ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, Supplement, December 2009, pp.321−329

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于无证书的两方认证密钥协商协议*

侯孟波+, 徐秋亮, 郭山清

(山东大学 计算机科学与技术学院,山东 济南 250101)

Certificateless-Based Two-Party Authenticated Key Agreement Protocol

HOU Meng-Bo+, XU Qiu-Liang, GUO Shan-Qing

(School of Computer Science and Technology, Shandong University, Ji'nan 250101, China)

+ Corresponding author: E-mail: houmb@sdu.edu.cn

Hou MB, Xu QL, Guo SQ. Certificateless-Based two-party authenticated key agreement protocol. *Journal of Software*, 2009,20(Suppl.):321−329. http://www.jos.org.cn/1000-9825/09037.htm

Abstract: Two-Party authenticated key agreement protocols are constructed mainly based on the traditional public key cryptography and identity-based public key cryptography. The certificateless-based authenticated key agreement protocols have the advantages of avoiding the complexity of identity management in the traditional certificate-based schemes, as well as the key escrow issues inherited in the identity-based schemes. In 2007, Park et al. proposed a certificateless-based public key encryption scheme which is provably secure against chosen plaintext attacks in the selective-ID security model (IND-sID-CPA). Inspired on such a scheme, this paper presents a two-party certificateless-based authenticated key agreement scheme and gives the comparisons with other comparable schemes in security and efficiency. The new proposed scheme achieves almost all of the desired security attributes, especially the Perfect forward secrecy, PKG forward secrecy, Known session-specific temporary information secrecy and Key escrowless. Meanwhile it keeps the nice efficiency.

Key words: authenticated key agreement; certificateless-based encryption; perfect forward secrecy; PKG forward secrecy; key escrow

摘 要: 两方认证密钥协商协议的设计主要基于传统公钥密码体制和基于身份的公钥密码体制.基于无证书的认证密钥协商方案避免了基于传统公钥证书方案存在的身份管理复杂性,同时也消除了基于身份方案中所固有的密钥托管问题.Park 等人在 2007 年提出了选择身份安全模型下抗选择明文攻击(IND-sID-CPA)的无证书加密方案,在该方案的启发下提出了基于无证书体制的两方认证密钥协商方案,并与其他方案进行了安全性和有效性比较.该方案满足目前已知的绝大多数安全属性要求,特别是完美前向安全性,PKG 前向安全性,已知会话相关临时秘密信息安全性以及无密钥托管等安全特性,同时保持了良好的计算效率.

关键词: 认证密钥协商;无证书加密;完美前向安全;PKG 前向安全;密钥托管

两方认证密钥协商协议作为重要的密码原语,为开放网络环境下两个实体的安全通信提供认证性,机密性

* Supported by the National Natural Science Foundation of China under Grant No.60873232 (国家自然科学基金); the Natural Science Foundation of Shandong Province of China under Grant Nos.Y2007G37, Q2008G01 (山东省自然科学基金)

Received 2009-05-03; Accepted 2009-09-30

和完整性保护.该类协议的设计大都基于各种公钥密码体制,如传统公钥密码体制(PKC-based),基于身份的密码体制(ID-based)[1],基于无证书密码体制(Certificateless-based)[2]等,基于不同公钥密码体制设计的认证密钥协商协议具有不同的安全特性.

Diffie和Hellman[3]在 1976 年提出DH密钥协商协议之后,为了解决DH协议本身无认证和容易遭受中间人攻击的问题,基于传统公钥证书的认证密钥协商方案大量出现,比较典型的方案如MQV协议[4],TS系列协议[5]以及CMQV[6]协议等.该类方案的主要问题是认证性的获得依赖于公钥证书的身份管理和公钥证书的有效性验证,从而存在身份管理的复杂性.自从Shamir[1]在 1984 年提出基于身份的公钥密码体制之后,相继出现一系列基于身份的认证密钥协商方案(Chen等人给出了基于身份的认证密钥协商方案综述,见文献[7]).这些方案最初基本是直接基于双线性对技术进行构造的,在基于身份的公钥加密方案出现之后,基于该类公钥加密方案[8]构造的认证密钥协商方案[9,10]也涌现出来.这类方案存在的主要问题是难以避免基于身份的密钥管理中固有的密钥托管问题.由于基于身份的密码体制依赖于私钥生成中心(private key generator,简称PKG)的支持,会话过程中任一方短期临时密钥的泄露,都会导致恶意PKG很容易计算出最终协商的会话密钥.2003 年Al-Riyami和Paterson[2]提出了基于无证书的公钥密码体制,该类密码体制的基本思想是将基于身份的公钥密码体制与传统公钥密码体制相结合,一方面保持了基于身份的公钥密码体制的身份易管理性,消除了传统公钥密码体制中公钥证书管理的负担,同时也解决了基于身份的公钥密码体制中固有的密钥托管问题.这使得基于无证书公钥密码体制构建认证密钥协商协议成为一个新的研究点[11−14].目前基于无证书公钥密码体制设计的认证密钥协商协议还比较少,对该类方案的可证安全模型以及可证安全的研究有待深入[15].

Al-Riyami和Paterson[2]在提出无证书公钥密码体制的同时,设计了第一个基于无证书的认证密钥协商协议,一次协议执行的每一方需要计算四个双线性对运算,计算开销较高.后来Mandt和Tan[11]提出了一个基于BDH(Bilinear Diffie-Hellman)计算困难性假设的两方无证书认证密钥协商方案,但是该协议方案存在密钥泄露伪装(key-compromise impersonation,简称KC-I)攻击和已知会话相关临时信息 (Known Session-specific Temporary Information)安全攻击.Wang等人[12]也提出了一个类似方案,同样容易遭受KC-I攻击.Shi和Li[13]基于无证书公钥加密方案构造了另一个认证密钥协商方案,Swanson[16]分析表明该方案不具备完美前向安全属性和已知会话相关临时信息安全属性,同时外部攻击者可以发起中间人攻击导致协议隐式认证失败.我们同时发现[17]该方案也容易遭受密钥复制攻击(key replicating attack,简称KR-A).最近,Wang等人[14]提出了第一个在网格计算环境下基于DH密钥协商协议和无证书公钥密码体制的认证密钥协商方案,我们发现该方案不能有效抵抗KC-I攻击和KR-A攻击.目前已知的无证书认证密钥协商方案几乎全部都是采用非形式化的方法进行安全分析,还没有建立有效的可证安全模型.最近,Lippold等人[15]首次对无证书认证密钥协商方案引进了敌手安全模型并进行了有益的可证安全探索.

2007 年,Park等人[18]提出了一个无证书公钥加密方案(称之为PCHL-CL-PKE方案).该方案的设计思想来自于Gentry[19]的基于身份的公钥加密方案,作者基于判定q-BDHI和判定 1-BDHI计算复杂性假设,在选择身份和选择明文攻击安全下给出了方案的标准模型下的安全证明.在该无证书加密方案思想的启发下,通过适当修改密钥产生方法,我们构造了一个有效的无证书两方认证密钥协商协议,并给出了方案的安全性分析和效率分析.安全分析表明,新方案几乎满足所有目前已知的安全属性要求,同时保持了较好的计算效率.

第 1 节介绍必要的背景知识和定义.第 2 节简要回顾 Park 等人提出的 PCHL-CL-PKE 加密方案.第 3 节提出新的两方无证书认证密钥协商方案的详细设计.第 4 节对新方案的安全性进行详细分析并与类似方案进行安全性比较.第 5 节对新方案的计算效率与其它方案进行了比较.第 6 节给出总结并对下一步工作提出展望.

1 背景知识与定义

1.1 认证密钥协商协议应具有的基本安全属性

一个具有良好安全性的密钥协商协议应至少满足以下安全属性要求[20]:

已知会话密钥安全性.已知旧的会话密钥不会影响到其他会话密钥的安全性.

前向安全性与完美前向安全性.如果参与通信的一方或多方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全部泄露,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.对于任意经由公钥认证也无曾经安全共享状态的两消息密钥协商协议来说,在主动攻击者存在的情况下不可能达到真正意义的完美前向安全,我们把被动攻击者存在情况下的完美前向安全性称为弱完美前向安全性[21].

PKG 前向安全性.在基于身份的认证密钥协商协议中,攻击者即使获得私钥生成中心 PKG 的主密钥,仍然无法计算参与实体的会话密钥.这隐含着无密钥托管特性,即 PKG 无法被动托管会话密钥.

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伪装成 A 是显然的,但是这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.

无密钥控制与密钥完整性.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.实际上很难达到真正完美的无密钥控制安全属性,这是因为在单轮两方隐式认证密钥协商协议中, 总是有一方首先初始化协议的执行并首先选择它的短期临时密钥,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, 因而协议执行的响应方就具备通过自己一方合适的短期临时密钥的选取来达到估计最终会话密钥部分比特内容的能力,从而具备比发起方更多的主动性,这种不公平性将导致不可能实现真正意义上的无密钥控制.该缺点存在于一切两方单轮会话密钥协商协议中[22].一般意义上的无密钥控制指的是最终会话密钥的生成必须是双方共同贡献的结果.对于攻击者而言,也不应有效控制最终协商的会话密钥值,通常我们将对应于攻击者的密钥控制归结为会话密钥完整性的要求.

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.

消息独立性.两方或多方参与会话密钥协商的实体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交互消息之间是独立的,但是在带有密钥确认的多轮密钥协商协议中无法保证交互消息独立性,用于密钥确认的消息一定与对方发送的消息产生关联.该安全属性不适用于带有密钥确认的密钥协商协议.

已知会话相关临时秘密信息安全性[11].当协议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泄露后(必须保证长期私钥未泄露),不应当影响到最终会话密钥的安全性.这种秘密泄露一方面针对一般攻击者,同时也包含恶意的PKG.该安全属性要求首先被 Canetti 等人在文献[23]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,将导致攻击者可能通过内存劫持等方法获取本地状态信息.

1.2 双线性对

本文协议执行双方需要依赖于双线性对的运算.假定 G_1 是一个阶为素数 q 的循环加法群, G_2 是一个阶为素数 q 的循环乘法群, P 为 G_1 的生成元.假定在群 G_1 和 G_2 中离散对数 (DLP) 问题是困难的.双线性映射(双线性对) e 定义为 $e:G_1\times G_1\to G_2$ 满足以下 3 个属性:

双线性:对所有的 $P,Q\in G_1$ 以及 $a,b\in Z_q^*$, $e(aP,bQ)=e(P,Q)^{ab}$ 成立;

非退化: $e(P,P)\neq 1$, 1 是 G_2 的单位元;

可计算:对 $\forall P,Q\in G_1$,计算 $e(P,Q)\in G_2$ 可在在多项式时间里完成.

椭圆曲线上的 Weil 对和 Tate 对可用于构造这样的双线性映射.

1.3 计算复杂性假设

方案的安全性基于以下计算复杂性假设,定义如下.

定义 1. Computational Diffie-Hellman. 假设(*CDH*):设定 $g\in G_2$ 为群 G_2 的一个生成元,给定 $\forall a,b\in Z_q^*$ 以及 g^a 和 g^b,计算 g^{ab} 是困难的.

定义 2. q-Bilinear Diffie-Hellman Inversion. 假设(q-*BDHI*):给定元组 $(g,g^{\alpha},g^{\alpha^2},...,g^{(\alpha^q)})\in G_1^{q+1}$ 作为输入,计算 $e(g,g)^{1/\alpha}\in G_2$ 是困难的.

定义 3. 判定 q-BDHI 问题:是指给定元组 $(g,g^{\alpha},g^{\alpha^2},...,g^{(\alpha^q)},T)\in G_1^{q+1}\times G_2$ ($\alpha\in Z_p^*$), 判断 $T=e(g,g)^{1/\alpha}$ 或者 $T=e(g,g)^{\gamma}$ ($\gamma\in Z_p^*$)是否成立.我们说判定 $(t,q,\varepsilon)-BDHI$ 问题成立,如果没有 t-time 算法以至少 ε 的优势解决 $(t,q,\varepsilon)-BDHI$ 问题.

2 PCHL-CL-PKE 加密方案回顾

2007 年Park等人[18]在Gentry[19]的基于身份的公钥加密方案基础上构造了一个无证书公钥加密方案.该方案在选择身份安全模型(selective-ID)和标准安全模型下被证明是选择明文攻击可证安全的,基于的计算复杂性假设为判定q-BDHI和判定 1-BDHI问题.现将该方案简要回顾如下:

假定 G_1 和 G_2 是素阶为 p 的双线性群, $e:G_1\times G_1\to G_2$ 为双线性映射关系.加密方案包括如下五个阶段.

系统建立(Setup).为了提供实体的私钥产生服务,私钥生成中心 PKG 首先随机产生一个生成元 $g\in G_1$ 和两个随机元素 $h,u\in G_1$.随机产生一个秘密 $\alpha\in Z_p^*$ 并定义 $g_1=g^{\alpha}\in G_1$.系统的公共参数为 $\langle g,g_1,h,u\rangle$,PKG 的主密钥为 α .

部分私钥产生(Extract-Partial-Private-Key).针对一个实体,其身份为 $ID\in Z_p$ .PKG 为了给该实体颁发部分私钥,它首先为该实体随机产生 $s_{ID}\in Z_p$,输出部分私钥为 $d_{ID}=\langle s_{ID},h_{ID}\rangle$,其中 $h_{ID}=(hg^{-s_{ID}})^{1/(\alpha-ID)}$ .PKG 要保证 $ID\neq\alpha$ 并且对给定身份 ID,总是赋予相同的 s_{ID} .

设定实体密钥(Set-Entity-Key).实体 ID 随机选择 $x_{ID}\in Z_p^*$ 作为自己的秘密值,完整私钥为 $SK_{ID}=\langle x_{ID},s_{ID},h_{ID}\rangle$,完整公钥为 $PK_{ID}=\langle X_{ID},Y_{ID}\rangle$,其中 $g_{ID}=g_1g^{-ID}$, $X_{ID}=g_{ID}^{x_{ID}}=(g_1g^{-ID})^{x_{ID}}$, $Y_{ID}=u^{x_{ID}}$.

加密(Encryption).加密实体首先验证解密实体公钥合法性($e(X_{ID},u)=e(g_{ID},Y_{ID})$),然后随机选择 $r\in Z_p^*$,并使用解密实体的身份信息 ID,对给定明文 $m\in G_2$ 进行加密,密文形式为:

$$C=(C_1,C_2,C_3)=(X_{ID}^r,\ e(g,g)^r,\ m\cdot e(g,h)^{-r}).$$

解密(Decryption).身份信息为 ID 的实体为了解密密文 $C=(C_1,C_2,C_3)$,计算明文为:

$$m=e(C_1^{1/x_{ID}},h_{ID})\cdot C_2^{s_{ID}}\cdot C_3 .$$

一致性检查:解密实体能够正确解密获取明文.因为

$$e(C_1^{1/x_{ID}},h_{ID})\cdot C_2^{s_{ID}}=e(g^{r(\alpha-ID)},\ h^{1/(\alpha-ID)}g^{-s_{ID}/(\alpha-ID)})\cdot e(g,g)^{rs_{ID}}=e(g,h)^r .$$

3 新的无证书两方认证密钥协商方案

我们基于前述Park等人[18]提出的PCHL-CL-PKE无证书加密方案的思想,通过对密钥产生过程进行适当修改,构造了一个安全有效的无证书两方认证密钥协商方案.

假定两个需要进行密钥协商的实体分别为 C 和 S(如 C 为客户端,S 为服务器端).新方案包含 3 个阶段,分别是系统建立阶段(Setup),密钥产生阶段(Key Generation)和密钥协商阶段(Key Agreement).其中系统建立阶段与 PCHL-CL-PKE 加密方案基本相同,密钥产生阶段做了一定的修改.具体方案描述如下.

系统建立阶段(Setup).私钥生成中心 PKG 首先产生系统参数 $\langle g,g_1,h,u\rangle$,主密钥 α ,主公钥 $g_1=g^{\alpha}\in G_1$.对于身份为 ID 的实体,定义 $g_c=g_1g^{-ID_c}$, $g_s=g_1g^{-ID_s}$, $g_T=e(g,g)$.并定义一个 HASH 函数 $H:\{0,1\}^*\to\{0,1\}^{k_1}$ 作为系统的会话密钥演化函数(key derivation function,简称KDF),其中 $k_1=|sk|$,sk是两个实体C和S通过协议建立的最终的会话密钥.由于本方案基于的无证书加密方案是选择明文安全的,最终协商会话密钥的导出经由KDF函数非常必要.

密钥产生阶段(key generation).根据 PCHL-CL-PKE 加密方案中的密钥产生方法,PKG 为实体生成并安全分发部分密钥,实体自主产生自己的秘密值.所不同的是,实体在计算自己的部分公钥时变为 $Y_{ID}=u^{x_{ID}+s_{ID}}$.对于

身份为 ID_c 的实体 C,定义其完整私钥为 $SK_c=\langle x_c,s_c,h_c\rangle$,其完整公钥为 $PK_c=\langle X_c,Y_c\rangle$,其中 $X_c=g_c^{x_c}=(g_1g^{-ID_c})^{x_c}$,$Y_c=u^{x_c+s_c}$;对于身份为 ID_s 的实体 S,定义其完整私钥为 $SK_s=\langle x_s,s_s,h_s\rangle$,其完整公钥为 $PK_s=\langle X_s,Y_s\rangle$.其中 $X_s=g_s^{x_s}=(g_1g^{-ID_s})^{x_s}$,$Y_s=u^{x_s+s_s}$.

密钥协商阶段(Key Agreement). 实体 C 和 S 按照如下协议步骤进行消息交互,并最终通过隐式认证协商出会话密钥 sk.该协议为单轮密钥协商协议,具体协议步骤如下.

实体 C 选择 $r_c\in_R Z_p^*$,并计算 $T_{c1}=T_{c_{11}}\|T_{c_{12}}$,其中 $T_{c_{11}}=g_s^{r_c}$,$T_{c_{12}}=g_T^{r_c}$,然后将 T_{c1} 发送给实体 S.

实体 S 选择 $r_s\in_R Z_p^*$,并计算 $T_{s1}=T_{s_{11}}\|T_{s_{12}}$,其中 $T_{s_{11}}=g_c^{r_s}$,$T_{s_{12}}=g_T^{r_s}$,然后将 T_{s1} 发送给实体 C.

实体 C 验证实体 S 的公钥合法性,并计算:

$$T_{c2}=e(T_{s_{11}},h_c)\cdot(T_{s_{12}})^{s_c}\cdot e(g,h)^{r_c},$$

$$T_{c3}=T_{s_{12}}^{r_c}=e(g,g)^{r_cr_s},$$

$$T_{c4}=Y_s^{(x_c+s_c)}=u^{(x_c+s_c)(x_s+s_s)}=u^{(x_cx_s+x_cs_s+s_cx_s+s_cs_s)},$$

$$sk_c=H(ID_c\|ID_s\|T_{c1}\|T_{s1}\|T_{c2}\|T_{c3}\|T_{c4}).$$

实体 S 验证实体 C 的公钥合法性,并计算:

$$T_{s2}=e(T_{c_{11}},h_s)\cdot(T_{c_{12}})^{s_s}\cdot e(g,h)^{r_s},$$

$$T_{s3}=T_{c_{12}}^{r_s}=e(g,g)^{r_sr_c},$$

$$T_{s4}=Y_c^{(x_s+s_s)}=u^{(x_s+s_s)(x_c+s_c)}=u^{(x_cx_s+x_cs_s+s_cx_s+s_cs_s)},$$

$$sk_s=H(ID_c\|ID_s\|T_{c1}\|T_{s1}\|T_{s2}\|T_{s3}\|T_{s4}).$$

会话密钥正确性验证:协议执行结束后,实体 C 和实体 S 将协商出相同的会话密钥,因为

$$\begin{aligned}T_{c2}&=e(T_{s_{11}},h_c)\cdot(T_{s_{12}})^{s_c}\cdot e(g,h)^{r_c}\\&=e(g_c^{r_s},(hg^{-s_c})^{1/(\alpha-ID_c)})\cdot(g_T^{r_s})^{s_c}\cdot e(g,h)^{r_c}\\&=e(g^{r_s(\alpha-ID_c)},(hg^{-s_c})^{1/(\alpha-ID_c)})\cdot g_T^{r_ss_c}\cdot e(g,h)^{r_c}\\&=e(g^{r_s},hg^{-s_c})\cdot g_T^{r_ss_c}\cdot e(g,h)^{r_c}\\&=e(g^{r_s},g^{-s_c})\cdot e(g^{r_s},h)\cdot e(g,g)^{r_sr_c}\cdot e(g,h)^{r_c}\\&=e(g,h)^{r_s+r_c}\end{aligned}\quad(1)$$

$$\begin{aligned}T_{s2}&=e(T_{c_{11}},h_s)\cdot(T_{c_{12}})^{s_s}\cdot e(g,h)^{r_s}\\&=e(g_s^{r_c},(hg^{-s_s})^{1/(\alpha-ID_s)})\cdot(g_T^{r_c})^{s_s}\cdot e(g,h)^{r_s}\\&=e(g^{r_c(\alpha-ID_s)},(hg^{-s_s})^{1/(\alpha-ID_s)})\cdot g_T^{r_cs_s}\cdot e(g,h)^{r_s}\\&=e(g^{r_c},hg^{-s_s})\cdot g_T^{r_cs_s}\cdot e(g,h)^{r_s}\\&=e(g^{r_c},g^{-s_s})\cdot e(g^{r_c},h)\cdot e(g,g)^{r_cs_s}\cdot e(g,h)^{r_s}\\&=e(g,h)^{r_c+r_s}\end{aligned}\quad(2)$$

由等式(1)和等式(2)可以得出 $T_{c2}=T_{s2}$.又因为 $T_{c3}=T_{s3}=e(g,g)^{r_cr_s}$,$T_{c4}=T_{s4}=u^{(x_cx_s+x_cs_s+s_cx_s+s_cs_s)}$,通过使用会话密钥演化函数 H,我们可以得出 $sk=sk_c=sk_s$,即协议诚实执行结束后可以协商出共同的会话密钥 sk (如图 1 所示).

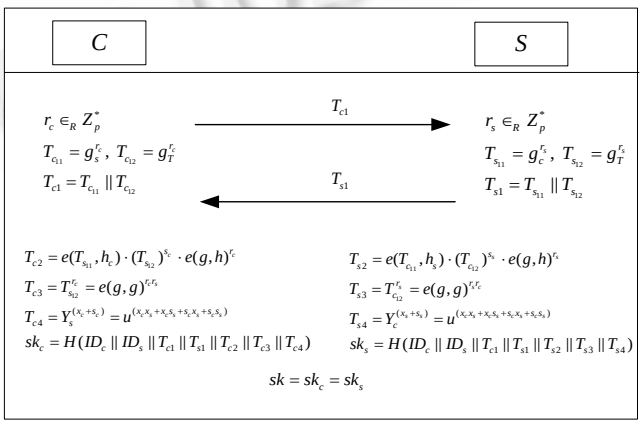

Fig.1 Key agreement phase

图1 密钥协商阶段

无会话密钥托管特性:PKG 知道实体 C 和实体 S 的部分长期密钥, 能计算 $e(g,h)^{r_c}=e(T_{c_{11}},h_s)\cdot(T_{c_{12}})^{s_s}$ 以及 $e(g,h)^{r_s}=e(T_{s_{11}},h_c)\cdot(T_{s_{12}})^{s_c}$,所以 PKG 可以计算 T_{c2} 或者 T_{s2}.同时 PKG 知道系统参数$\langle \alpha, ID_c, ID_s \rangle$,所以它可以通过 $(\alpha-ID_c)\cdot(\alpha-ID_c)^{-1}=1 \bmod p$ 计算 $(\alpha-ID_c)^{-1}$,并通过 $(\alpha-ID_s)\cdot(\alpha-ID_s)^{-1}=1 \bmod p$ 计算 $(\alpha-ID_s)^{-1}$,从而它可以计算 $g^{r_s}=(T_{s11})^{(\alpha-ID_c)^{-1}}$, $g^{r_c}=(T_{c11})^{(\alpha-ID_s)^{-1}}$,进而计算 $T_{c3}=T_{s3}=e(g,g)^{r_c r_s}=e(g^{r_c},g^{r_s})$.但是 T_{c4} 和 T_{s4} 的计算必须借助于实体 C 和实体 S 秘密产生的部分私钥 x_c 和 x_s,对此 PKG 是不可知的,这意味着 PKG 不能有效计算最终的会话密钥 sk_c 或者 sk_s.也就是说, PKG 不能有效恢复实体之间建立的会话密钥,从而无法被动托管.

4 新方案的安全性分析

我们按照上文所提出的认证密钥协商协议应具备的一些安全属性进行了逐一分析.分析表明,新的认证密钥协商方案全部满足安全要求.并且方案可以有效抵抗一些安全攻击,如密钥复制攻击和公钥替换攻击.

已知会话密钥安全性.本方案中每次会话密钥协商的实例中, $r_c\in Z_q^*$ 和 $r_s\in Z_q^*$ 是由实体 C 和实体 S 分别随机选取的临时秘密密钥,即使是协议的不同实例执行中参与实体保持相同(即实体 C 和实体 S 多次执行协议),协议执行结果所产生的共享会话密钥也会不同.这是一般认证密钥协商协议引入短期临时密钥的重要原因.密钥复制攻击可以被认为是对已知会话密钥安全的一种违背,我们将在无密钥控制部分进行分析.

前向安全性与完美前向安全性.本方案满足完美前向安全性.因为即使攻击者拥有两个实体的长期私钥可以计算 $T_{c2}, T_{s2}, T_{c4}, T_{s4}$,但是他无法有效计算 T_{c3} 或者 T_{s3},计算 T_{c3} 或者 T_{s3} 面临 CDH 困难问题.

PKG 前向安全性.无密钥托管也就是 PKG 前向安全性,是无证书密码方案隐含的安全属性.PKG 主密钥 α 的泄露不会使得攻击者(包括 PKG 本身)有效获得以前产生的会话密钥.本方案中,虽然攻击者可以通过掌握 PKG 的主密钥计算获得实体的部分私钥信息,但是为了计算已建立的会话密钥,攻击者需要获得一次会话中两方实体的长期私钥和临时私钥信息方能奏效.

抗密钥泄露伪装.本协议能有效抵抗密钥信息泄露伪装攻击.考虑攻击者试图通过持有实体 S 的长期私钥信息而声称是实体 C 和实体 S 进行会话密钥协商的情况.首先在不替换实体 S 的公钥信息情况下, 实体 S 在验证实体 C 的公钥时会发现冒用自己的公钥信息.如果攻击者试图通过替换实体 S 的公钥信息达到伪装成功的目的,它在未知实体 C 的私钥信息情况下无法有效计算 T_{c2} 或者 T_{s2},这是因为攻击者计算 T_{c2} 需要知道实体 C 的密钥或者计算 T_{s2} 需要知道 S 选取的 r_s.这一点是本方案所基于的加密方案本身所具有的特点决定的.

抗未知密钥共享.假设攻击者 E 试图使得实体 C 相信正在和实体 S 建立共享会话密钥,而实体 S 却认为会话密钥的建立是与实体 E 完成的,那么攻击者 E 必须强迫实体 C 和实体 S 共享相同的秘密才能使得攻击成功.然而实体 C 和实体 S 永远不会共享一个相同的会话密钥, 因为两方都是用对方真实的身份信息参与到共享会话密钥产生过程中的.

无密钥控制与密钥完整性.在会话密钥产生过程中,两方实体都是通过独立随机选取的短期临时密钥信息 $r_c\in Z_q^*$ 和 $r_s\in Z_q^*$ 来产生共享会话密钥的,任何一方都无法控制对方短期临时密钥的随机选取,从而任何一方都无法独立强迫最终的共享会话密钥值为一个特定的值.因而本方案满足一般意义上的无密钥控制.

密钥复制攻击是影响无密钥控制安全属性的一种中间人攻击形式[21].本方案中,对交互消息的任何篡改都将导致密钥协商的两方分别计算产生不同的会话密钥,也就是说交互消息的任何篡改都将无法协商出共同的会话密钥.一个第三方的攻击者可能通过选取合适的 k 用 $T'_{c1}=T_{c1}^k$ 替换 T_{c1},用 $T'_{s1}=T_{s1}^k$ 替换 T_{s1} 来发起密钥复制攻击,强迫 $T_{c3}=T_{s3}$,但这将导致 $T_{c2}\neq T_{s2}$,从而使得攻击无效.

已知会话相关临时秘密信息安全性.本方案中的攻击者即使是获取了在任何一次会话中用于会话密钥建立的两方短期临时密钥信息 r_c 和 r_s,并有效计算 T_{c2}(或 T_{s2})和 T_{c3}(或 T_{s3}),但在不掌握两方实体长期私钥的情况下无法有效计算 T_{c4}(或 T_{s4}),从而无法计算最终的会话密钥.

消息独立性.本方案作为一个两方单轮隐式认证密钥协商协议,交互消息 T_{c1} 不依赖于 r_s, T_{s1} 不依赖于 r_c,从

而交互消息的产生完全独立于对方.

另外一个需要考虑的攻击形式为公钥替换攻击,这是无证书方案中可能存在的一种攻击形式.本文构造的无证书密钥协商协议在这方面的安全性依赖于所基于的PCHL-CL-PKE无证书公钥加密方案的特点,正如抗密钥泄露伪装部分分析的情况一样,公钥替换攻击不能奏效.

表1给出了本方案与目前作者已知的其他几个文献[2,14,13,12,11]中提出的两方无证书认证密钥协商方案和一个基于身份加密方案构造的两方认证密钥协商方案(文献[9])在几个重要的可满足安全属性方面的比较.从比较结果可以看出,新方案具有更高的安全性. (PFS:完美前向安全; KCI-R:抗密钥泄露伪装; UKS-R:抗未知密钥共享; KSSTIS:已知会话相关临时秘密信息安全; KRA-R:抗密钥复制攻击).

Table 1 Comparisons of security attributes

表 1 安全属性比较

Schemes	Security attributes				
	PFS	KCI-R	UKS-R	KSSTIS	KRA-R
Scheme[2]	√	√	√	×	×
Scheme[14]	√	×	√	√	×
Scheme[13]	×	√	√	×	×
Scheme[12]	√	×	√	×	×
Scheme[11]	√	×	√	×	√
Scheme[9]	×	√	√	×	√
New scheme	√	√	√	√	√

Lippold[15]等人最近提出了针对无证书认证密钥协商方案的强安全敌手模型指出在无证书方案中所涉及实体的三种密钥(包括PKG产生的部分长期私钥,实体产生的长期私钥,实体产生的会话短期临时私钥)只要有至少一个未被泄露,方案都应保持安全.可以看出前述方案连基本安全属性都不能很好的满足,更不能满足这样的强安全性.新方案在任意组合私钥泄露的情况下分析可知,仍能保持安全(限于篇幅,省略具体分析).

5 新方案的计算效率分析

密钥协商方案的有效性主要用计算和通信成本来衡量.通信成本指的是一次协议执行所需的消息数量(或比特数量), 由于都是两方单轮方案,通信成本比较意义不大.计算成本指的是每个实体为了最终协商会话密钥所需的所有算数运算数量.表 2 给出了新方案和目前作者已知的几个两方无证书认证密钥协商方案[2,14,13,12,11]和一个基于身份的两方认证密钥协商方案(文献[9])在在线操作的计算成本比较.如果针对两方实体确定的情况下进行多次密钥协商,则Exponentiation运算个数可以减少到 5 个.从比较可以看出,新方案提高安全性后虽然计算效率并非最优,但是仍保持了较好的计算效率.Lippold[15]等人最近提出了针对无证书认证密钥协商方案的强安全敌手模型并设计了一个在该模型下可证安全的方案, 该方案需要每方进行 10 个Pairing运算,5 个Scalar multiplication运算以及 5 个Exponentiation运算,显然计算成本是非常高的.

Table 2 Comparisons of computational costs

表 2 计算成本比较

Schemes	Computational operations		
	Pairing	Scalar multiplication	Exponentiation
Scheme[2]	4	2	1
Scheme[14]	1	3	0
Scheme[13]	1	2	1
Scheme[12]	2	2	1
Scheme[11]	2	3	1
Scheme[9]	1	0	4
New scheme	1	0	6*

Note. Computational costs of Pairing and Scalar multiplication are higher than that of Exponentiation.

6 总结与展望

本文基于一个可证安全的无证书加密方案构造了一个安全有效的无证书两方认证密钥协商协议,并给出

了详细的安全属性分析,同时与目前已知的几个基于无证书的认证密钥协商方案进行了安全性和计算效率比较.分析表明,新方案满足完美前向安全性,PKG 前向安全性以及其他一些已知的安全属性,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,已知会话相关临时秘密信息安全性,消息独立性等.与其他同类方案相比,具有更高的安全性并保持较好的计算效率.

目前基于无证书的认证密钥协商方案安全性分析还基本限于非形式化描述,迫切需要合适的安全模型以及实现可证安全[15].基于传统公钥密码和基于身份的两方认证密钥协商协议已经出现较为成熟的敌手安全模型[23−25],并有大量方案在这些不同敌手安全模型下得到在随机预言模型或标准模型下的安全证明.不同的敌手模型赋予攻击者的能力有强有弱,从而表明方案的安全性有高有低.可证安全正在朝着强敌手安全模型,弱计算困难性假设和标准安全证明的方向发展.目前基于无证书方案构造的认证密钥协商方案还很少,而且该背景下敌手安全模型的研究以及可证安全方案鲜有文献涉及.下一步将对本方案涉及的基于无证书公钥密码体制下的敌手安全模型以及对本方案进行合适敌手安全模型下的可证安全展开深入研究.

致谢 对匿名审稿人对本文进行的仔细阅读以及所提出的宝贵修改意见,作者在此表示衷心的感谢.

References:

[1] Shamir A. Identity-based cryptosystems and signature schemes. In: Blakley GR, Chaum D, eds. Proc. of the Advances in Cryptology (CRYPTO 1984). LNCS 196, Berlin/Heidelberg: Springer-Verlag, 1984. 47−53.

[2] Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: Laih CS, ed. Proc. of the Advances in Cryptology (ASIACRYPT 2003). LNCS 2894, Berlin/Heidelberg: Springer-Verlag, 2003. 452−473.

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

[4] Law L, Menezes A, Qu M, Solinas J, Vanstone S. An efficient protocol for authenticated key agreement. Designs, Codes and Cryptography, 2003,28(2):119−134.

[5] Jeong IR, Katz J, Lee DH. One-Round protocols for two-party authenticated key exchange. In: Jakobsson M, Yung M, Zhou J, eds. Proc. of the Applied Cryptography and Network Security (ACNS 2004). LNCS 3089, Berlin/Heidelberg: Springer-Verlag, 2004. 220−232.

[6] Ustaoglu B. Obtaining a secure and efficient key agreement protocol from (H)MQV and NAXOS. Designs, Codes and Cryptography, 2008,46(3):329−342.

[7] Chen L, Cheng Z, Smart NP. Identity-Based key agreement protocols from pairings. Int'l Journal of Information Security, 2007,6(4):213−241.

[8] Dent AW. A survey of certificateless encryption schemes and security models. Int'l Journal of Information Security, 2008, 7(5):349−377.

[9] Wang SB, Cao ZF, Dong XL. Provably secure identity-based authenticated key agreement protocols in the standard model. Chinese Journal of Computers, 2007,30(10):1842−1854 (in Chinese with English abstract).

[10] Wang XF, Chen Y, Xiao GZ, Analysis and improvement of an ID-based authenticated key agreement protocol. Journal on Communications, 2008,29(12):16−21 (in Chinese with English abstract).

[11] Mandt TK, Tan CH. Certificateless authenticated two-party key agreement protocols. In: Okada M, Satoh I, eds. Proc. of the 11th Annual Asian Computing Science Conf. (ASIAN 2006). Secure Software and Related Issues, LNCS 4435, Berlin/Heidelberg: Springer-Verlag, 2008. 37−44.

[12] Wang SB, Cao ZF, Wang LC. Efficient certificateless authenticated key agreement protocol from pairings. Wuhan University Journal of Natural Sciences, 2006,11(5):1278−1282.

[13] Shi YJ, Li JH. Two-Party authenticated key agreement in certificateless public key cryptography. Wuhan University Journal of Natural Sciences, 2007,12(1):71−74.

[14] Wang SB, Cao ZF, Bao HY. Efficient certificateless authentication and key Agreement (CL-AK) for Grid computing. Int'l Journal of Network Security, 2008,7(3):342−347.

[15] Lippold G, Boyd C, Nieto JG. Strongly secure certificateless key agreement. In: Shacham H, Waters B, eds. Proc. of the Pairing-Based Cryptography (PAIRING 2009). LNCS 5671, Berlin/Heidelberg: Springer-Verlag, 2009. 206−230.

[16] Swanson CM. Security in key agreement: two-party certificateless schemes [MS. Thesis]. Waterloo: University of Waterloo, 2008.

[17] Hou MB, Xu QL. Key replicating attack on certificateless authenticated key agreement protocol. In: Luo Q, ed. Proc. of the 2009 Asia-Pacific Conference on Information Processing (APCIP 2009), Vol 2. Los Alamitos: IEEE Computer Society Press, 2009. 574−577.

[18] Park JH, Choi KY, Hwang JY, Lee DH. Certificateless public key encryption in the selective-ID security model (without random oracles). In: Takagi T, Okamoto T, Okamoto E, Okamoto T, eds. Proc. of the Pairing-Based Cryptography (PAIRING 2007). LNCS 4575, Berlin/Heidelberg: Springer-Verlag, 2007. 60−82.

[19] Gentry C. Practical identity-based encryption without random oracles. In: Vaudenay S, ed. Proc. of the Advances in Cryptology (EUROCRYPT 2006). LNCS 4004, Berlin/Heidelberg: Springer-Verlag, 2006. 445−464.

[20] Blake-Wilson S, Johnson D, Menezes A. Key agreement protocols and their security analysis. In: Darnell M, ed. Proc. of the 6th IMA International Conference on Cryptography and Coding. LNCS 1355, Berlin/Heidelberg: Springer-Verlag, 1997. 30−45.

[21] Krawczyk H. HMQV: A high-performance secure Diffie-Hellman protocol. In: Shoup V, ed. Proc. of the Advances in Cryptology (CRYPTO 2005). LNCS 3621, Berlin/Heidelberg: Springer-Verlag, 2005. 546−566.

[22] Mitchell CJ, Ward M, Wilson P. Key control in key agreement protocols. Electronics Letters, 1998,34(10):980−981.

[23] Canetti R, Krawczyk H. Analysis of key exchange protocols and their use for building secure channels. In: Pfitzmann B, ed. Proc. of the Advances in Cryptology (EUROCRYPT 2001). LNCS 2045, Berlin/Heidelberg: Springer-Verlag, 2001. 453−474.

[24] Bellare M, Rogaway P. Entity authentication and key distribution. In: Stinson DR, ed. Proc. of the Advances in Cryptology (CRYPTO 1993). LNCS 773, Berlin/Heidelberg: Springer-Verlag, 1993. 110−125.

[25] LaMacchia B, Lauter K, Mityagin A. Stronge329 security of authenticated key exchange. In: Susilo W, Liu JK, Mu Y, eds. Proc. of the 1st Int'l Conf. on Provable Security (ProvSec 2007). LNCS 4784, Berlin/Heidelberg: Springer-Verlag, 2007. 1−16.

附中文参考文献:

[9] 王圣宝,曹珍富,董晓蕾.标准模型下可证安全的身份基认证密钥协商协议.计算机学报,2007,30(10):1842−1854.

[10] 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.通信学报,2008,29(12):16−21.

侯孟波(1970－),男,山东济南人,博士生,讲师,主要研究领域为密码协议,网络安全.

郭山清(1976－),男,博士,副教授,主要研究领域为信息安全.

徐秋亮(1960－),男,博士,教授,博士生导师,主要研究领域为密码学,信息安全.