身份基认证密钥协商协议的分析与改进

侯孟波,徐秋亮
HOU Meng-bo,XU Qiu-liang

山东大学 计算机科学与技术学院,济南 250101
School of Computer Science and Technology,Shandong University,Jinan 250101,China
E-mail:houmb@sdu.edu.cn

HOU Meng-bo,XU Qiu-liang.Analysis and improvement of ID-based authenticated key agreement protocols.Computer Engineering and Applications,2010,46(7):25-28.

Abstract: The security attributes of three provable secure ID-based authenticated key agreement protocols are analyzed,and an enhanced ID-based authenticated key agreement protocol is presented based on the previous work.The new scheme achieves most of the known security attributes,such as known-key secrecy,key-compromise impersonation resilience,unknown key-share resilience,no-key control and message independence,especially the PKG-forward secrecy and known session-specific temporary information secrecy attributes,meanwhile keeping with the nice efficiency.

Key words: ID-based authenticated key agreement;security attributes;PKG-forward secrecy;known session-specific temporary information secrecy

摘 要: 对三个标准模型下可证明安全的身份基认证密钥协商协议进行了安全属性缺陷分析,在原方案基础上提出了一个安全增强的新方案。新方案满足目前已知的绝大多数安全属性要求,包括已知会话密钥安全性、抗密钥泄露伪装、抗未知密钥共享、无密钥控制以及消息独立性,特别是满足完美前向安全性、PKG 前向安全性、已知会话相关临时秘密信息安全性,同时保持了良好的计算效率。

关键词: 身份基认证密钥协商;安全属性;PKG 前向安全性;已知会话相关临时秘密信息安全性
DOI: 10.3778/j.issn.1002-8331.2010.07.008 **文章编号:** 1002-8331(2010)07-0025-04 **文献标识码:** A **中图分类号:** TN918.1

1 前言

在开放分布式网络环境中,认证性和机密性是安全通信必备的安全要求。认证密钥协商协议作为重要的密码原语为安全通信提供了重要保证。它使得通信的两方(或多方)在身份认证基础上可以建立共享的会话密钥,用于后续的数据加密和完整性保护。认证密钥协商协议分为隐式密钥认证和带有密钥确认的显式密钥认证。一个隐式密钥认证密钥协商协议可以转化为一个带有密钥确认的显式认证密钥协商协议,以提供更高的安全性,防止某些安全性攻击,如密钥复制攻击等[1]。

基于身份(或身份基,ID-based)密码系统是由 Shamir 在 1984 年提出的[2],后来相继出现了许多基于身份的公钥加密方案和数字签名方案,利用基于身份的密码技术和双线性对技术构造密钥协商协议成为继基于离散对数困难性构造密钥协商协议之后的一个重要研究方向。由于在基于身份的密码系统中实体的身份常常被用作公开钥,而秘密钥是通过一个可信赖的私钥产生中心 PKG 产生的,所以不可避免地存在密钥托管问题。对于基于身份的密钥协商协议而言,需要解决会话密钥托管问题(PKG 不能有效计算实体的会话密钥)或者称为 PKG 前向安全性(或主密钥安全性),也要解决私钥泄露带来的会话密钥泄密问题(即完美前向安全性)。目前设计的这类协议大部分并不满足这类安全属性。而且这些已有的协议存在各种各样的安全问题。Shim 方案[3]虽然满足完美前向安全性,但存在中间人攻击[4],McCullagh 等提出的方案[5]无法抵抗密钥泄露伪装攻击[6],Chen 等人的方案[7]虽然在 ROM 模型[8]下被证明是达到了其安全设计目标,但他们的方案并不满足更高的安全性——完善前向安全性和主密钥前向安全性。

王等利用 Gentry 基于身份的加密方案[9]设计了两个认证密钥协商协议[10](分别简称 WCD-1 和 WCD-2 方案),其中 WCD-1 方案用于密钥托管环境下,自然不需要考虑 PKG 前向安全问题。事实上,该方案连完美前向安全性也不具备。作者构造的 WCD-2 方案用于无密钥托管环境下,并在标准模型下证明了其安全性。该方案具备完美前向安全性,但是汪等[11]指出该协议不能满足主密钥前向安全性,恶意的 PKG 能计算出所有的会话密钥。针对无托管的要求,他们提出一个改进的

基金项目: 国家自然科学基金(the National Natural Science Foundation of China under Grant No.60873232);山东省自然科学基金(the Natural Science Foundation of Shandong Province of China under Grant No.Y2007G37)。

作者简介: 侯孟波(1970-),男,博士研究生,讲师,CCF 会员,主要研究领域为密码学与信息安全;徐秋亮(1960-),男,博士,教授,主要研究领域为密码学与信息安全。

收稿日期: 2009-11-26 **修回日期:** 2010-01-14

基于身份的认证密钥协商协议(简称 WCX 方案)并在标准模型下证明新协议的安全性,并且分析了新协议满足完善前向安全性和主密钥前向安全性。以上三个方案都不具备一个重要的安全属性,即已知会话相关临时秘密信息安全性。在以上方案基础上,设计了一个新的安全的密钥协商协议。分析表明,该协议几乎具备所有的已知安全属性要求,包括已知会话密钥安全性、抗密钥泄露伪装、抗未知密钥共享、无密钥控制以及消息独立性等,特别满足完美前向安全、PKG 前向安全、已知会话相关临时秘密信息安全性,同时保持了较好的计算效率。

下面首先介绍基本的技术背景和安全属性,然后回顾王等利用 Gentry 基于身份的加密方案构造的 WCD-1 和 WCD-2 方案以及汪等改进的 WCX 方案。在分析这些方案的安全属性基础上,给出新的方案设计,以满足目前已知绝大多数安全属性。通过分析新方案的安全性和有效性,最终给出结论。

2 技术背景

2.1 密钥协商协议安全属性

一个具有良好安全性的密钥协商协议应满足以下安全属性[1]:

(1)已知会话密钥安全性。已知旧的会话密钥不会影响其他会话密钥的安全性。

(2)前向安全性和完美前向安全性。如果一方或多方参与实体的长期私钥泄露,攻击者不能有效计算旧的会话密钥,称之为部分前向安全性;如果所有参与实体的长期私钥泄露,攻击者仍然不能有效计算旧的会话密钥,称之为完美前向安全性。

(3)PKG 前向安全性。在基于身份的密钥协商协议中,攻击者即使获得私钥产生中心 PKG 的主密钥,仍然无法计算参与实体的会话密钥。

(4)抗密钥泄露伪装。一个参与实体 A 的长期密钥泄露将使得攻击者可以伪装 A,但不应导致攻击者可以伪装成其他实体与 A 进行成功的密钥协商。

(5)无密钥控制(密钥完整性)。参与实体的任何一方或者第三方都不能在协议执行结束时使得会话密钥成为其预先选定的值。由于一轮两方隐式认证密钥协商协议的特殊性,协议交互的响应方总是在收到协议发起方的交互消息之后产生响应消息的,因而响应方天生具备比发起方更多的主动性,这种不公平性导致不可能实现真正意义上的无密钥控制。但是最终会话密钥的生成一定是双方共同贡献产生的。对于攻击者而言,同样不能控制协商的会话密钥,通常我们将对应于攻击者的密钥控制归结到会话密钥完整性的要求。

(6)抗未知密钥共享。一个参与实体 A 不应被强迫与一个实体 C 实现共享会话密钥,而实际上参与实体 A 却认为他是在和一个参与实体 B 完成的密钥协商。

(7)消息独立性。两方或多方参与会话密钥协商的实体交互的消息应是独立产生并交互的,不受其他方的制约和强迫。显然在单轮两方密钥协商协议中消息之间是独立的,但是在带有密钥确认的多轮密钥协商协议中不能保证独立性,用于密钥确认的消息一定与对方发送的消息相关联。该安全属性不适用于带有密钥确认的密钥协商协议。

(8)已知会话相关临时秘密信息安全性。当参与实体在一次会话密钥协商过程中使用的临时秘密信息(短期密钥)泄露后(但长期私钥未泄露),不应当影响到会话密钥的安全性。

已知会话相关临时秘密信息安全性的属性要求首先被 Canetti 等在文献[12]中研究并讨论。事实上,和会话相关的临时秘密的选取与安全保护对最终会话密钥的安全影响是举足轻重的。例如敌手可能控制协议执行环境中的随机数发生源;协议参与者可能相比临时秘密信息选取更加注重长期秘密的保管,如协议执行后协议执行环境未及时妥善清除本地状态,内存环境欠缺安全考虑等,导致攻击者通过劫持获取本地状态。

2.2 双线性映射和困难问题假设

假定 G_1 和 G_2 是两个阶为素数 p 的(乘法)循环群,g 为 G_1 的生成元。假设在群 G_1 和 G_2 中计算离散对数(DLP)是困难的。双线性映射 e 定义为 $e:G_1\times G_1\to G_2$ 满足以下三个条件:

(1)双线性性:对所有的 $u,v\in G_1$ 以及 $a,b\in Z_p^*$,有 $e(u^a,v^b)=e(u,v)^{ab}$;

(2)非退化性:$e(g,g)\neq 1$,1 是 G_2 的单位元;

(3)可计算性:如果任意 $u,v\in G_1$,$e(u,v)\in G_2$ 在多项式时间里可有效计算。

定义 1(判定性 q-ABDHE 问题) 给定$(g',g'^{\alpha},g,g^{\alpha},\cdots,g^{\alpha^q},Z)$,判断 $Z=e(g^{\alpha^{q+1}},g')$是否成立。这里 $g,g'\in G_1$,$\alpha\in Z_q$,$Z\in G_2$。

前述三个基于身份的密钥协商协议安全性证明都是基于判定性 q-ABDHE 问题的,构造的新方案同样基于该困难问题。

3 三个密钥协商协议的安全属性分析

本章简要回顾王等和汪等基于 Gentry 的公钥加密方案构造的三个基于身份的密钥协商协议,并给出其安全属性分析。王等在文献[10]中给出的一个会话密钥托管模型下的基于身份的认证密钥协商协议 WCD-1 方案和一个无会话密钥托管模型下的基于身份的认证密钥协商协议 WCD-2 方案。WCD-1 方案直接利用 Gentry 公钥加密方案构造,该方案巧妙地利用了公钥加密方案中为保证明文加解密安全而采用的随机盲化方法以达成在加密方和解密方安全传递秘密,该方法正好可以利用来实现密钥协商,而不需要真正的加解密手段实现密钥协商,因而有较高的计算效率。WCD-2 方案对 WCD-1 方案进行了改进,改进方法试图引入 PKG 不可计算部分,以达到无会话密钥托管的目的。汪等针对无密钥托管的认证密钥协商协议的要求提出了一个改进的无会话密钥托管的认证密钥协商协议 WCX 方案[11]。

3.1 WCD-1 方案及安全属性分析

首先对 WCD-1 方案进行简要回顾:

(1)系统建立阶段:PKG 随机选取两个生成元 $g,h\in G_1$ 和 $\alpha\in Z_p$,计算 $g_1=g^{\alpha}$。系统公开参数为(g,g_1,h),系统主密钥为 α,H_2 为会话密钥抽取函数。

(2)私钥生成阶段:对给定身份 $ID\in Z_p$,随机选择 $h_{ID}\in Z_p$,计算身份的私钥 $d_{ID}=<r_{ID},h_{ID}>$,其中 $h_{ID}=(hg^{-r_{ID}})^{1/\alpha-ID}$。对每一个身份 ID 选择固定的 r_{ID}。

(3)密钥协商阶段:假设 ID_A 与 ID_B 进行会话密钥协商。令 $g_A=g_1g^{-ID_A}$,$g_B=g_1g^{-ID_B}$ 和 $t_T=e(g,g)$。协议过程如下:

ID_A 随机选择 $x\in Z_p$,计算 $T_{A1}=g_B^x$,$T_{A2}=t_T^x$,将 $T_A=T_{A1}\parallel T_{A2}$ 发送给 ID_B;

ID_B 随机选择 $y\in Z_p$,计算 $T_{B1}=g_A^y$,$T_{B2}=t_T^y$,将 $T_B=T_{B1}\parallel T_{B2}$ 发送给ID_A;

ID_A 计算共享秘密:

$K_{AB}=e(T_{B1},h_A)\cdot(T_{B2})^{r_A}\cdot e(g,h)^x$;

ID_B计算共享秘密:

$K_{BA}=e(T_{A1},h_B)\cdot(T_{A2})^{r_B}\cdot e(g,h)^y$;

由以上等式容易看出$K_{AB}=K_{BA}=e(g,h)^{x+y}$,从而$ID_A$与$ID_B$可以计算出相同的会话密钥:

$sk=H_2(ID_A\|ID_B\|T_A\|T_B\|e(g,h)^{x+y})$

显然方案最终会话密钥只关联于临时秘密x和y的选取。只掌握长期密钥的情况下可以很容易计算最终的会话密钥,因而不具备完美前向安全性,只具有部分前向安全性;只掌握临时秘密的情况下同样可以很容易计算出共享会话密钥,因而不具备已知会话相关临时秘密信息安全性;由于PKG掌握系统主密钥,容易计算得到实体的长期私钥,进而可以容易地计算实体的会话密钥,从而不具有PKG前向安全性,只能用于会话密钥托管环境中。

3.2 WCD-2 方案及安全属性分析

首先对WCD-2方案进行简要回顾:

(1)系统建立阶段:PKG随机选取三个生成元$g,h,t\in G_1$和$\alpha\in Z_p$,计算$g_1=g^\alpha$。系统公开参数为(g,g_1,h,t),系统主密钥为α,H_2为会话密钥抽取函数。

(2)私钥生成阶段:对给定身份$ID\in Z_p$,随机选择$r_{ID}\in Z_p$,计算身份的私钥$d_{ID}=<r_{ID},h_{ID}>$,其中$h_{ID}=(ht^{-r_{ID}})^{1/\alpha-ID}$。对每一个身份$ID$选择固定的。

(3)密钥协商阶段:假设ID_A与ID_B进行会话密钥协商。令$g_A=g_1g^{-ID_A}$,$g_B=g_1g^{-ID_B}$和$t_T=e(g,t)$。协议交互过程如下:

ID_A随机选择$x\in Z_p$,计算$T_{A1}=g_B^x$,$T_{A2}=t_T^x$,将$T_A=T_{A1}\|T_{A2}$发送给ID_B;

ID_B随机选择$y\in Z_p$,计算$T_{B1}=g_A^y$,$T_{B2}=t_T^y$,将$T_B=T_{B1}\|T_{B2}$发送给ID_A;

ID_A计算共享秘密:

$K_{AB1}=e(T_{B1},h_A)\cdot(T_{B2})^{r_A}\cdot e(g,h)^x$,$K_{AB2}=T_{B2}^x$

ID_B计算共享秘密:

$K_{BA1}=e(T_{A1},h_B)\cdot(T_{A2})^{r_B}\cdot e(g,h)^y$,$K_{BA2}=T_{A2}^y$

从以上公式容易看出$K_{AB1}=K_{BA1}=e(g,h)^{x+y}$与$K_{AB2}=K_{BA2}=e(g,t)^{xy}$,从而$ID_A$与$ID_B$可以计算出相同的会话密钥:

$sk=H_2(ID_A\|ID_B\|T_A\|T_B\|e(g,h)^{x+y}\|e(g,t)^{xy})$

汪等在文献[11]中指出,恶意的PKG通过在系统建立阶段选定$t=g^\gamma$(随机选择整数$\gamma\in Z_p$),就能使得PKG获得ID_A与ID_B协商的所有会话密钥,详细攻击手段参见文献[11]中的描述。该攻击说明恶意PKG通过特意的构造参数可以实施有效的针对PKG前向安全性进行攻击。同时也发现,WCD-2协议最终会话密钥仍然只关联于临时秘密信息x和y。在不知道密钥协商双方长期密钥的情况下,如果获得了临时秘密信息x和y,攻击者就能容易地计算旧的会话密钥,因而该方案也不满足已知会话相关临时秘密信息安全属性。

3.3 WCX 方案及安全属性分析

汪等针对无密钥托管的认证密钥协商协议的要求提出了一个改进的无会话密钥托管的认证密钥协商协议WCX方案[11]。以下简要描述改进协议的主要过程(详见参考文献[11]):

(1)系统建立阶段:与WCD-1协议基本相同。其中H为会话密钥抽取函数。

(2)实体密钥对生成阶段:与WCD-1协议相同,令$g_T=e(g,g)$。

(3)密钥协商阶段:

ID_A随机选择$x\in Z_p$,计算

$T_{A1}=g_B^x$,$T_{A2}=g_T^x$,$T_{A3}=g^x$

将$T_A=T_{A1}\|T_{A2}\|T_{A3}$发送给$ID_B$;

ID_B随机选择$y\in Z_p$,计算

$T_{B1}=g_A^y$,$T_{A2}=g_T^y$,$T_{B3}=g^y$

将$T_B=T_{B1}\|T_{B2}\|T_{B3}$发送给$ID_A$;

ID_A计算共享秘密:

$K_{AB1}=e(T_{B1},h_A)\cdot T_{B2}^{r_A}\cdot e(g,h)^x$,$K_{AB2}=T_{B3}^x$

ID_B计算共享秘密:

$K_{BA1}=e(T_{A1},h_B)\cdot T_{A2}^{r_B}\cdot e(g,h)^y$和$K_{BA2}=T_{A3}^y$

ID_A计算会话密钥:

$sk_{AB}=H(ID_A\|ID_B\|T_A\|T_B\|K_{AB1}\|K_{AB2})$

ID_B计算会话密钥:

$sk_{BA}=H(ID_A\|ID_B\|T_A\|T_B\|K_{BA1}\|K_{BA2})$

显然

$K_{AB1}=K_{BA1}=e(g,h)^{x+y}$,$K_{AB2}=K_{BA2}=g^{xy}$

因此ID_A与ID_B计算出相同的会话密钥为:

$sk=H(ID_A\|ID_B\|T_A\|T_B\|e(g,h)^{x+y}\|g^{xy})$

该协议满足完美前向安全性和PKG前向安全性。即使敌手获得ID_A和ID_B的私钥,以及系统主密钥α,只能计算出第一个共享秘密$K_{AB1}=K_{BA1}=e(g,h)^{x+y}$。若要得到第二个共享秘密,必须由$g^x$和$g^y$计算出$g^{xy}$,这是CDH困难问题。该方案通过增加交互消息$T_{A3}=g^x$和$T_{B3}=g^y$,使得在会话密钥生成中增加PKG不可计算因素,从而达到PKG前向安全属性。当然这势必会影响协议执行的效率。同时注意到,改进协议中$(g,h)^{x+y}$和g^{xy}两个因素仍然是在已知会话相关临时秘密信息下可计算的,因而该方案仍然不满足已知会话相关临时秘密信息安全属性。

4 安全增强的身份基认证密钥协商协议

为了提供更多的安全属性,提高方案的安全性,本章构造了一个安全增强的认证密钥协商方案。改进后的新方案几乎满足全部已知的安全属性,特别是满足完美前向安全性、PKG前向安全性以及已知会话相关临时秘密信息安全属性。与此同时,新方案保持了良好的计算效率。新方案描述如下:

(1)系统建立阶段:PKG随机选取两个生成元$g,h\in G_1$和$\alpha\in Z_p$,计算$g_1=g^\alpha$。系统公开参数(g,g_1,h),系统主密钥为α,H为会话密钥抽取函数$H:\{0,1\}^*\to\{0,1\}^k$,k为会话密钥长度。

(2)密钥生成阶段:对给定身份$ID\in Z_p$,随机选择$r_{ID}\in Z_p$,计算身份的私钥$d_{ID}=<r_{ID},h_{ID}>$,其中$h_{ID}=(hg^{-r_{ID}})^{1/(\alpha-ID)}$。对每一个身份$ID$选择固定的$r_{ID}$。

(3)密钥协商阶段:假设ID_A与ID_B进行会话密钥协商。令

$g_A=g_1g^{-ID_A}$，$g_B=g_1g^{-ID_B}$和$g_T=e(g,g)$。协议过程如下：

ID_A随机选择$x\in Z_p$，并计算

$T_{A1}=g_B^x$，$T_{A2}=g_T^x$，$T_{A3}=g_T^{r_A}$

将$T_A=T_{A1}\|T_{A2}\|T_{A3}$发送给$ID_B$；

ID_B随机选择$y\in Z_p$，并计算

$T_{B1}=g_A^y$，$T_{B2}=g_T^y$，$T_{B3}=g_T^{r_B}$

将$T_B=T_{B1}\|T_{B2}\|T_{B3}$发送给$ID_A$；

ID_A计算共享秘密如下：

$K_{AB1}=e(T_{B1},h_A)\cdot T_{B2}^{r_A}\cdot e(g,h)^x$，$K_{AB2}=(T_{B2}\cdot T_{B3})^{(x+r_A)}$

ID_B计算共享秘密如下：

$K_{BA1}=e(T_{A1},h_B)\cdot T_{A2}^{r_B}\cdot e(g,h)^y$，$K_{BA2}=(T_{A2}\cdot T_{A3})^{(y+r_B)}$

ID_A计算会话密钥为：

$sk_{AB}=H(ID_A\|ID_B\|T_A\|T_B\|K_{AB1}\|K_{AB2})$

ID_B计算会话密钥为：

$sk_{BA}=H(ID_A\|ID_B\|T_A\|T_B\|K_{BA1}\|K_{BA2})$

容易看出

$K_{AB1}=K_{BA1}=e(g,h)^{x+y}$

$K_{AB2}=K_{BA2}=g_T^{(x+r_A)(y+r_B)}=g_T^{xy}\cdot g_T^{xr_B}\cdot g_T^{yr_A}\cdot g_T^{r_Ar_B}$

因此ID_A与ID_B计算出共享会话密钥为：

$$sk=H(ID_A\|ID_B\|T_A\|T_B\|e(g,h)^{x+y}\|g_T^{xy+xr_B+yr_A+r_Ar_B})$$

5 新方案安全性和效率分析

5.1 安全性分析

限于篇幅，本节只给出新方案的非形式化安全属性分析。

(1)已知会话密钥安全性。该方案中已知旧的会话密钥不会影响新的会话密钥安全性。每一次协议的执行，临时秘密x和y都是分别由参与实体A和B独立随机选取的。多个会话密钥值之间具有无关性。

(2)前向安全性和完美前向安全性。如果A 或者B以及A和B的长期密钥$d_{ID}=<r_{ID},h_{ID}>$泄露，将不会影响旧的会话密钥安全性。虽然这将导致攻击者可以根据历史交互消息和长期密钥计算$K_{AB1}=K_{BA1}=e(g,h)^{x+y}$，$g_T^{r_Ar_B}$，$g_T^x$，$g_T^{r_A}$，$g_T^y$，$g_T^{r_B}$，但是由$(g_T^x,g_T^{r_B})$和$(g_T^{r_A},g_T^y)$计算$g_T^{xr_B}$和$g_T^{yr_A}$进而计算$K_{AB2}=K_{BA2}=g_T^{xy}\cdot g_T^{xr_B}\cdot g_T^{yr_A}\cdot g_T^{r_Ar_B}$需要解决CDH困难问题。通过$(g_T^x,g_T^y)$计算$g_T^{xy}$同样需要解决CDH困难问题。

(3)PKG前向安全性。新协议是一个基于身份的密钥协商协议，攻击者即使获得PKG的主密钥α，可以计算参与实体A和B的长期密钥（因为A和B的长期私钥生成算法是随机算法，所以无法计算出与以前生成的相同的私钥），以及计算得到g_T^{xy}（可计算g^x和g^y，$g_T^{xy}=e(g^x,g^y)$，详细计算方法参见文献[11]），但是因为不知道r_A和r_B，从而无法计算$g_T^{xr_B}$和$g_T^{yr_A}$（需要解决CDH困难问题）。所以仍然无法计算参与实体的最终会话密钥。

(4)抗密钥泄露伪装。一个参与实体A的长期密钥泄露将使得攻击者C可以伪装A，但是这不会导致攻击者C可以伪装成其他实体B与A进行成功的密钥协商。因为攻击者C的成功伪装需要知道B的私钥来计算$e(g,h)^x$。仅仅知道A的私钥是无济于事的。

(5)无密钥控制（密钥完整性）。由于最终会话密钥的生成依赖于参与实体A和B的临时秘密x和y以及A和B的长期私钥，任何一方都不能强制最终会话密钥为自己预先选择的值。对于第三方攻击者C，可能通过截获以及篡改的手段形成一种典型的攻击—密钥复制攻击，这种攻击的效果是依然能使A和B协商得到一个相同的会话密钥，但是并非是应该协商得到的值。这是一种典型的破坏会话密钥完整性的攻击手段。在该方案中，密钥复制攻击是不能奏效的，因为如果攻击者C通过合适的交互消息篡改（如令$T'_{A1}=(T_{A1})^a$，$T'_{A2}=(T_{A2})^a$；$T'_{B1}=(T_{B1})^b$，$T'_{B2}=(T_{B2})^b$等）试图达到目的，则将导致A和B双方协商的第一个秘密变成$K_{AB1}=e(g,h)^{x+by}$和$K_{BA1}=e(g,h)^{ax+y}$的形式，要想保证$K_{AB1}=K_{BA1}$，则只能是$a=b=1$。也就是说，任何的篡改都将使得$K_{AB1}\neq K_{BA1}$；同理，试图对T_{A3}和T_{B3}的篡改也会导致$K_{AB2}\neq K_{BA2}$。

(6)抗未知密钥共享。一个参与实体A不可能被强迫与一个实体C实现共享会话密钥，而A却认为他是在和一个参与实体B完成密钥协商。因为A所发出的交互消息是用B的公钥加密的，C是不能解密得出$e(g,h)^x$的。

(7)已知会话相关临时秘密信息安全性。方案中最终会话密钥协商的结果关联于A和B独立选择的临时秘密x和y以及他们的长期部分密钥r_A和r_B。仅仅知道临时密密x和y，只能计算

$K_{AB1}=K_{BA1}=e(g,h)^{x+y}$

$K_{AB2}=K_{BA2}=g_T^{(x+r_A)(y+r_B)}=g_T^{xy}\cdot g_T^{xr_B}\cdot g_T^{yr_A}\cdot g_T^{r_Ar_B}$

中的$g_T^{xy}\cdot g_T^{xr_B}\cdot g_T^{yr_A}$，而无法计算$g_T^{r_Ar_B}$。

(8)消息独立性。本协议是一个两方两轮会话密钥协商协议，很显然两个方向上的实体交互消息是完全独立产生并交互的，临时秘密x和y是A和B独立选择并参与计算的。

分析表明新方案满足目前已知的全部安全属性，特别是完美前向安全性、PKG前向安全性和已知会话相关临时秘密信息安全性。表1对前述几个方案进行了主要的安全属性比较。结果表明，新协议具有更高的安全性（PFS：完美前向安全性；PKG-FS：PKG前向安全性；KSSTSIS：已知会话相关临时秘密信息安全性）。

表1 安全属性比较

方案	安全属性		
	PFS	PKG-FS	KSSTSIS
WCD-1	×	×	×
WCD-2	√	×	×
WCX	√	√	×
新方案	√	√	√

5.2 效率分析

一个认证密钥协商协议的效率通常考虑计算量、通信量以及轮数。前述方案都是两方两轮认证密钥协商协议，在通信量上是相当的，但是计算量不同。由于几个协议都是基于Gentry的基于身份的公钥加密方案，在计算量比较的时候主要考虑对运算、指数运算和点乘运算代价。表2给出了几个协议的计算量比较。比较说明，新方案在提高安全性的同时，依然保持良好的计算有效性。

（下转51页）