i,D_1}(0)})^{x_a}=$$

$$(\prod_{i\in D_i}e(g^{l_jx_b},g^{f_1(i+1)/t_i})^{\Delta_{i,D_1}(0)})^{x_a}=$$

$$(\prod_{i\in D_i}e(g,g)^{x_bf_1(i+1)\Delta_{i,D_1}(0)})^{x_a}=$$

$$e(g,g)^{x_b\sum_{i\in D_1}^{d-1}f_1(i+1)\Delta_{i,D_1}(0)x_a}=e(g,g)^{f_1(0)x_ax_b}=Y^{x_ax_b}$$

同理，域 D_2 的代表节点 B_0 利用来自域内节点的 $d-1$ 个子密钥和自己计算的子密钥计算域 D_2 与域 D_1 的共享密钥为

$$K_{D_2,D_1}=(\prod_{j\in D_2}e(A_{A_i},sk_{B_j})^{\Delta_{j,D_2}(0)})^{x_b}=$$

$$(\prod_{j\in D_2}e(g^{t_ix_a},g^{f_2(j+1)/l_j})^{\Delta_{j,D_2}(0)})^{x_b}=$$

$$(\prod_{j\in D_2}e(g,g)^{x_af_2(j+1)\Delta_{j,D_2}(0)})^{x_b}=$$

$$e(g,g)^{x_a\sum_{j\in D_2}^{d-1}f_2(j+1)\Delta_{j,D_2}(0)x_b}=(e(g,g))^{f_2(0)x_ax_b}=Y^{x_ax_b}$$

所以，域 D_1 与域 D_2 协商的共享密钥为：$K=K_{D_1,D_2}=K_{D_2,D_1}$。

3.2 安全性分析

3.2.1 安全模型

本文提出的协议安全性是基于下述的“敌手-挑战者”游戏定义的一种语义安全性[16]。在“敌手-挑战者”游戏中，敌手模拟了攻击者，通过敌手询问预言器来模拟攻击者的攻击能力。挑战者是一个理想实体，知道系统中所有的秘密和公开参数，同时还承担预言器的功能。该游戏包括以下几个阶段：

(1) 系统初始阶段。挑战者模拟系统可信第三方执行域 D_1 与域 D_2 之间的注册过程，并将生成的所有系统公开参数发给敌手。

(2) 敌手训练阶段一。域 D_1 和域 D_2 分别为系统中不同的合法节点集，敌手在该阶段中可以询问两个预言器：

Execute(D_1, D_2)、Corrupt(TTP)。当敌手询问 Execute(D_1, D_2)预言器时，挑战者执行一次域 D_1 和域 D_2 之间的密钥协商协议，并将所产生的临时公钥集发给敌手，该预言器模拟了攻击者具有窃听协议执行中所有交互信息的能力。当敌手询问 Corrupt(TTP)预言器时，挑战者将域 D_1 的代表节点的私钥发送给敌手，该预言器模拟了攻击者具有入侵某参与方并获取其长期秘密私钥的能力。

(3) 挑战阶段。一旦敌手认为训练阶段一结束，敌手向挑战者提交两个合法节点集域 D_1 和域 D_2，且敌手未询问过 Corrupt(D_1)和 Corrupt(D_2)。挑战者执行一次域 D_1 和域 D_2 之间的密钥协商协议得到密钥后将产生的交互信息发给敌手后，抛掷随机硬币 b，若 $b=1$，则发送该密钥给敌手；若 $b=0$，则随机选择 $r\in_R G_2$ 并发送 r 给敌手。

(4) 敌手训练阶段二。和敌手训练阶段一相同，并且要求敌手不能访问 Corrupt(D_1)和 Corrupt(D_2)。

(5) 攻击阶段。敌手输出对 b 的猜测 b'。若 $b=b'$，称敌手赢得该游戏；并称概率 $|\Pr(\text{敌手赢得该游戏})-1/2|$ 为敌手在游戏中的优势。

定义 1　如果任意的概率多项式时间敌手赢得上述游戏的优势均可忽略，则称该协议是安全的。

3.2.2　安全性证明

定理 1　本文提出的协议安全性是基于 DDH 假定的，如果 DDH 假定成立，则该协议是安全的。

证明　域 D_1 和域 D_2 的代表节点分别与域内普通节点之间拥有共享密钥，即它们之间具有安全通道，因此不考虑普通节点和代表节点之间的安全问题，它们之间的通信是安全可信的(参见 3.3.2 分析)，只考虑域外的安全性。这里采用反证法，假设存在概率多项式时间敌手能以不可忽略的优势 ε 赢得上述游戏，则可以构造概率多项式时间算法 F 能以不可忽略的概率解决 G_2 群上的 DDH 问题。

假设算法 F 收到四元组(g, g^a, g^b, C)，并要求判断 C 是否等于 g^{ab}，其中 g 为 G_1 的生成元。除以下三点改动外，算法 F 完全模拟一个挑战者并与敌手进行上述“敌手-攻击者”游戏：

(1) 在挑战阶段，当敌手向算法 F 提交两个合法节点集域 D_1 和域 D_2，算法 F 运行域 D_1 和域 D_2 之间的密钥协商协议时，算法 F 并不为 D_1 选取 Z_q^* 上的随机值 x_a，而是以 g^a 作为 g^{x_a}，并计算 $A_{D_1}=\{g^{t_i a}\mid i=0,1,\cdots,n\}$；同时算法 F 并不为 D_2 选取 Z_q^* 上的随机值 x_b，而是以 g^b 作为 g^{x_b}，并计算 $A_{D_2}=\{g^{t_j b}\mid j=0,1,\cdots,m\}$，然后将产生的交互信息发送给敌手，并抛掷随机硬币 b。

(2) 在挑战阶段，当算法 F 抛掷随机硬币 b 得到 $b=1$ 时，将 $e(g,C)^y$ 作为密钥发给敌手。

(3) 在攻击阶段，当算法 F 收到敌手对 b 的猜测 b'后，算法 F 根据如下规则执行：如果 $b=1$ 且 $b'=1$，算法 F 认为 $C=g^{ab}$；如果 $b=1$ 且 $b'=0$，算法 F 认为 $C\neq g^{ab}$；如果 $b=0$，则算法 F 以 1/2 概率认为 $C=g^{ab}$，以 1/2 概率认为 $C\neq g^{ab}$。

因为在挑战阶段，域 D_1 和域 D_2 在运行密钥协商协议时，两个域的代表节点选定的随机值 x_a 和 x_b 以及协商生成的共享密钥不对敌手公开，所以从敌手的角度而言，算法 F 完善地模拟了挑战者。另一方面，由于 $e(g,g^{ab})^y=e(g,g)^{aby}$，同时 $b=1$ 时算法 F 将 $e(g,C)^y$ 作为密钥发给敌手，所以敌手能够分辨正确的密钥和随机数，相当于能正确分辨 g^{ab} 和 C。因此如果敌手能以不可忽略的优势 ε 赢得上述游戏，那么算法 F 能以 $\varepsilon/2$ 的概率解决 G_2 群上的 DDH 问题。这与 DDH 问题的困难性相矛盾，故假设不成立，证明了本文提出的协议是安全的。　　证毕

3.3　安全目标分析

3.3.1 基本安全目标分析

本方案是基于判定性的 Diffie-Hellman 假定，以下分析该协议满足前文所述的密钥协商协议的基本安全目标。

(1) 已知密钥安全：该协议在密钥协商过程中使用了秘密随机参数 x_a 和 x_b，所以即使攻击者获得当前协商的共享密钥 K，也无法根据已获得的会话密钥求出其他会话密钥，且每次协商的会话密钥具有唯一性。

(2) 完美前向保密安全：若攻击者获得域 D_1 或域 D_2 的代表节点的长期私钥，由于域间共享密钥是由域内节点共同参与协商的，而且秘密参数 x_a 和 x_b 分别由域 D_1 和 D_2 的代表节点随机选取，因此，攻击者不能计算出域间协商的共享密钥。另外，TTP 的私钥是用来计算系统公开参数的，即使 TTP 的私钥被攻击者获得，也无法破解共享密钥，显然满足 TTP 前向安全，即本协议密钥托管安全。

(3) 抗未知共享密钥安全：想要进行通信的两个域 D_1 和 D_2 首先要向可信第三方注册，通过可信第三方的认证后，域内所有节点分别获得协商共享密钥所需的系统公开参数和其私钥，显然攻击者 E 要使域 D_1 确信它与 E 协商获得了一个共享密钥，E 就必须获得域 D_2 中至少 d 个(域中节点数目很庞大，d 一般设定的值很大)节点的私钥计算共享密钥，这对于 E 是困难的，很显然该协议也满足抗密钥泄漏伪装攻击安全。

(4) 无密钥控制安全：域 D_1 和域 D_2 之间的共享密钥协商需要域中节点共同参与，任何一方不能将正在协商的会话密钥的全部或部分设置成某个预先设定的参数。假设域 D_2 想要将共享密钥 K 设置为某个预先设定的参数 K'，那么域 D_2 的代表节点在收到域 D_1 的临时公钥集 $A_{D_1}=\{g^{t_i x_a}\mid i=0,1,\cdots,n\}$，并向域内节点广播后，就必须等待

收集域内节点计算的至少($d-1$)个共享子密钥,然后选择合适的随机数 $x_b' \in Z_q^*$ 使得($\prod_{j \in D_2} e(A_{A_i}, sk_{B_j})^{\Delta_{j,D_2}(0)})^{x_b'} = K'$后才能计算临时公钥集 $A_{D_2} = \{g^{x_j x_b'} \mid j=0,1,\cdots,m\}$ 发送给域 D_1 的代表节点,而域 D_1 的代表节点在发送出临时公钥集后会设置一个等待时间 t_{out},若在 t_{out} 时间内没有收到域 D_2 的临时公钥集,就终止本次协商。由于域内节点数目巨大且 t_{out} 一般设置的很短,域 D_2 想在极短的时间内完成收集和计算过程几乎是不可能的,随着网络中用户数目的不断增多,这会变得更困难。所以,本文提出的协议满足无密钥控制。

通过以上安全属性分析,可知本文提出的协议是满足密钥协商协议基本安全目标的。

3.3.2 其他安全目标

本文提出的域间认证及密钥协商方案,在协商密钥过程中还可提供:

(1) 数据保密性:在密钥协商过程中,域内代表节点与域内普通节点之间拥有共享密钥。以域 D_1 为例,代表节点与域内普通节点进行信息交互时,利用 hash 函数由共享密钥 $K_{A_i \cdot A_0}$(或 $K_{A_0 \cdot A_i}$)导出加/解密密钥 KE_{A_i, A_0}(或 $KE_{A_0 \cdot A_i}$)和完整性校验密钥 KI_{A_i, A_0}(或 $KI_{A_0 \cdot A_i}$),利用加/解密密钥 KE_{A_i, A_0}(或 $KE_{A_0 \cdot A_i}$)加/解密消息,只要保证域内节点之间共享密钥不公开,就能保证消息的安全和保密。

(2) 数据完整性:同上所述,在密钥协商过程中,利用完整性校验密钥 KI_{A_i, A_0}(或 $KI_{A_0 \cdot A_i}$)计算加密消息的 MIC 校验值,当接收到对方发送的消息后计算消息的 MIC 校验值,验证计算的 MIC 校验值与接收到的消息的 MIC 校验值是否相等,若相等,则接收,否则返回出错信息,从而保证了消息的完整性。

(3) 抗代表节点假冒:域的代表节点是由域内所有节点通过随机选举算法选举的,在密钥协商过程中,域内普通节点与代表节点共同参与协商,而且域 D_1 和域 D_2 的代表节点分别与域内普通节点之间拥有共享密钥,即它们之间具有安全通道。如果敌手假冒代表节点即获取了代表节点的私钥,由于代表节点与域内普通节点之间的共享密钥安全,敌手不能解密获得域内普通节点参与域间共享密钥协商所计算的子密钥,这有效保障了代表节点不被假冒。

(4) 抗代表节点欺骗:抗代表节点欺骗指的是防止代表节点在协商了会话密钥后不及时将其分发给普通节点,甚至不进行密钥分发,而不是指代表节点发一个错误的会话密钥给某个普通节点。在排除通信错误的前提下,普通节点总是可以通过与邻域节点通信来判断会话密钥的正确性,从而能够及时发现错误的会话密钥。本文协议能够防止代表节点不及时或不进行密钥分发,是因为代表节点进行密钥协商时,需要通告普通节点并要求普通节点参与。因此,普通节点如果在一定时间内不能收到代表节点的密钥分发信息,就可以怀疑代表节点这种欺骗行为。

(5) 抗代表节点联合欺骗:当怀疑两个域的代表节点在密钥协商过程中摆脱域内普通节点的参与,联合起来自行计算域间共享密钥并分发给各自的域内节点时,域内普通节点可以通过协议中的共享密钥验证过程发现这种欺骗行为,从而进一步对代表节点做出适当惩罚。结合实际应用中的信任机制和管理策略,共享密钥验证机制可以有效地保证域的代表节点无法成功实施联合欺骗,也使得代表节点不愿意冒信任等级降低风险试图实施联合欺骗。

3.4 性能分析

尽管有如本文所述的安全需求,但我们还没有找到解决由代表节点执行且普通节点参与的安全认证及密钥协商协议,因此,将本文协议和传统两方协议进行比较,考虑传统两方协议在保证节点参与度的情况下与本文方案的性能比较。本文提出的协议与现有的两方密钥协商协议在进行域间密钥协商方面相比,具有以下两个突出优点:

(1) 可靠性。本文提出的协议运行过程中,域内代表节点与域内普通节点进行信息交互,共同参与协商密钥有效保障了代表节点的可靠性,从而确保了协商的共享密钥的可靠性。而采用现有的两方密钥协商协议进行域间密钥协商,并不支持域内普通节点参与协商,只是在两个代表节点之间进行协商,最后由代表节点将所协商的密钥通告给普通节点,这并不能确保代表节点可靠。

(2) 高效率。本协议在域内节点协商共享密钥成功后,由域内代表节点向域内普通节点进行安全分发,从而域中所有节点都获得了共享会话密钥且域内每个节点只需存储一个域间共享密钥。若要确保域内普通节点的高参与度和所协商的共享密钥的可靠性,采用两方密钥协商协议实现两个域中任意节点之间的认证和密钥协商,必然需要运行两个域中节点个数相乘次密钥协商协议,而且若有 N 个节点,每个节点就必须存储 $N-1$ 个共享密钥,这不仅增加了协议运行次数,也增加了节点的存储负荷。从这个角度考虑,本文方案是非常有效的。

另外,通信量和计算量也是影响密钥协商协议运行效率的主要方面。域 D_1(n 个节点)和域 D_2(m 个节点)之间协商共享密钥,在确保域内普通节点的高参与度和所协商的共享密钥的可靠性的前提下,考虑本文提出的协议、McCullagh-Barreto 方案、Chen-dudla 方案、Smart 方案执行域 D_1(n 个节点)和域 D_2(m 个节点)之间的密钥协商在性能方面的优劣,如表 1 所示。M 表示椭圆曲线上的一次乘操

作，E 表示有限域上的一次指数操作，P 表示双线性对操作。

表 1　本文提出的协议与现有的两方密钥协商协议的性能比较

方案	本文提出的协议	McCullagh-Barreto	Chen-dudla	Smart
通信量/轮	1	$n\times m$	$n\times m$	$n\times m$
计算量/操作数	$(d-1)M+dP+(n+d+1)E$	$n\times m\times(M+P+E)$	$n\times m\times(2M+P)$	$n\times m\times(2M+2P)$

由于门限 d 小于域中的节点数 n 和 m，由表 1 可以看出，在想要通信的域 D_1 和域 D_2 之间分别执行本文提出的协议、McCullagh-Barreto 方案、Chen-dudla 方案、Smart 方案实现域 D_1 和域 D_2 中的任意节点之间的认证和密钥协商，本文提出的协议极大地降低了通信轮数和其计算量。

4　结　论

提出了一种基于身份的域间认证及密钥协商协议，使得域间认证及密钥协商更加安全可靠。协议中域内代表节点和普通节点共同参与协商的机制，既保证了代表节点的可靠性，也提高了普通节点在协商过程中的参与度。域间协商共享密钥成功后，由代表节点负责向域内普通节点进行安全分发，这有效地提高了网络通信的整个系统的安全性和通信效率。与现有的两方密钥协商协议实现共享密钥可靠相比较，本文提出的协议有效降低了密钥协商过程的通信量和计算量，这对于网络通信安全的发展具有很重要的实用意义，尤其对于实现如 WMAN 中的无缝安全广播、无缝安全切换更为有用。

参考文献：

[1] 王圣宝，曹福珍，董晓蕾. 标准模型下可证安全的身份基认证密钥协商协议[J]. 计算机学报，2007，30(10)：1842－1854.（Wang S B，Cao F Z，Dong X L. Provably secure identity-based authenticated key agreement protocols in the standard model[J]. *Journal of Computers*，2007，30(10)：1842－1854.）

[2] 汪小芬，陈原，肖国镇. 基于身份的认证密钥协商协议的安全分析与改进[J]. 通信学报，2008，29(12)：16－21.（Wang X F，Chen Y，Xiao G Z. Analysis and improvement of an ID-based authenticated key agreement protocol[J]. *Journal on Communications*，2008，29(12)：16－21.）

[3] Diffie W，Hellman M E. New directions in cryptography[J]. *IEEE Trans. on Information Theory*，1976，22(6)：644－654.

[4] Boyd C，Cliff Y，Nieto J G，et al. One-round key exchange in the standard model[J]. *International Journal of Applied Cryptography*，2009，1(3)：181－199.

[5] Shamir A. Identity based cryptosystems and signature schemes[C]// *Proc. of Crypto Advances in Cryptology*，1984：47－53.

[6] McCullaugh N，Barreto P S L M. A new two-party identity-based authenticated key agreement[C]// *Proc. of the Cryptographers Track at the RSA Conference*，2005：262－274.

[7] Boneh D，Franklin M. Identity-based encryption from the weil pairing[C]// *Proc. of the 21st Annual International Cryptology Conference*，2001：213－229.

[8] Smart N P. Identity based authenticated key agreement protocol based on the Weil pairing[J]. *Electronics Letters*，2002，38(12)：630－632.

[9] Wang H，Xu Q L，Fu X. Two-party attribute-based key agreement protocol in the standard model[C]// *Proc. of the International Symposium on Information Processing*，2009：325－328.

[10] Wang H，Xu X，Ban T. A provably secure two-party attribute-based key agreement protocol[C]// *Proc. of the 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*，2009：1042－1045.

[11] Chen L，Kudla C. Identity based authenticated key agreement protocols from pairings[C]// *Proc. of the 16th IEEE Computer Security Foundations Workshop*，2003：219－233.

[12] Sahai A，Waters B. Fuzzy identity-based encryption[C]// *Proc. of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*，2005：457－473.

[13] Zhao X H，Pang L J，Bi J J，et al. Secure communication model of WSN based on secret sharing[C]// *Proc. of the International Conference on Computational Intelligence and Security*，2010：483－487.

[14] Shamir A. How to share a secret[J]. *Communication of the ACM*，1979，22(11)：612－613.

[15] Wilson S B，Johnson D，Menezes A. Key agreement protocols and their security analysis[C]// *Proc. of the the 6th IMA International Conference on Cryptography and Coding*，1997：30－45.

[16] Bethencourt J，Sahai A，Waters B. Ciphertext-policy attribute-based encryption[C]// *Proc. of the 28th IEEE Symposium on Security and Privacy*，2007：321－334.