◎博士论坛◎

构建无证书的两方认证密钥协商协议

侯孟波,徐秋亮,蒋 瀚
HOU Meng-bo,XU Qiu-liang,JIANG Han

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,JIANG Han.Constructing certificateless-based two-party authenticated key agreement protocol.Computer Engineering and Applications,2010,46(8):1-4.

Abstract: The certificateless-based authenticated key agreement protocols have the advantages of simplicity of managing identities compared to the PKI-based schemes,as well as avoiding the key escrow issues inherited in the identity-based schemes. This paper proposes a two-party certificateless-based authenticated key agreement scheme based on a provably secure certificateless-based public key encryption scheme.The comparisons with other comparable schemes in security and efficiency show that,the new scheme achieves more of the desired security attributes,such as perfect forward secrecy,PKG forward secrecy, known session-specific temporary information secrecy and key escrowless.Meanwhile it keeps the nice computational efficiency.

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

摘 要:基于无证书的认证密钥协商方案相比基于PKI的方案具有身份管理的简单性,同时相比基于身份的方案具有无密钥托管性。基于可证安全的无证书加密方案提出了一个两方认证密钥协商方案.通过与其他方案在安全性和有效性方面的比较,该方案满足更多的安全属性要求,如完美前向安全性,PKG前向安全性,已知会话相关临时秘密信息安全性和无密钥托管等安全特性,同时具有良好的计算有效性。

关键词:认证密钥协商;无证书加密;完美前向安全;私钥生成中心(PKG)前向安全;密钥托管
DOI:10.3778/j.issn.1002-8331.2010.08.001 **文章编号:**1002-8331(2010)08-0001-04 **文献标识码:**A **中图分类号:**TN918.1

1 前言

目前利用公钥密码体制设计认证密钥协商协议主要基于传统公钥密码体制(PKC-based)和基于身份的密码体制(ID-based)。随着无证书密码体制(Certificateless-based)[1]的出现,基于无证书密码体制成为设计认证密钥协商协议的新思路。基于传统公钥证书的认证密钥协商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。基于身份的认证密钥协商方案(该类方案可参阅Chen等人的方案综述,见文献[2])可以直接基于双线性配对技术构造,也可以基于身份基公钥加密方案进行设计。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。基于身份的密码体制需要一个可信的私钥生成中心(Private Key Generator,PKG),通过自己持有的秘密主密钥并根据用户身份产生对应的用户私钥。也就是说PKG掌握着所有用户的长期私钥。而用户在一次具体会话中进行密钥协商时往往通过临时选取短期密钥来构造最终的会话密钥。在这种情况下会话中任一方短期密钥的泄露,都会导致恶意PKG容易计算最终协商的会话密钥。也就是会话密钥可以被动托管。2003年Al-Riyami和Paterson[1]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。该体制也需要一个可信PKG的支持,但是用户的私钥包含两部分,一部分来自于PKG的生成,另一部分来自于自身的生成,从而该类方案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,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具有更多的优势。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(目前

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协议与网络安全;徐秋亮(1960-),男,博士,教授,主要研究领域为密码学与信息安全;蒋瀚(1974-),男,博士,讲师,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:**2010-01-13

已知的文献包括[1,3-6]),设计和分析该类方案具有较好的理论和实用价值。

2003 年,Al-Riyami 和 Paterson[1]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,但是该方案的计算开销较大。后来 Mandt 和 Tan[4]提出了一个基于 Bilinear Diffie-Hellman 计算困难性假设的两方无证书认证密钥协商方案,该方案存在密钥泄露伪装攻击和已知会话相关临时信息安全攻击[7]。Wang 等人[3]也提出了一个类似方案,同样容易遭受密钥泄露伪装攻击。Shi 和 Li[5]基于 Libert 和 Quisquater[8]的无证书公钥加密方案(称之为 LQ 方案)构造了另一个认证密钥协商方案,Swanson[7]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从而导致协议隐式认证失败。该方案也容易遭受密钥复制攻击。最近 Wang 等人[6]提出了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,但是该方案不能有效抵抗密钥泄露伪装攻击和密钥复制攻击。

该文在 LQ 无证书加密方案思想的启发下构造了一个安全有效的两方无证书认证密钥协商协议并给出安全性和计算效率分析。与其他同类方案的分析比较表明,新方案满足所有目前已知的安全属性要求,同时保持了良好的计算有效性。

2 预备知识

2.1 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[9]:

(1)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。

(2)前向安全性(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。

(3)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。

(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。

(5)无密钥控制与密钥完整性。参与实体的任何一方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[10],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选择它的短期临时密钥,交互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。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,也就是说第三方攻击者的主动攻击行为不应破坏最终会话密钥的完整性[11]。

(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 完成密钥协商。

(7)已知会话相关临时秘密信息安全性[4]。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[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。

2.2 双线性配对

文中协议执行双方需要依赖于双线性配对的运算。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(双线性配对)e 定义为 $e:G_1\times G_1\rightarrow G_2$ 满足以下三个属性:

(1)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;

(2)非退化:$e(P,P)\neq 1$,1 是 G_2 的单位元;

(3)可计算:如果任意 $P,Q\in G_1$,计算 $e(P,Q)\in G_2$ 可在多项式时间里完成。

2.3 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 1 Computational Diffie-Hellman(CDH)假设: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 Bilinear Inverse Diffie-Hellman(BIDH)假设:对 $\forall a,b\in Z_q^*$,P 是 G_1 的生成元,给定 aP 和 bP,计算 $e(P,P)^{a^{-1}b}$ 是困难的。

定义 3 p-Bilinear Diffie-Hellman Inversion(p-BDHI)假设:给定$<P,\alpha P,\alpha^2 P,\cdots,\alpha^p P>\in G_1^{p+1}$,计算 $e(P,P)^{1/\alpha}\in G_2$ 是困难的。

3 LQ 无证书加密方案回顾

2007 年 Libert 和 Quisquater[8]提出了一个安全性依赖于 p-BDHI 困难性问题的无证书公钥加密方案。该方案可以认为是传统 ElGamal 类加密方案和基于身份的公钥方案的有效结合。方案包括如下几个部分:

系统建立:PKG 产生一系列系统公共参数$<k,k_0,q,n,G_1,G_2,P,P_{pub},e,g,H_1,H_2,H_3,M,C>$,其中

k,k_0:安全参数;

q:k 比特大素数;

G_1,G_2:两个阶为 q 的循环群;

P:$P\in G_1$,G_1 的一个生成元;

P_{pub}:PKG 的公开钥,$P_{pub}=sP(s\in_R Z_q^*$,是 PKG 的主密钥);

e:双线性映射关系,$e:G_1\times G_1\rightarrow Z_q^*$;

g:$g=e(P,P)\in G_2$;

H_1:散列函数 $H_1:\{0,1\}^*\rightarrow Z_q^*$;

H_2:散列函数 $H_2:G_2^2\rightarrow\{0,1\}^{n+k_0}$;

H_3:散列函数 $H_3:\{0,1\}^*\rightarrow Z_q^*$;

M:明文空间 $M:=\{0,1\}^n$(n 是 M 的比特长度);

C:密文空间 $C:=G_1\times\{0,1\}^{n+k_0}$。

用户部分私钥生成:输入用户 A 的身份 $ID_A\in\{0,1\}^*$,输出用户 A 的部分私钥 $d_A=(H_1(ID_A)+s)^{-1}P\in G_1$。

用户秘密值生成:给定系统公共参数和用户身份作为输入,算法随机选取 $x_A\in_R Z_q^*$ 作为用户 A 的秘密值。

用户完全私钥生成:给定系统公共参数,用户 A 的部分私钥 $d_A\in G_1$ 和秘密值 $x_A\in_R Z_q^*$ 作为输入,算法输出二元组 $S_A=(x_A,d_A)\in Z_q^*\times G_1$ 作为用户 A 的完全私钥。

用户公钥生成:算法输入系统公共参数和用户的秘密值 $x_A\in_R Z_q^*$,输出用户 A 的公钥 $y_A=g^{x_A}\in G_2$。

加密过程:加密者使用身份 $ID_A\in\{0,1\}^*$ 和用户公钥 $y_A=g^{x_A}$ 对明文消息 $m\in\{0,1\}^n$ 进行加密。首先检查 $y_A^q=1_{G_2}$,随机选择 $\sigma\in_R\{0,1\}^{k_0}$,计算 $r=H_3(m\|\sigma\|y_A\|ID_A)\in Z_q^*$,密文为:

$$C=<rH_1(ID_A)P+rP_{pub},(m\|\sigma)\oplus H_2(g^r\|y_A^r)>$$

解密过程:给定密文 $C=<c_1,c_2>$,计算 $\omega=e(c_1,d_A)$,$(m\|\sigma)=c_2\oplus H_2(\omega\|\omega^{x_A})\in\{0,1\}^{n+k_0}$。接受明文 m 当且仅当

$$c_1=r(H_1(ID_A)P+P_{pub})\quad(r=H_3(m\|\sigma\|y_A\|ID_A)\in Z_q^*)$$

一致性验证:加解密过程是正确的,因为

$$e(rH_1(ID_A)P+rP_{pub},(H_1(ID_A)+s)^{-1}P)=e(P,P)^r$$

4　新的两方无证书认证密钥协商方案

假定用户 A 和用户 B 是协议执行的两方实体,其身份分别为 ID_A 和 ID_B,方案包括如下几个部分。

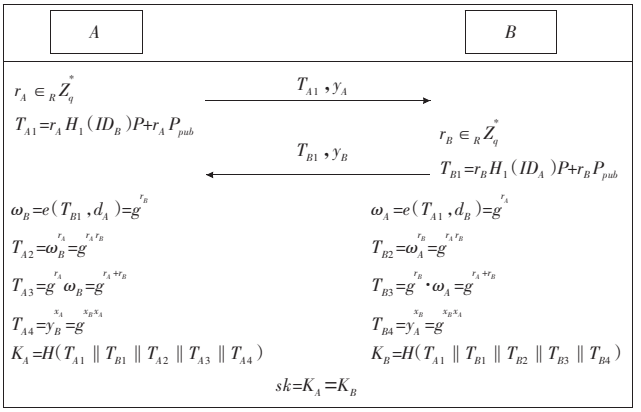

图 1　新的两方无证书认证密钥协商协议

系统建立:与 LQ 无证书加密方案相同,另外定义一个会话密钥演化算法 $H:\{0,1\}^*\rightarrow\{0,1\}^{k_1}$,其中 $k_1=|sk|$,sk 是协议一次执行后协商出的会话密钥。

用户密钥生成:对一个身份为 ID 的用户,PKG 产生用户部分私钥 $d_{ID}=(H_1(ID)+s)^{-1}P$;用户 ID 自己随机选取 $x_{ID}\in_R Z_q^*$ 作为他的秘密值。$y_{ID}=g^{x_{ID}}$ 就是他的公开钥,关联的完全私钥为 $S_{ID}=<x_{ID},d_{ID}>$。对用户 A 和 B 而言,他们的密钥分别为:

$$A:<y_A,S_A>=<g^{x_A},x_A:d_A>;$$

$$B:<y_B,S_B>=<g^{x_B},x_B:d_B>$$

密钥协商过程:用户 A 和用户 B 分别随机产生临时密钥 $r_A\in Z_q^*$ 以及 $r_B\in Z_q^*$,并执行单轮消息交互如下(如图 1 所示):

$$A\rightarrow B:<T_{A1},y_A>,T_{A1}=r_AH_1(ID_B)P+r_AP_{pub}$$

$$B\rightarrow A:<T_{B1},y_B>,T_{B1}=r_BH_1(ID_A)P+r_BP_{pub}$$

用户 A 和用户 B 分别做如下计算:

$$A:\omega_B=e(T_{B1},d_A)=e(P,P)^{r_Br_A}=g^{r_Br_A}$$

$$T_{A2}=\omega_B^{r_A+1}\cdot g^{r_A}\cdot y_B^{x_A}=g^{r_Ar_B+r_A+r_B+x_Ax_B}$$

$$K_A=H(T_{A1}\|T_{B1}\|T_{A2})\qquad(1)$$

$$B:\omega_A=e(T_{A1},d_B)=e(P,P)^{r_Ar_B}=g^{r_Ar_B}$$

$$T_{B2}=\omega_A^{r_B+1}\cdot g^{r_B}\cdot y_A^{x_B}=g^{r_Ar_B+r_A+r_B+x_Ax_B}$$

$$K_B=H(T_{A1}\|T_{B1}\|T_{B2})\qquad(2)$$

会话密钥一致性验证:从式(1)和(2)可知 $T_{A2}=T_{B2}$,因而一次协议的执行得出的会话密钥 sk 为:

$$sk=K_A=K_B=H(T_{A1}\|T_{B1}\|g^{r_Ar_B+r_A+r_B+x_Ax_B})$$

5　方案分析与比较

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,新提出的认证密钥协商方案满足全部安全要求。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。而且该方案与其他同类方案相比具有更高的安全性,同时具有较好的计算有效性。

5.1　安全属性分析

(1)已知会话密钥安全性。该方案中用户在执行一次协议过程中引入了短期临时密钥 $r_A\in Z_q^*$ 和 $r_B\in Z_q^*$。由于每次协议执行(即使是协议执行用户保持不变)该短期临时密钥都是由用户 A 和 B 独立随机产生并经由会话密钥演化函数参与最终会话密钥的演化过程,从而保证任意历史会话密钥的泄露都不会影响到其他会话密钥的泄露。密钥复制攻击本质上可以认为是对已知会话密钥安全的一种中间人攻击形式,也可以归结为是一种对密钥完整性攻击(具体见(6)的讨论)。

(2)前向安全性与完美前向安全性。该方案中即使参与协议执行的两方用户长期私钥泄露,也不会导致历史会话密钥的泄露。虽然敌手可以通过掌握用户的长期私钥 d_A 和 d_B 计算

$$\omega_A=e(T_{A1},d_B)=e(P,P)^{r_Ar_A}=g^{r_Ar_A}$$

$$\omega_B=e(T_{B1},d_A)=e(P,P)^{r_Br_B}=g^{r_Br_B}$$

以及通过掌握长期私钥 x_A 和 x_B 计算 $g^{x_Ax_B}$,但他无法计算 $g^{r_Ar_B}$,由 ω_A 和 ω_B(g^{r_A} 和 g^{r_B})计算 $g^{r_Ar_B}$ 需要解决 CDH 困难问题。

(3)PKG 前向安全性。无密钥托管性是无证书方案固有的特性,无密钥托管性同时也意味着 PKG 前向安全性。PKG 主密钥的泄露虽然可以导致敌手能够掌握用户的部分长期私钥(d_A 和 d_B),但是会话密钥的产生还关联于用户自主选取的秘密值(x_A 和 x_B),因而 PKG 无法计算 $g^{x_Ax_B}$,这将保证任意敌手(包括恶意的 PKG)都无法计算其他的历史会话密钥。

(4)抗密钥泄露伪装。该方案能有效抵御密钥泄露伪装攻击。考虑敌手在掌握用户 B 的长期私钥情况下试图伪装成用户 A 和真正的用户 B 进行密钥协商的情况,敌手在获得用户 B 的响应消息$<T_{B1},y_B>$后,由于 T_{B1} 是用用户 A 的身份构造的,只能通过掌握用户 A 的私钥信息才能有效计算 ω_B,已知用户 B 的私钥信息是无用的从而无法计算相同的会话密钥。

(5)抗未知密钥共享。假设敌手 E 试图使得用户 A 相信正在与用户 B 协商会话密钥，而用户 B 却认为是与 E 协商的会话密钥。那么敌手 E 要使这样的攻击成功必须强迫 A 和 B 也共享相同的会话密钥。然而用户 A 和用户 B 永远都不可能在未知对方情况下共享相同的会话密钥,因为方案中每方计算会话密钥都需要意定对方的身份信息。

(6)无密钥控制与密钥完整性。协议执行的任一方都是独立随机产生自身的短期临时密钥来参与会话密钥的生成,任一方都不能决定对方短期临时密钥的产生值。该方案为两方一轮消息交互的隐式认证协议,因而只具有一般意义上的无密钥控制安全属性。

密钥复制攻击是第三方攻击者通过篡改交互消息来影响最终会话密钥的生成。虽然可以使得协议执行的合法两方协商密钥,但是协商出的密钥并非合法值,是中间人攻击形式的一种[9,11]。假设在该方案中敌手试图替换交互消息 T_{A1} 为 $T'_{A1}=kT_{A1}$ 和替换 T_{B1} 为 $T'_{B1}=kT_{B1}$,这将导致

$$T_{A2}=\omega_B^{k(r_A+1)}\cdot g^{r_A}\cdot y_B^{x_A}=g^{kr_Ar_B+r_A+kr_B+x_Ax_B}$$

$$T_{B2}=\omega_A^{k(r_B+1)}\cdot g^{r_B}\cdot y_A^{x_B}=g^{kr_Ar_B+kr_A+r_B+x_Ax_B}$$

要使得 $T_{A2}=T_{B2}$,在 $r_A\neq r_B$ 的情况下,唯一的选择是 $k=1$。其他选择都将使得合法两方无法协商相同的会话密钥。所以密钥复制攻击对该方案无效。

(7)已知会话相关临时秘密信息安全性。该方案中协议执行的两方用户短期临时密钥的泄露不会影响到会话密钥的安全性。因为敌手即使获得了协议执行中选取的短期临时密钥 r_A 和 r_B,这虽然可以使得敌手能够计算 $g^{r_Ar_B+r_A+r_B}$,但无法有效计算 $g^{x_Ax_B}$,从而无法计算最终产生的会话密钥。

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。该方案中任何替换公钥的行为将导致 $y_B^{x_A}\neq y_A^{x_B}$,从而无法协商相同的会话密钥。

表 1 给出了该方案与目前作者已知的其他几个文献[1,3-6]中提出的两方无证书认证密钥协商方案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)。

表 1　安全属性比较

协议	安全属性				
	PFS	KCI-R	UKS-R	KSSTIS	KRA-R
方案[1]	√	√	√	×	×
方案[6]	√	×	√	√	×
方案[5]*	×	√	√	×	×
方案[3]	√	×	√	×	×
方案[4]	√	×	√	×	√
新方案	√	√	√	√	√

注:* 表示还易遭受中间人攻击。

Lippold[13]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。

5.2　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通信实体为了最终协商会话密钥所需的所有运算数量。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[1,3-6]在线操作的计算成本比较。新方案提高安全性后计算效率并非最优,但是仍保持了较好的计算效率。

表 2　计算有效性比较

协议	计算操作		
	对运算	点乘运算	指数运算
方案[1]	4	2	1
方案[6]	1	3	0
方案[5]	1	2	1
方案[3]	2	2	1
方案[4]	2	3	1
新方案	1	2	3

6　结束语

在一个可证安全的无证书加密方案基础上构造了一个无证书两方认证密钥协商协议，通过详细的安全属性分析和与目前已知的几个类似方案进行的安全性和计算效率比较表明，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,而且在保持良好计算效率的同时具有更高的安全性。

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[11-12,14],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。目前基于无证书方案构造的认证密钥协商方案还很少,安全性分析还基本限于非形式化描述,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,迫切需要合适的安全模型以及实现可证安全[13]。下一步将对该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该方案进行可证安全深入研究。

参考文献:

[1] Al-Riyami S S,Paterson K G.Certificateless public key cryptography[C]//Laih C S.LNCS 2894:Advances in Cryptology-ASIACRYPT'03.Heidelberg:Springer-Verlag,2003:452-473.

[2] Chen L,Cheng Z,Smart N P.Identity-based key agreement protocols from pairings[J].International Journal of Information Security,2007,6(4):213-241.

[3] Wang S B,Cao Z F,Wang L C.Efficient certificateless authenticated key agreement protocol from pairings[J].Wuhan University Journal of Natural Sciences,2006,11(5):1278-1282.

[4] Mandt T K,Tan C H.Certificateless authenticated two-party key agreement protocols[C]//Okada M,Satoh I.LNCS 4435:Advances in Computer Science-ASIAN 2006,Secure Software and Related Issues.Heidelberg:Springer-Verlag,2008:37-44.

[5] Shi Y J,Li J H.Two-party authenticated key agreement in certificateless public key cryptography[J].Wuhan University Journal of Natural Sciences,2007,12(1):71-74.

(下转 28 页)