一种改进的无证书两方认证密钥协商协议

周彦伟[1),2),3)] 杨 波[1),2),3)] 张文政[2)]

[1)](陕西师范大学计算机科学学院 西安 710119)

[2)](保密通信重点实验室 成都 610041)

[3)](中国科学院信息工程研究所信息安全国家重点实验室 北京 100093)

摘 要 在不使用双线性映射的前提下,文中提出可证安全的高效无证书两方认证密钥协商协议,并在 *eCK* 安全模型和随机谕言机模型下基于离散对数困难问题证明了文中协议的安全性和不可伪造性;与目前已有的同类协议相比,文中协议具有更高的计算效率,同时具有已知密钥安全、完美的前后向安全性、抵抗未知密钥共享和密钥泄露伪装攻击等安全属性.文中协议更适用于基于身份的公钥系统,并在带宽受限的通信环境(如无线传感器网络、Ad-Hoc 网络等)中具有较好的推广性.

关键词 无证书密钥协商;可证明安全;离散对数;无双线性映射;*eCK* 安全模型

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2017.01181

An Improved Two-Party Authenticated Certificateless Key Agreement Protocol

ZHOU Yan-Wei[1),2),3)] YANG Bo[1),2),3)] ZHANG Wen-Zheng[2)]

[1)](*School of Computer Science, Shaanxi Normal University, Xi'an* 710119)

[2)](*Science and Technology on Communication Security Laboratory, Chengdu* 610041)

[3)](*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093)

Abstract Based on discrete logarithm (DL) problem, this paper proposes a safely authenticated and efficient two party certificateless key agreement protocol without using the bilinear pairings, which is provably secure and unforgeability in the *eCK* security model and random oracle model (ROM) under the DL assumption. Compared with other similar protocols, this one is more efficient and also has known key security, perfect forward and backward secrecy, resistance to unknown key-share attacks and key-compromise impersonation attacks, etc. It is more suitable for the identity-based public key cryptography, and has better popularization in the restricted bandwidth of the communication environment (e.g. wireless sensors networks, Ad-Hoc networks, etc.).

Keywords certificateless key agreement; provably security; discrete logarithm; without bilinear pairing; *eCK* security model

收稿日期:2015-10-05;在线出版日期:2016-01-18.本课题得到国家自然科学基金(61272436,61402275,61303092,61572303)、中国科学院信息工程研究所信息安全国家重点实验室开放课题(2015-MS-10)、保密通信重点实验室基金(9140C110206140C11050)、中央高校基本科研业务费专项资金(GK201504016)及陕西师范大学优秀博士论文项目(X2014YB01)资助.**周彦伟**,男,1986 年生,博士研究生,主要研究方向为密码学、匿名通信技术等.E-mail:zyw_snnu@foxmail.com.**杨 波**(通信作者),男,1963 年生,博士,教授,博士生导师,陕西省"百人计划"特聘教授,主要研究领域为信息安全、密码学等.E-mail:byang@snnu.edu.cn.**张文政**,男,1966 年生,研究员,主要研究领域为信息安全等.

1 引 言

公钥加密机制是信息安全领域的关键技术,然而传统基于证书的密码体制中,由于证书保证了持有人与公钥间的对应关系,故涉及证书的管理、颁发和撤销等操作,导致证书的管理过程复杂且代价极高.基于身份的公钥密码体制(Identity-Based Public Key Cryptography,ID-PKC)[1]改进了传统公钥密码体制中证书管理的问题.ID-PKC 中由于身份信息(如姓名、电子邮箱等)直接被作为公钥使用,使得公钥无需与证书绑定;而用户的私钥由可信第三方密钥生成中心(Key Generation Center,KGC)负责生成,因此恶意的 KGC 具备伪造任意用户的合法密文或替代用户进行解密的能力,即 ID-PKC 存在密钥托管的不足,该不足制约了 ID-PKC 在实际中的应用.为了克服 ID-PKC 的密钥托管不足,无证书公钥密码系统(Certificateless Public Key Cryptography,CL-PKC)[2]被提出,CL-PKC 中,依然存在拥有系统主密钥的 KGC,KGC 根据用户的身份和系统主密钥为用户生成部分私钥;用户基于 KGC 为其计算的部分私钥和随机选取的秘密值生成完整的私钥;公钥由用户的秘密值、身份和系统参数计算得出,CL-PKC 中用户参与其私钥的生成,增强了私钥生成过程中用户的自主性,很好地解决了 ID-PKC 的密钥托管问题.

国内外研究者相继提出了不同的无证书两方密钥协商协议[3-22],其中文献[3-5]中的协议都不能抵抗密钥泄露伪装攻击或临时私钥泄露产生的攻击,文献[6-8]分别介绍了针对上述方案的具体攻击算法;相较于指数运算和点乘运算,双线性运算是更为耗时的运算①,由于协议[9-14,20-21]都是基于双线性映射构建的,因此运算量较大,均存在计算效率低的不足;为提高协议的执行效率,无双线性运算的无证书两方密钥协商协议[15-19]相继被提出,但是文献[17]指出协议[15-16]均不安全;虽然文献[19]的协议相较于其他方案而言具有较高的计算效率,但该方案的安全性是在较弱的安全模型 mBR(modified Bellare-Rogaway)模型下进行证明的,分析发现文献[18-19]中的协议易受到 A_I 类敌手的伪造攻击,无法满足其所声称的对此类敌手不可伪造性攻击的抵抗;协议[17]是一个可证安全的无证书两方密钥协商协议,并在 eCK(extended Canetti-Krawczyk)强安全模型下证明了方案的安全性,但该方案存在计算效率低的不足;文献[20]提出了能同时满足前向安全性和无密钥托管等安全属性的无证书两方密钥协商协议,由于仅需进行 1 轮的消息通信,该协议的执行效率较高;文献[21]基于数字签名技术提出了两方无证书密钥协商协议,并分析了协议所具有的私钥泄露安全等相关安全属性;遗憾的是文献[22]分析发现文献[20-21]中的协议都无法满足其所声称的安全性.

由于文献[22]是从消息泄露的角度出发对文献[20-21]进行安全性分析的;因此本文从安全模型的敌手类型出发,在无消息泄露的前提下,基于公开信息和敌手自身已有的攻击能力构造具体的伪造性攻击算法,证明协议[20]无法满足其所声称的对 $\mathcal{A}_I$ 类敌手的不可伪造性,$\mathcal{A}_I$ 类敌手对文献[18-19]中协议的伪造攻击算法与文献[20]的相关算法的构造相类似,本文以文献[20]为例详细介绍.

针对现有方案[15-21]所存在的不足,本文提出可证安全的高效无证书两方认证密钥协商协议,并分别在 eCK 强安全模型和随机谕言机模型下基于离散对数困难问题的困难性证明了本文密钥协商协议的安全性和不可伪造性;此外该协议还具有完美的前后向安全性、抵抗重放攻击、抗伪造性攻击和无密钥托管等安全属性,相较于现有的无证书密钥协商协议,本文协议具有较高的计算和通信效率.

2 相关基础知识

2.1 相关困难问题

离散对数(Discrete logarithm,DL)问题.令 P 是阶为大素数 q 的循环群 G 的一个生成元;给定 P 和 $cP\in G$,对任意未知的 $c\in Z_q^*$,DL 问题的目标是计算 c.算法 $\mathcal{A}$ 在概率多项式时间内成功解决 DL 问题的概率定义如下:

$$Adv^{DL}(\mathcal{A})=Pr[A(P,cP)=c\,|\,c\in Z_q^*],$$

其中概率来源于算法 $\mathcal{A}$ 的随机选择及 c 在 Z_q^* 上的随机选取.

定义 1. DL 假设.对于任意的多项式时间算法 $\mathcal{A}$ 概率 $Adv^{DL}(\mathcal{A})$ 是可忽略的.

① MIRACL. Multiprecision integer and rational arithmetic C/C++ library. http://indigo.ie/mscott/

计算性 Diffie-Hellma(CDH)问题. 令 P 是阶为大素数 q 的循环群 G 的一个生成元；对于任意未知的 $a,b\in Z_q^*$，已知 $P,aP,bP\in G$，CDH 问题的目标为计算 abP. 算法 $\mathcal{A}$ 在概率多项式时间内成功解决 CDH 问题的概率定义如下：

$Adv^{\mathrm{CDH}}(\mathcal{A})=Pr[\mathcal{A}(P,aP,bP)=abP\,|\,a,b\in Z_q^*]$，其中，概率来源于算法 $\mathcal{A}$ 的随机选择及 a,b 在 Z_q^* 上的随机选取.

定义 2.　CDH 假设. 对于任意的多项式时间算法 $\mathcal{A}$ 概率 $Adv^{\mathrm{CDH}}(\mathcal{A})$ 是可忽略的.

2.2　安全属性及安全模型

文献[13]详细介绍了认证密钥协商协议需满足的协商密钥安全性、抵抗密钥泄露伪装攻击和会话密钥托管等相关安全属性. 参照文献[19]所定义的安全模型，无证书密钥协商协议将面临两种类型的敌手攻击，将这两种敌手分别简写为 $\mathcal{A}_{\mathrm{I}}$ 和 $\mathcal{A}_{\mathrm{II}}$ 两类.

$\mathcal{A}_{\mathrm{I}}$：此类敌手无法掌握系统的主密钥，但可利用合法用户的公钥完成对密钥协商协议安全性的攻击，即具有替换合法用户公钥的能力；则 $\mathcal{A}_{\mathrm{I}}$ 类敌手为恶意的用户.

$\mathcal{A}_{\mathrm{II}}$：此类敌手可掌握系统的主密钥，但其不具有替换合法用户公钥的能力；则 $\mathcal{A}_{\mathrm{II}}$ 类敌手为恶意的 KGC.

eCK 安全模型[17]中将会话的相应参与者形式化为谕言机；攻击者具有执行 *Send*，*Reveal*，*Corrupt* 和 *Test* 等询问请求的能力；并且攻击者在相应的攻击游戏结束后输出对会话密钥的一个猜测. 通过下述敌手与挑战者间的游戏来定义密钥协商协议的安全性；并且在该游戏中，敌手可自适应的对谕言机进行查询.

令 $\Pi_{i,j}^S$ 和 $\Pi_{j,i}^S$ 为第 S 次执行协议时的两个参与者，其中 i 和 j 为用户标号，即表示第 i 个用户 ID_i 和第 j 个用户 ID_j.

密钥协商游戏包 2 个阶段，在第 1 个阶段中，攻击者可自适应地进行 *Send*，*Reveal* 和 *Corrupt* 询问. 相关询问的具体执行及新鲜参与者的定义详见文献[17]，本文不再赘述.

第 1 阶段的询问结束后，攻击者随机选取新鲜参与者 $\Pi_{i,j}^S$，并对其执行 $Test(\Pi_{i,j}^S)$ 请求，获得该请求的相应输出消息.

$Test(\Pi_{i,j}^t)$：当 $\Pi_{i,j}^S$ 是新鲜参与者时，挑战者选取随机数 $b\in\{0,1\}$，并根据 b 的取值返回相应的应答. 若 $b=0$，则输出相应的会话密钥；否则，输出会话密钥空间中的一个随机值.

攻击者收到 $Test(\Pi_{i,j}^t)$ 询问的相应输出后，可自适应地进行 *Send*，*Reveal* 和 *Corrupt* 询问，但不能对参与者 $\Pi_{i,j}^S$ 进行 *Reveal* 询问，不能对与 $\Pi_{i,j}^S$ 相匹配的参与者 $\Pi_{i,j}^t$ 进行 *Reveal* 询问；也不能对参与者 j 进行 *Corrupt* 询问. 游戏结束时，攻击者输出 b' 作为对随机数 b 的猜测，若 $b=b'$，则攻击者在攻击游戏中获胜.

综上所述，攻击者 $\mathcal{A}$ 在上述攻击游戏中获胜的优势为 $Adv_{\mathcal{A}}(k)=\left|Pr[b'=b]-\frac{1}{2}\right|$，其中 k 是安全参数.

定义 3.　密钥协商安全. 当一个认证密钥协商协议同时满足下述条件时，则称该协议是安全的认证密钥协商协议.

(1) 若敌手忠实地传送消息，对协议消息不做任何修改，且参与者接受该会话，则参与者协商了相同的会话密钥，并且该会话在密钥空间上服从均匀分布；

(2) 对于任意的多项式时间敌手 $\mathcal{A}$ 在上述游戏中获胜的优势 $Adv_{\mathcal{A}}(k)$ 是可忽略的.

3　Liu 等人方案的安全性分析

本节针对文献[20]所提出的方案构造具体的不可伪造性攻击算法，证明该方案不具备其所声称的对 A_{I} 类敌手的不可伪造性.

令用户 Alice 和 Bob 分别为文献[20]中无证书两方密钥协商方案的参与者，则 Alice 的公私钥为 $\langle PK_A=(R_A,X_A),SK_A=(D_A,x_A)\rangle$，Bob 的公私钥为 $\langle PK_B=(R_B,X_B),SK_B=(D_B,x_B)\rangle$.

$\mathcal{A}_{\mathrm{I}}$ 类敌手 $\mathcal{A}_{\mathrm{I}}$ 具有替换合法用户公钥的能力，但其不掌握系统主密钥. 敌手 $\mathcal{A}_{\mathrm{I}}$ 获悉 Alice 的公钥 $PK_A=(R_A,X_A)$ 后，使用伪造公钥替代 Alice 的公钥，并生成伪造的密钥协商信息. 敌手 $\mathcal{A}_{\mathrm{I}}$ 与 Bob 间的具体交互过程如下所示：

① $\mathcal{A}_{\mathrm{I}}$ 获悉 Alice 的公钥 $PK_A=(R_A,X_A)$ 和身份 ID_A 等信息后，计算 $X'_A=-(R_A+yH_1(ID_A,R_A))$，其中 y 为 KGC 计算的系统公钥；

② $\mathcal{A}_{\mathrm{I}}$ 使用 $PK'_A=(R_A,X'_A)$ 代替参与者 Alice 的原始公钥 $PK_A=(R_A,X_A)$，则参与者 Bob 认为

Alice 的公钥就为 $PK'_A=(R_A,X'_A)$.

敌手$\mathcal{A}_1$按下述步骤伪装成 Alice 与参与者 Bob 进行会话密钥协商：

$\mathcal{A}_1$选取随机数 $a\in Z_q^*$，计算 $T_A=aP$、$h'=H_2(T_A\|ID_A\|m)$、$S'=\frac{1}{h'}$. 即生成签名(h',S')，将(ID_A,h',S',m)传递给 Bob.

③Bob 收到消息(ID_A,h',S',m)后，验证密钥协商消息(h',S')的合法性. 若合法性验证通过，则 Bob 通过了对敌手$\mathcal{A}_1$的身份合法性验证，即敌手$\mathcal{A}_1$伪装 Alice 成功.

Bob 收到消息(ID_A,h',S',m)后，密钥协商消息的合法性验证过程如下所示：

①计算 $h'_2=H_1(ID_A,R_A)$；

②计算 $T'_A=S'(X'_A+R_A+yh'_2+h'P)=aP=T_A$；

③由于$T'_A=T_A$，则等式 $h'=H_2(T'_A\|ID_A\|m)$成立，即 Bob 认为签名是由 Alice 生成的合法签名.

因此伪造消息通过了参与者 Bob 的合法性验证，即$\mathcal{A}_1$类敌手$\mathcal{A}_1$具有伪装 Alice 的能力.

由上述过程可知，敌手$\mathcal{A}_1$的伪造密钥协商消息通过了 Bob 的合法性验证，则$\mathcal{A}_1$伪装 Alice 成功.

敌手$\mathcal{A}_1$通过 Bob 的身份合法性验证后，与 Bob 间进行会话密钥协商，具体协商过程如下所述：

Bob 选取随机数 $b\in Z_q^*$，计算 $T_B=bP$ 和 $P_A=R_A+yH_1(ID_A,R_A)$，并发送消息(ID_B,R_B)给敌手$\mathcal{A}_1$(Bob 认为是与 Alice 在协商密钥)，并计算：

$K_{B,1}=x_B(X'_A+P_A+T_A)=x_B(aP)=ax_BP$；

$K_{B,2}=D_B(X'_A+P_A+T_A)=D_B(aP)=aD_BP$；

$K_{B,1}=b(X'_A+P_A+T_A)=b(aP)=abP$.

敌手$\mathcal{A}_1$收到消息(ID_B,R_B)后，计算 $P_B=R_B+yH_1(ID_B,R_B)$，并计算：

$$K_{A,1}=aX_B=ax_BP=K_{B,1}=K_1;$$

$$K_{A,2}=aP_B=aD_BP=K_{B,2}=K_2;$$

$$K_{A,3}=aT_B=abP=K_{B,3}=K_3.$$

Bob 与敌手$\mathcal{A}_1$最终协商的会话密钥为

$$K=H(ID_A,ID_B,X_A,X_B,T_A,T_B,K_1,K_2,K_3).$$

综上所述，文献[20]的方案无法满足其所声称的对$\mathcal{A}_1$类敌手的不可伪造性.

4 本文密钥协商协议

本节提出可证安全的高效无证书两方认证密钥协商协议，具体细节如下所述.

4.1 系统建立

群 G 是阶为大素数 $q(q>2^k,k$ 为安全参数)的循环群，P 是群 G 的一个生成元；选择抗碰撞的单向哈希函数 $H_1:\{0,1\}^L\times G\times G\to Z_q^*$，$H_2:\{0,1\}^L\times\{0,1\}^L\times G\to Z_q^*$，$H:\{0,1\}^*\to\{0,1\}^k$，其中 L 为用户身份标识的长度；KGC 随机选择主密钥 $s\in Z_q^*$，计算系统公开钥 $P_{Pub}=sP$，并公开系统参数 $Params=\langle q,P,G,P_{Pub},H_1,H_2,H\rangle$，秘密保存 s.

4.2 用户密钥生成

用户 ID_i随机选取秘密值 $x_{ID_i}\in Z_q^*$，计算公开参数 $X_{ID_i}=x_{ID_i}P$；并发送身份标识 ID_i和公开参数 X_{ID_i}给 KGC.

给定用户的身份标识 ID_i及公开参数 X_{ID_i}，KGC 随机选取秘密数 $r_{ID_i}\in Z_q^*$，并计算 $Y_{ID_i}=r_{ID_i}P$ 和 $y_{ID_i}=r_{ID_i}+sH_1(ID_i,X_{ID_i},Y_{ID_i})$，并通过安全信道将 y_{ID_i}和 Y_{ID_i}返回给用户 ID_i；用户 ID_i通过验证等式 $y_{ID_i}P=Y_{ID_i}+P_{Pub}H_1(ID_i,X_{ID_i},Y_{ID_i})$是否成立，判断 y_{ID_i}和 Y_{ID_i}的有效性；若上述等式成立，则 ID_i的公私钥为 $PK_{ID_i}=\langle X_{ID_i},Y_{ID_i}\rangle$和 $SK_{ID_i}=\langle x_{ID_i},y_{ID_i}\rangle$.

4.3 身份认证及密钥协商

用户 Alice(身份标识为 ID_A)与 Bob(身份标识为 ID_B)间的消息交互及密钥协商过程如下所述：

首先，Alice 选取随机秘密数 $a_1,a_2\in Z_q^*$，分别计算 $S_A=a_1(x_A+y_A)^{-1}$、$Q_A=a_2(X_B+Y_B+P_{Pub}h_B)$和 $U_A=H_2(ID_A,ID_B,a_1P,a_2P)$；最后，Alice发送消息$(ID_A,ID_B,U_A,S_A,Q_A)$给 Bob.

其中，$h_B=H_1(ID_B,X_B,Y_B)$.

Bob 收到(ID_A,ID_B,U_A,S_A,Q_A)后，首先计算 $P_{B,1}=S_A(X_A+Y_A+P_{Pub}h_A)$和$P_{B,2}=(x_B+y_B)^{-1}Q_A$，若有等式 $U_A=H_2(ID_A,ID_B,P_{B,1},P_{B,2})$成立，即 Alice 通过了 Bob 对其的身份合法性验证，且 Bob 验证了消息的合法性，即确认该消息是 Alice 为其发送的密钥协商消息；否则终止.

对 Alice 的身份及消息合法性验证通过后，首先 Bob 随机选取秘密数 $b_1,b_2\in Z_q^*$，分别计算 $S_B=b_1(x_B+y_B)^{-1}$、$Q_B=b_2(X_A+Y_A+P_{Pub}h_A)$和 $U_B=H_2(ID_A,ID_B,b_1P,b_2P)$；最后 Bob 发送消息$(ID_A,ID_B,U_B,S_B,Q_B)$给 Alice.

其中，$h_A=H_1(ID_A,X_A,Y_A)$.

Bob 计算共享秘密：

$$K_B^1=b_1S_A(X_A+Y_A+P_{Pub}h_A);$$

$$K_B^2=b_2(x_B+y_B)^{-1}Q_A;$$

$$K_B^3=b_2P+(x_B+y_B)^{-1}Q_A.$$

Bob 计算的会话密钥 K_{BA} 为

$$K_{BA}=H(ID_A\parallel ID_B\parallel U_A\parallel U_B\parallel K_B^1\parallel K_B^2\parallel K_B^3).$$

Alice 收到(ID_A,ID_B,U_B,S_B,Q_B)后，首先计算 $P_{A,1}=S_B(X_B+Y_B+P_{Pub}h_B)$ 和 $P_{A,2}=(x_A+y_A)^{-1}Q_B$，若有等式 $U_B=H_2(ID_A,ID_B,P_{A,1},P_{A,2})$ 成立，即 Bob 通过了 Alice 对其的身份合法性验证，且 Alice验证了消息的合法性，即确认该消息是 Bob 为其发送的密钥协商消息；否则终止.

对 Bob 的身份及消息合法性验证通过后，Alice 计算共享秘密：

$$K_A^1=a_1S_B(X_B+Y_B+P_{Pub}h_B);$$

$$K_A^2=a_2(x_A+y_A)^{-1}Q_B;$$

$$K_A^3=a_2P+(x_A+y_A)^{-1}Q_B.$$

Alice 计算的会话密钥 K_{AB} 为

$$K_{AB}=H(ID_A\parallel ID_B\parallel U_A\parallel U_B\parallel K_A^1\parallel K_A^2\parallel K_A^3).$$

4.4　正确性

本节对本文密钥协商协议的正确性进行描述.

(1) 密钥的合法性验证

$$y_{ID_i}P=(r_{ID_i}+P_{Pub}h_{ID_i})P$$
$$=Y_{ID_i}+P_{Pub}H_1(ID_i,X_{ID_i},Y_{ID_i}).$$

其中 $h_{ID_i}=H_1(ID_i,X_{ID_i},Y_{ID_i})$ 和 $y_{ID_i}=r_{ID_i}+sh_{ID_i}$.

(2) 身份合法性验证

以 Alice 对 Bob 的身份合法性验证过程为例对验证过程进行分析：

$$P_{A,1}=S_B(X_B+Y_B+P_{Pub}h_B)$$
$$=b_1(x_B+y_B)^{-1}(x_BP+r_BP+sPh_B)=b_1P;$$

$$P_{A,2}=(x_A+y_A)^{-1}Q_B$$
$$=b_2(x_A+y_A)^{-1}(X_A+Y_A+P_{Pub}h_A)=b_2P;$$

$$U_B=H_2(ID_A,ID_B,P_{A,1},P_{A,2})$$
$$=H_2(ID_A,ID_B,b_1P,b_2P).$$

Bob 对 Alice 身份合法性验证过程的正确性分析与上述过程类似，本文不在赘述.

(3) 协商密钥的一致性

Bob 计算的共享秘密为

$$K_B^1=b_1S_A(X_A+Y_A+P_{Pub}h_A)$$
$$=b_1a_1(x_A+y_A)^{-1}(X_A+Y_A+P_{Pub}h_A)=a_1b_1P;$$

$$K_B^2=b_2(x_B+y_B)^{-1}Q_A$$
$$=a_2b_2(x_B+y_B)^{-1}(X_B+Y_B+P_{Pub}h_B)=a_2b_2P;$$

$$K_B^3=b_2P+(x_B+y_B)^{-1}Q_A=a_2P+b_2P.$$

Alice 计算的共享秘密为

$$K_A^1=a_1S_B(X_B+Y_B+P_{Pub}h_B)=a_1b_1P;$$

$$K_A^2=a_2(x_A+y_A)^{-1}Q_B=a_2b_2P;$$

$$K_A^3=a_2P+(x_A+y_A)^{-1}Q_B=a_2P+b_2P.$$

则有 $K_B^1=K_A^1$、$K_B^2=K_A^2$ 和 $K_B^3=K_A^3$；因此 $K_{BA}=K_{AB}$.

5　协议分析

5.1　安全性证明

本节将在 *eCK* 安全模型下对本文密钥协商协议的安全性进行证明.

定理 1.　由于 DL 问题是困难问题，则本文协议是安全的认证密钥协商协议.

证明.　(1) 证明本文协议满足密钥协商安全定义的条件 1.

由协议的正确性分析可知 $K_{BA}=K_{AB}$，所以 Alice和 Bob 协商的会话密钥相等，且相应参数的随机性确保会话密钥在密钥空间上满足均匀分布.

(2) 证明本文协议满足密钥协商安全定义的条件 2.

声称 1.　任意的$\mathcal{A}_1$类概率多项式时间敌手$\mathcal{A}_1$在游戏中获胜的优势 $Adv_{\mathcal{A}_1}(k)$是可忽略的.

构造解决 DL 困难问题的模拟器$\mathcal{T}$，其输入为 $cP\in G$，对于任意未知的 $c\in Z_q^*$，DL 问题的目标是计算 c. 假设在攻击实验中$\mathcal{A}_1$进行了下述操作：① 请求生成了 q_S 个用户的私钥；② 执行了 q_U 次密钥协商；③ 游戏的第 1 阶段询问中，对 q_C（其中 $q_S>q_C$）个用户执行了 *Corrupt* 询问.

模拟器$\mathcal{T}$任意选取随机数 $J\in(0,q_U)$，则 J 是$\mathcal{T}$猜测的在 *Test* 询问中$\mathcal{A}_1$要挑战的会话.

模拟器$\mathcal{T}$的构造如下：

初始化：$\mathcal{T}$运行 $Setup(\lambda,n)$算法，发送公开参数 $Params=\langle q,P,G,P_{Pub},H_1,H_2,H\rangle$给$\mathcal{A}_1$，其中令 $P_{Pub}=cP$；同时，$\mathcal{T}$维持列表 L_{KG}、L_{SK}、L_{PK}、L_S分别用于跟踪$\mathcal{A}_1$的部分密钥生成、私钥生成、公钥生成和 *Send* 询问，初始时各列表均为空.

部分密钥生成询问. 收到$\mathcal{A}_1$关于 ID_i和公开参数 X_i的部分密钥生成询问时，$\mathcal{T}$进行下述操作：

① 若$\langle ID_i,X_i,d_{ID_i}=(y_i,Y_i),r_i,Type_i\rangle\in L_{KG}$，则$\mathcal{T}$返回 $d_{ID_i}=(y_i,Y_i)$给$\mathcal{A}_1$；

② 否则，$\mathcal{T}$ 选取随机数 $Type\in\{0,1\}$，且 $Pr[Type=1]=\delta=\frac{1}{q_S}$；若 $Type=1$，设置 ID 所对应的元组为$\langle ID,X,\perp,\perp,0\rangle$. 若 L_{KG} 中多个元组中的 $Type=1$ 或不存在 $Type=1$ 的元组，但 L_{KG} 的长度等于 q_S，则 $\mathcal{T}$ 终止模拟；若 $Type=0$，则随机选取 $r_i\in Z_q^*$，计算 $Y_i=r_iP$，选取随机数 $y_i\in Z_q^*$，并添加 $\langle ID_i,X_i,d_{ID_i}=(y_i,Y_i),r_i,Type_i=1\rangle$ 到 L_{KG} 中，并返回 $d_{ID_i}=(y_i,Y_i)$给 $\mathcal{A}_1$.

私钥生成询问. 收到 $\mathcal{A}_1$ 关于 ID_i 的私钥生成询问时，$\mathcal{T}$ 进行下述操作：

① 若存在$\langle ID_i,x_i,y_i\rangle\in L_{SK}$，$\mathcal{T}$ 返回元组中相应的$\langle x_i,y_i\rangle$给 $\mathcal{A}_1$；

② 否则，$\mathcal{T}$ 选取随机数 $x_i\in Z_q^*$，计算 $X_i=x_iP$，就$\langle ID_i,X_i\rangle$进行部分密钥生成询问并获得相应的元组$\langle ID_i,y_i,Y_i\rangle$，添加$\langle ID_i,x_i,y_i\rangle$到 L_{SK} 中，返回$\langle x_i,y_i\rangle$给 $\mathcal{A}_1$；同时添加$\langle ID_i,X_i,Y_i\rangle$到 L_{PK} 中.

公钥生成询问. 收到 $\mathcal{A}_1$ 关于 ID_i 的公钥生成询问时，$\mathcal{T}$ 进行下述操作：

① 若存在$\langle ID_i,X_i,Y_i\rangle\in L_{PK}$，则返回元组中相应的$\langle X_i,Y_i\rangle$给 $\mathcal{A}_1$；

② 否则，$\mathcal{T}$ 随机选取 $x_i\in Z_q^*$，计算 $X_i=x_iP$，就$\langle ID_i,X_i\rangle$进行部分密钥生成询问获得相应的元组$\langle ID_i,y_i,Y_i\rangle$，添加$\langle ID_i,X_i,Y_i\rangle$到 L_{PK} 中，返回$\langle X_i,Y_i\rangle$给 $\mathcal{A}_1$；同时添加$\langle ID_i,x_i,y_i\rangle$到 L_{SK} 中.

$Send(\Pi_{i,j}^S,M)$. 列表 L_S 中的元组格式为$\langle\Pi_{i,j}^S,a,M,M',K,SK\rangle$，其中 M' 是 $\Pi_{i,j}^S$ 在会话过程中产生的消息，M 是 $\Pi_{i,j}^S$ 在会话过程中所接收到的消息，随机数 $a\in Z_q^*$ 由模拟器 $\mathcal{T}$ 为 $\Pi_{i,j}^S$ 选取，K(其中 $K=\{K^1,K^2,K^3\}$)表示密钥协商过程中相应的共享秘密，SK 表示会话密钥，初始时均设置 K 和 SK 为空；$Reveal$ 询问过程中会对 L_S 进行更新.

当 $\mathcal{T}$ 收到 M 时，进行如下操作：

① 若有$\langle\Pi_{i,j}^S,*,*,*,*,*\rangle\in L_S$，且 $\Pi_{i,j}^S$ 是相应会话的发起者，则 $\mathcal{T}$ 接受该会话，并设置 M 为 $\Pi_{i,j}^S$ 所接收的消息；否则，$\Pi_{i,j}^S$ 不存在，则进行公钥和私钥询问为 ID_i 生成相应的密钥.

② 若 $M=\lambda$，则设置 ID_i 为相应会话的发起者；否则，设置 ID_i 为相应会话的响应者，并且将 M 作为响应者 ID_i 的输入，同时设置 $\Pi_{i,j}^S$ 接受会话.

③ 如果 $S\neq J$，$\mathcal{T}$ 选取随机数 $a_1,a_2\in Z_q^*$ 作为参与者 i 的随机秘密数，并初始化消息 $M=\langle U_i=H_2(ID_i,ID_j,a_1P,a_2P),S=a_1(x_i+y_i),Q=a_2(X_j+Y_j+P_{Pub}h_j)\rangle$，更新 L_S 并返回 M；否则 $S=J$，则 $\mathcal{T}$ 在 L_{KG} 中查找 ID_j 对应的相关元组，如果 $Type=1$，则终止模拟；如果 $Type=0$，随机选择 $b_1,b_2\in Z_q^*$，并计算应答消息 $M=\langle U_j=H_2(ID_i,ID_j,b_1P,b_2P),S_j=b_1(x_j+y_j),Q_j=b_2(X_i+Y_i+P_{Pub}h_i)\rangle$，更新 L_S 并返回 M.

$Corrupt(i)$. $\mathcal{T}$ 根据 ID_i 查找 L_{KG}，若不存在相应的元组，则进行公钥询问和私钥询问；否则，$\mathcal{T}$ 获得 L_{KG} 中相应的元组，若 $Type=1$，则终止模拟，若 $Type=0$，进行私钥生成询问，并返回对应的私钥$\langle x_i,y_i\rangle$.

$Reveal(\Pi_{i,j}^S)$：若 L_S 中不存在 $\Pi_{i,j}^S$ 所对应的元组，则 $\mathcal{T}$ 返回 $\perp$；若 $\Pi_{i,j}^S$ 未接受相应的会话，则 $\mathcal{T}$ 返回 $\perp$；否则 L_S 中必存在 $\Pi_{i,j}^S$ 所对应的元组，$\mathcal{T}$ 进行下述操作.

① $SK\neq\perp$，则返回元组中相应的 SK.

② $SK=\perp$，若 L_{KG} 中不存在 ID_i 所对应的元组，则返回 $\perp$. 否则，L_{KG} 中存在 ID_i 对应的元组，根据元组中 $Type$ 的取值分类讨论：

如果 ID_i 对应元组中的 $Type=0$，则参与者 i 拥有合法的用户私钥$\langle x_i,y_i\rangle$，$\mathcal{T}$ 根据输入消息 $M=(U_j,S_j,Q_j)$和随机数 $a_1,a_2\in Z_q^*$ 计算 K，计算 ID_i 对应的 $U_i=H_2(ID_i,ID_j,a_1P,a_2P)$和 $K=\langle K^1=a_1S_j(X_j+Y_j+P_{Pub}h_j),K^2=a_2(x_i+y_i)^{-1}Q_j,K^3=a_2P+(x_i+y_i)^{-1}Q_j\rangle$，计算 $SK=\{ID_i,ID_j,U_i,U_j,K\}$，更新列表并返回 SK；

如果 ID_i 对应元组中的 $Type=1$，由于 $\mathcal{T}$ 不具有计算参与者 ID_i 私钥的能力，因此无法直接获知相应的会话密钥；若 L_S 中存在与该会话相匹配的元组$\langle\Pi_{i,j}^S,a,M,M',K,SK\rangle$，返回 SK；否则，从密钥空间中随机选取 $K\in G$ 和 $SK\in\{0,1\}^k$，更新列表 L_S 并返回 SK.

$Test(\Pi_{i,j}^S)$. 若第 1 阶段询问结束，并且攻击者完全遵循 eCK 安全模型的相关要求. 攻击者选择新鲜的参与者 $\Pi_{i,j}^t$ 发起 $Test$ 询问. 收到相应的询问后，$\mathcal{T}$ 进行下述操作.

① 若 $t\neq j$，则 $\mathcal{T}$ 停止，并终止模拟；

② 若 $t=j$ 且该会话已被打开，并且会话标识与 $\Pi_{i,j}^t$ 相同，则 $\mathcal{T}$ 停止，并终止模拟；

③ 否则，$\mathcal{T}$ 在 L_S 中查找 $\Pi_{i,j}^t$ 所对应的元组，并输出相应的应答消息给 $\mathcal{A}_1$.

猜测. 敌手$\mathcal{A}_1$询问完成后，输出会话密钥的猜测SK'，$\mathcal{T}$收到$\mathcal{A}_1$的猜测SK'时，若$SK'=SK$，则输出$c=[Q-a_1(X_i+Y_i)](a_1h_iP)^{-1}$(其中$h_i=H_1(ID_i,X_i,Y_i)$,$Q=a_1(X_i+Y_i+P_{Pub}h_i)$)作为DL困难问题的解；否则输出$\perp$.

若$\mathcal{A}_1$攻击本文协议成功，则$\mathcal{T}$输出DL困难问题的有效解；否则，$\mathcal{T}$没有解决DL困难问题.

(a)若$\mathcal{T}$未终止，则$\mathcal{A}_1$无法区分攻击是真实攻击还是模拟攻击.

由于在模拟游戏中，各参与者的输出消息均遵循本文协议的相关要求，并且在消息空间上是均匀分布的，因此敌手不具有区分攻击是真实攻击还是模拟攻击的能力.

(b)若$\mathcal{A}_1$能以不可忽略的优势ε成功攻击本文密钥协商协议，则$\mathcal{T}$至少能以不可忽略的优势$\frac{q_S-q_C}{eq_Uq_S^3}\varepsilon$解决DL困难问题.

在模拟过程中，若$\mathcal{T}$未终止，则$\mathcal{A}_1$攻击本文密钥协商协议成功. 事件E_1表示$\mathcal{A}_1$进行部分密钥生成询问时$\mathcal{T}$未终止；事件E_2表示$\mathcal{A}_1$进行*Send*询问时$\mathcal{T}$未终止；事件E_3表示$\mathcal{A}_1$进行*Corrupt*询问时$\mathcal{T}$未终止；事件E_4表示$\mathcal{A}_1$进行*Test*询问时$\mathcal{T}$未终止. 则有$Pr[E_1]=(1-\delta)^{q_S-1}\delta$; $Pr[E_2]=\frac{1}{q_S}$; $Pr[E_3]=\frac{q_S-q_C}{q_S}$; $Pr[E_4]=\frac{1}{q_U}$.

当$\mathcal{A}_1$以不可忽略的优势ε成功攻击本文密钥协商协议时，模拟器$\mathcal{T}$输出正确DL困难问题有效解的优势为

$$Pr[\Re wins]=Pr[E_1\cap E_2\cap E_3\cap E_4\cap A_1wins]$$
$$=\frac{q_S-q_C}{q_Uq_S^2}(1-\delta)^{q_S-1}\delta\varepsilon.$$

由于$\delta=\frac{1}{q_S}$，则q_S足够大时$(1-\delta)^{q_S-1}$趋向于e^{-1}(e是自然对数底数)，因此，若$\mathcal{T}$在模拟过程中未终止，且$\mathcal{A}_1$以不可忽略的优势ε成功攻击本文协议，则$\mathcal{T}$赢得上述游戏的优势至少为$\frac{q_S-q_C}{eq_Uq_S^3}\varepsilon$. 则$\mathcal{T}$输出DL困难问题解的优势至少为$\frac{q_S-q_C}{eq_Uq_S^3}\varepsilon$.

由于DL问题是困难的，因此$\mathcal{A}_1$在游戏中获胜的优势$Adv_{\mathcal{A}_1}(n)$是可忽略的，即对于$\mathcal{A}_{\mathrm{I}}$类敌手本文协议满足密钥协商安全定义的条件2.

声称2.　任意的$\mathcal{A}_{\mathrm{II}}$类概率多项式时间敌手$\mathcal{A}_2$在游戏中获胜的优势$Adv_{\mathcal{A}_2}(k)$是可忽略的.

证明过程与声称1证明相类似，不再赘述.

由声称1和声称2可知，本文协议满足密钥协商安全定义的条件2. 综上所述，若DL困难假设成立，则本文协议是安全的认证密钥协商协议. 证毕.

5.2　不可伪造性证明

定理3.　$\mathcal{A}_{\mathrm{I}}$类敌手的不可伪造性. 若$\mathcal{A}_{\mathrm{I}}$类敌手$\mathcal{A}_1$能以不可忽略的优势ε在多项式时间内赢得相关游戏($\mathcal{A}_1$最多进行q_K次密钥协商询问、q_D次部分密钥提取询问和q_S次私钥提取询问)，则算法$\mathcal{T}$能以优势$Adv(\mathcal{T})\geq\left(1-\frac{q_D}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)\frac{\varepsilon}{e(q_K+1)}$(e是自然对数底数)在多项式时间内解决DL困难问题.

证明.　假设算法$\mathcal{T}$是一个DL困难问题的解决者，其困难问题的输入为(P,cP)，其中$c\in Z_q^*$且未知，其目标是计算出c. $\mathcal{T}$以$\mathcal{A}_1$为子程序并充当游戏的挑战者. $\mathcal{T}$运行初始化算法，并发送公开参数$Params=\langle q,P,G,P_{Pub},H_1,H_2,H\rangle$给$\mathcal{A}_1$，令$P_{Pub}=cP$，同时$\mathcal{T}$维持列表$L_1,L_2,L_D,L_{SK},L_{PK},L_K,L_U$分别用于跟踪$\mathcal{A}_1$对谕言机$H_1$、$H_2$、部分密钥生成、私钥生成、公钥生成、密钥协商和合法性验证询问，开始时各列表均为空.

询问. 敌手$\mathcal{A}_1$进行下述询问：

H_1查询. 当$\mathcal{A}_1$向谕言机H_1询问$H_1(ID_i,X_i,Y_i)$时，若$\langle ID_i,X_i,Y_i,h_1\rangle\in L_1$，则返回$h_1$给$\mathcal{A}_1$；否则，$\mathcal{T}$选取满足$\langle *,*,*,h_1\rangle\notin L_1$的随机数$h_1\in Z_q^*$，并添加$\langle ID_i,X_i,Y_i,h_1\rangle$到$L_1$中，同时返回$h_1$给$\mathcal{A}_1$.

H_2查询. 当$\mathcal{T}$收到$\mathcal{A}_1$对谕言机H_2的询问$H_2(ID_i,ID_j,U_i,S_i,Q_i)$时，$\mathcal{T}$进行下述操作：

① 若存在$\langle ID_i,ID_j,U_i,S_i,Q_i,h_2,Type_i\rangle\in L_2$，则返回$h_2$给$\mathcal{A}_1$；

② 否则，$\mathcal{T}$随机选取$Type\in\{0,1\}$，且$Pr[Type=1]=\delta=\frac{1}{q_K+1}$；若$Type=0$，$\mathcal{T}$选取满足$\langle *,*,*,*,*,h_2,*\rangle\in L_2$的随机数$h_2\in Z_q^*$，添加元组$\langle ID_i,ID_j,U_i,S_i,Q_i,h_2,Type_i\rangle$到$L_2$中，并返回$h_2$给$\mathcal{A}_1$；否则，$Type=1$，令$h_2=\perp$，并返回“$\perp$”给$\mathcal{A}_1$.

部分密钥生成询问. 当$\mathcal{T}$收到$\mathcal{A}_1$对身份ID_i和公开参数X_i的部分密钥生成询问时，若存在$\langle ID_i,y_i,Y_i\rangle\in L_D$，则返回相应的值$\langle y_i,Y_i\rangle$给$\mathcal{A}_1$；否则，$\mathcal{T}$随机选取$y_i,h_1\in Z_q^*$，计算$Y_i=y_iP-P_{Pub}h_1$，添加元组$\langle ID_i,y_i,Y_i\rangle$到$L_D$中，并返回$\langle y_i,Y_i\rangle$给$\mathcal{A}_1$；同时添加$\langle ID_i,X_i,Y_i,h_1\rangle$到$L_1$中.

私钥生成询问. 当收到$\mathcal{A}_1$对ID_i的私钥生成询问时,$\mathcal{T}$进行下述操作.

① 若存在$\langle ID_i, x_i, y_i\rangle \in L_{SK}$,则返回相应的私钥$SK=\langle x_i, y_i\rangle$给$\mathcal{A}_1$;

② 否则,$\mathcal{T}$随机选取$x_i \in Z_q^*$,计算$X_i=x_iP$,对身份ID_i和X_i进行部分密钥生成询问获得相应的元组$\langle ID_i, y_i, Y_i\rangle$,添加$\langle ID_i, x_i, y_i\rangle$到$L_{SK}$中,返回$\langle x_i, y_i\rangle$给$\mathcal{A}_1$,并添加$\langle ID_i, X_i, Y_i\rangle$到$L_{PK}$中.

公钥生成询问. 当收到$\mathcal{A}_1$对ID_i的公钥生成询问时,$\mathcal{T}$进行下述操作:

① 若存在$\langle ID_i, X_i, Y_i\rangle \in L_{PK}$,则返回相应的公钥$PK=\langle X_i, Y_i\rangle$给$\mathcal{A}_1$;

② 否则,$\mathcal{T}$查询L_2,若$Type=0$,则$\mathcal{T}$随机选取$x_i \in Z_q^*$,计算$X_i=x_iP$,对身份ID_i和X_i进行部分密钥生成询问获得相应的元组$\langle ID_i, y_i, Y_i\rangle$,添加$\langle ID_i, X_i, Y_i\rangle$到$L_{PK}$中,返回$PK=\langle X_i, Y_i\rangle$给$\mathcal{A}_1$,同时添加$\langle ID_i, x_i, y_i\rangle$到$L_{SK}$中;若$Type=1$,则$\mathcal{T}$随机选取$X_i, Y_i \in G$,并添加$\langle ID_i, X_i, Y_i\rangle$到$L_{PK}$中,并返回$PK=\langle X_i, Y_i\rangle$给$\mathcal{A}_1$.

公钥替换. $\mathcal{A}_1$可以选择一个新的公钥替换任意合法用户的原始合法公钥.

密钥协商询问. 当$\mathcal{T}$收到$\mathcal{A}_1$对身份$\langle ID_A, ID_B\rangle$的密钥协商询问时,$\mathcal{T}$首先在列表$L_2$中查询$\langle ID_A, ID_B\rangle$:

① 若$Type=1$,则$\mathcal{T}$放弃,并终止模拟;

② 否则,$\mathcal{T}$根据身份$\langle ID_A, ID_B\rangle$分别在列表$L_{SK}$和$L_{PK}$中分别查询元组$\langle ID_A, x_A, y_A\rangle$和$\langle ID_B, X_B, Y_B\rangle$,并选取随机秘密数$a_1, a_2 \in Z_q^*$,分别计算$U_A=H_2(ID_A, ID_B, a_1P, a_2P)$,$S_A=a_1(x_A+y_A)^{-1}$,$Q_A=a_2(X_B+Y_B+P_{Pub}h_B)$(其中$h_B=H_1(ID_B, X_B, Y_B)$),发送$(ID_A, ID_B, U_A, S_A, Q_A)$给$\mathcal{A}_1$.

合法性验证询问. 当$\mathcal{T}$收到$\mathcal{A}_1$对身份$\langle ID_A, ID_B\rangle$和消息$(U_A, S_A, Q_A)$的合法性验证询问时,$\mathcal{T}$首先在列表$L_2$和$L_P$查询$\langle ID_A, ID_B\rangle$:

① 若L_2中存在相应的元组且其对应的$Type=0$,则$\mathcal{T}$首先在L_{PK}和L_{SK}中分别查询ID_A和ID_B对应的元组$\langle ID_A, X_A, Y_A\rangle$和$\langle ID_B, x_B, y_B\rangle$,计算$P_{A,1}=S_A(X_A+Y_A+P_{Pub}h_A)$和$P_{A,2}=(x_B+y_B)^{-1}Q_A$,验证等式$U_A=H_2(ID_A, ID_B, P_{A,1}, P_{A,2})$是否成立,若成立则返回"通过"给$\mathcal{A}_1$,否则结束,并终止模拟;

② 若L_2中存在相应的元组且其对应的$Type=1$,则返回"通过"给$\mathcal{A}_1$,否则终止模拟;

③ 若列表L_{PK}中不存在相应的元组,若存在元组$\langle ID_A, ID_B, U_A, S_A, Q_A, h_2\rangle \in L_2$,则返回"通过"给$\mathcal{A}_1$,否则终止模拟.

伪造. 经过多项式有界次上述询问后,$\mathcal{A}_1$随机选取秘密数$a_1, a_2 \in Z_q^*$和$S \in Z_q^*$,计算$U=H_2(ID_A, ID_B, a_1P, a_2P)$和$Q=a_2(X_B+Y_B+P_{Pub}h_B)$,$\mathcal{A}_1$输出关于身份$ID_A$和$ID_B$的伪造密钥协商消息$(ID_A, ID_B, U, S, Q)$,并对该元组之前未进行过密钥协商询问,同时$\mathcal{T}$知道被替换的公钥.

若$\mathcal{A}_1$伪造成功,同时身份ID_A和ID_B在L_2中对应元组中的$Type=1$,则$\mathcal{T}$输出$c=[Q-a_2(X_B+Y_B)](a_2h_BP)^{-1}$作为DL困难问题的解;否则,$\mathcal{T}$没有解决DL问题. 特别的,$\mathcal{A}_1$不能对挑战信息进行合法性验证询问.

在询问阶段,当$\mathcal{A}_1$出现下述询问时,则$\mathcal{T}$会终止模拟:① 对身份ID_A进行了部分密钥生成询问;② 对身份ID_A进行了私钥生成询问.

定义事件E_1表示$\mathcal{A}_1$对ID_A未进行部分密钥生成询问和私钥生成询问;事件E_2表示密钥协商询问过程中$\mathcal{T}$未终止;则有$Pr[E_1]=\left(1-\frac{q_D}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)$,$Pr[E_2]=(1-\delta)^{q_K}$. 因此,询问阶段$\mathcal{T}$不终止的概率为$\left(1-\frac{q_D}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)(1-\delta)^{q_K}$;伪造阶段$\mathcal{A}_1$伪造正确密钥协商消息的概率为$\delta$.

因此,若$\mathcal{T}$在模拟过程中未终止,并且$\mathcal{A}_1$以不可忽略的优势ε攻破了本文密钥协商协议时,则$\mathcal{T}$输出DL困难问题有效解的优势至少为$\left(1-\frac{q_D}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)(1-\delta)^{q_K}\delta\varepsilon$. 由于$\delta=\frac{1}{q_K+1}$,则当$q_K$足够大时,$(1-\delta)^{q_K}$趋向于$e^{-1}$.

综上所述,若$\mathcal{T}$在模拟过程中未终止,并且敌手$\mathcal{A}_1$能以不可忽略的优势ε攻破了本文密钥协商协议的不可伪造性,则$\mathcal{T}$能以优势$Adv(\mathcal{T})\geq\left(1-\frac{q_D}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)\frac{\varepsilon}{e(q_K+1)}$成功解决DL困难问题. 证毕

定理 4. $\mathcal{A}_{\mathrm{II}}$类敌手的不可伪造性. 若$\mathcal{A}_{\mathrm{II}}$类敌手$\mathcal{A}_2$能以不可忽略的优势$\varepsilon$在多项式时间内赢得相关游戏($\mathcal{A}_2$最多进行$q_K$次密钥协商询问、$q_D$次部分密钥提取询问和$q_S$次私钥提取询问),则算法$\mathcal{T}$能以优势$Adv(\mathcal{T})\geq\left(1-\frac{q_D}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)\frac{\varepsilon}{e(q_K+1)}$(e是自

然对数底数)在多项式时间内解决 DL 困难问题.

证明过程与定理 3 证明相类似,不再赘述.

6　效率及性能分析

本节将从计算开销、公私钥长度、消息长度和消息交互次数等方面综合分析无证书密钥协商协议的计算和通信效率及安全性,其中计算效率以参与者执行一次密钥协商协议的运算量来衡量,通信效率以消息交互次数来衡量.

本节将本文协议与现有使用双线性映射[9,12-14]和不使用双线性映射[15-20]的相关协议进行比较,比较结果如表 1 所示,其中表 1 中未统计协议中可提前计算的相关运算;同时,消息长度未统计参与者的身份、公钥等公开信息.

表 1 中相关符号的定义如下:

E_M表示群上的点乘运算;E_e表示群上的双线性运算;E_{Mac}表示消息认证码运算;E_{inv}表示模块倒置操作;$|G|$表示群 G 中元素的长度;$|Z_q^*|$表示 Z_q^* 中元素的长度;$|Sig|$表示消息签名的长度;$|\{0,1\}^k|$表示字符串$\{0,1\}^k$的长度;*UnSec* 表示协议不满足所声称的安全性,*Sec* 表示协议满足所声称的安全性.

由表 1 可知,文献[9,12-14]的计算量较大,导致相关方案的计算效率较低,但上述方案[9,12-14]具有公私钥长度较短的优势,并且文献[14]实现了三方参与者间会话密钥的安全协商. 文献[15-16]的安全性较弱,接收者无法确认消息的真实接收者;文献[17]中协议参与者的运算量较大,导致协议的执行效率较低;虽然相关文献[18-20]声称其方案能够满足对任意敌手的安全性,但是分析发现$\mathcal{A}_{\mathrm{I}}$类敌手能够伪造文献[18-20]中任意用户的密钥协商信息,故上述方案[18-20]对$\mathcal{A}_{\mathrm{I}}$类敌手不具备不可伪造性;文献[15-19]未实现双方的身份认证,而文献[20]仅实现了单向的身份认证,即发送者无法验证消息接收者的身份合法性. 本文协议在实现会话密钥安全协商的同时,完成参与者身份合法性的双向认证;由于本文协议实现了双向的身份合法性认证,导致其消息长度较长.

表 1　性能比较结果

方案	运算量	安全性	密钥长度		交互次数	消息长度
			私钥	公钥		
文献[9]-I	$4E_{MI}+4E_e+2E_{Mac}$	*Sec*	$\|Z_q^*\|$	$\|G\|$	2	$4\|G\|+2\|E_{Mac}\|$
文献[9]-II	$4E_M+4E_e$	*Sec*	$\|Z_q^*\|$	$\|G\|$	2	$4\|G\|$
文献[12]	$6E_M+2E_e$	*Sec*	$\|Z_q^*\|+\|G\|$	$\|G\|$	2	$2\|G\|$
文献[13]	$6E_M+4E_e$	*Sec*	$2\|G\|$	$\|G\|$	2	$4\|G\|$
文献[14]	$15E_M+6E_e$	*Sec*	$3\|Z_q^*\|$	$\|G\|$	8	$11\|G\|$
文献[15]	$7E_M$	*UnSec*	$2\|Z_q^*\|$	$2\|G\|$	2	$2\|G\|$
文献[16]	$6E_M$	*UnSec*	$2\|Z_q^*\|$	$2\|G\|$	2	$2\|G\|$
文献[17]	$9E_M$	*Sec*	$\|Z_q^*\|+\|G\|+\|Sig\|$	$2\|G\|+\|Sig\|$	2	$2\|G\|$
文献[18]	$5E_M+E_{inv}$	*UnSec*	$2\|Z_q^*\|+\|G\|$	$\|G\|$	3	$5\|G\|$
文献[19]	$5E_M$	*UnSec*	$2\|Z_q^*\|$	$2\|G\|$	2	$2\|G\|$
文献[20]	$5E_M$	*UnSec*	$\|Z_q^*\|+\|G\|$	$\|G\|+\|G\|$	2	$2\|Z_q^*\|+1\|G\|$
本文方案	$5E_M$	*Sec*	$2\|Z_q^*\|$	$2\|G\|$	2	$4\|Z_q^*\|+2\|G\|$

综上所述,在安全性方面,由于 *eCK* 安全模型优于 *mBR* 模型,所以协议[15-16,18-19]的安全性是在较弱的安全模型下进行的证明;文献[15-16]中的协议无法满足其所声称的安全性;文献[18-20]中的协议都无法抵抗$\mathcal{A}_{\mathrm{I}}$类敌手的不可伪造性攻击($\mathcal{A}_{\mathrm{I}}$类敌手对文献[18-19]的伪造攻击过程与文献[20]类似). 在计算效率方面,由于文献[9,12-14]中的协议均基于双线性映射构建,运算量较大,计算效率较低;同时,文献[15-17]中协议的点乘运算次数较多,导致协议的计算效率较低;文献[14,18]中协议的消息交互次数较多,致使其通信效率较低;由于在密钥协商过程中完成参与者身份合法性的双向认证,因此本文协议的消息长度较长.

相较与现有的无证书密钥协商协议[9,12-20]而言,本文密钥协商协议在计算和通信效率及安全性方面具有明显的优势,即本文协议的性能更优.

7　结束语

本文提出了高效可证安全的无证书两方认证密钥协商协议,并在 *eCK* 强安全模型和随机谕言机模型下基于 DL 困难问题分别证明了本文协议的安全

性和不可伪造性.该协议具有无密钥托管、完美的前后向安全性等安全属性;同时本文协议的双方参与者实现了相互的身份认证,具有更强的抗伪造能力.相较于其他相关协议而言,本文协议具有更高的计算和通信效率,在带宽受限的网路环境(如无线传感器网络、Ad-Hoc 网络等)下具有较好的推广性.

致 谢 感谢审稿专家和编辑老师的细致审阅!

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes//Proceedings of the Advances in Cryptology-Crypto 84. Santa Barbara, USA, 1984: 47-53

[2] Al-Riyami S S, Paterson K G. Certificate less public key cryptography//Proceedings of the 9th International Conference on the Theory and Application of Cryptology and Information Security. Taipei, China, 2003: 452-473

[3] Mandt T K. Certificateless authenticated two-party key agreement protocols[M. S. dissertation]. Gjøvik University College, Gjøvik, 2006

[4] Wang Sheng-Bao, Cao Zhen-Fu, Wang Li-Cheng. Efficient certificateless authenticated key agreement protocol form pairings. Wuhan University Journal of Natural Sciences, 2006, 11(5): 1278-1282

[5] Shao Zhu-Hua. Efficient authenticated key agreement protocol using self-certified public keys from pairings. Wuhan University Journal of Natural Sciences, 2005, 10(1): 267-270

[6] Xia Liang, Wang Sheng-Bao, Shen Jia-Jun, et al. Breaking and repairing the certificateless key agreement protocol. Wuhan University Journal of Natural Sciences, 2008, 13(5): 562-566

[7] Swanson C M. Security in key agreement: Two-party certificateless protocols[M. S. dissertation]. University of Waterloo, Waterloo, 2008

[8] Swanson C, Jao D. A study of two-party certificateless authenticated key-agreement protocols//Proceedings of the 10th International Conference on Cryptology. New Delhi, India, 2009: 57—71

[9] T. Mandt, C. Tan. Certificateless authenticated two-party key agreement protocols//Proceedings of the 11th Asian Computing Science Conference. Tokyo, Japan, 2007: 37-44

[10] Shi Yi-Juan, Li Jian-Hua. Two-party authenticated key agreement in certificateless public key cryptography. Wuhan University Journal of Natural Sciences, 2007, 12(1): 71-74

[11] Lippold G, Boyd C, Nieto J. Strongly secure certificateless key agreement//Proceedings of the 3rd International Conference. Palo Alto, USA, 2009: 206-230

[12] Zhang Lei, Zhang Fu-Tai, Wu Qian-Hong, et al. Simulatable certificateless two-party authenticated key agreement protocol. Information Sciences, 2010, 180(6): 1020-1030

[13] Gao Zhi-Gang, Feng Deng-Guo. Efficient identity-based authenticated key agreement protocol in the standard model. Journal of Software, 2011, 22(5): 1031-1040(in Chinese)
(高志刚,冯登国. 高效的标准模型下基于身份认证密钥协商协议. 软件学报, 2011, 22(5): 1031-1040)

[14] Xiong Hu, Chen Zhong, Li Fagen. Provably secure and efficient certificateless authenticated tripartite key agreement protocol. Mathematical and Computer Modelling, 2012, 55(3): 1213-1221

[15] Geng Man-Man, Zhang Fu-Tai. Provably secure certificateless two-party authenticated key agreement protocol without pairing//Proceedings of the International Conference on IEEE Computational Intelligence and Security. Beijing, China, 2009: 208-212

[16] Hou Meng-Bo, Xu Qiu-Liang. A two-party certificateless authenticated key agreement protocol without pairing//Proceedings of the International Conference on IEEE Computer Science and Information Technology. Beijing, China, 2009: 412-416

[17] Yang Guo-Min, Tan C H. Strongly secure certificateless key exchange without pairing//Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. New York, USA, 2011: 71-79

[18] He De-Biao, Chen Jian-Hua, Hu Jin. A pairing-free certificateless authenticated key agreement protocol. International Journal of Communication Systems, 2012, 25(2): 221-230

[19] He De-Bao, Chen Yi-Tao, Chen Jian-Hua, et al. A new two-round certificateless authenticated key agreement protocol without bilinear pairings. Mathematical and Computer Modelling, 2011, 54(11): 3143-3152

[20] Liu Wen-Hao, Xu Chun-Xiang. Two party certificateless key agreement schemes. Journal of Software, 2011, 22(11): 2843-2852(in Chinese)
(刘文浩,许春香. 无证书两方密钥协商方案. 软件学报, 2011, 22(11): 2843-2852)

[21] Yang Hao-Min, Zhang Yao-Xue, Zhou Yue-Zhi. Certificateless two-party authenticated key agreement protocol based on bilinear pairings. Journal of Tsinghua University (Science and Technology), 2012, 52(9): 1293-1297(in Chinese)
(杨浩民,张尧学,周悦芝. 基于双线性对的无证书两方认证密钥协商协议. 清华大学学报(自然科学版), 2012, 52(9): 1293-1297)

[22] Cheng Qing-Feng, Lu Si-Qi. Analysis of two certificateless two-party authenticated key agreement protocols. Journal of Luoyang Normal University, 2013, 32(5): 53-56(in Chinese)
(程庆丰,陆思奇. 两个无证书两方认证密钥协商协议分析. 洛阳师范学院学报, 2013, 32(5): 53-56)

ZHOU Yan-Wei, born in 1986, Ph. D. candidate. His research interests include cryptography and wireless communication.

YANG Bo, born in 1963, Ph. D., professor, Ph. D. supervisor. His research interests include information security and cryptography.

ZHANG Wen-Zheng, born in 1966, professor. His research interests focus on information security.

Background

Traditional public key cryptography requires a trusted certification authority to issue a certificate binding the identity and the public key of an entity. Shamir defined a new public key cryptography called identity-based public key cryptography (ID-PKC). However, ID-PKC needs a trusted key generation center to generate the private key for every entity according to his identity. So we are confronted with the key escrow problem. Fortunately, the problems in traditional public key infrastructure and ID-PKC can be prohibited by certificateless public key cryptography.

This paper proposes a safely authenticated and efficient two party certificateless key agreement protocol without using the bilinear pairings, which is provably secure and unforgeable in the *eCK* security model and ROM under the DL assumption. Compared with other existing protocol in the computational complexity, this one is more efficient and also has known key security, perfect forward secrecy and resistance to unknown key-share attacks and key-compromise impersonation attacks, etc. It is more suitable for the identity-based public key cryptography, and has better popularization in the restricted bandwidth of the communication environment (e. g. a wireless sensors networks, Ad-Hoc networks, etc.).

This research was supported by the National Natural Science Foundation of China under Grant Nos. 61272436, 61402275, 61303092 and 61572303, Shaanxi Province Natural Science Basic Research Plan under Grant No. 2014JQ8309. The NSFC projects were researched on the theory, application, roaming authentication technology, CK security and anonymous communication in trusted Mobile Internet. The team has published several research articles about anonymous communication, trusted computing, internet of things and cryptography, submitted three industry specifications for trusted digital home, and registered five computer software copyrights.