文章编号：1004-4353(2022)02-0143-08

一个改进的无证书跨域认证密钥协商协议

李慧敏[1,2]， 梁红梅[3]， 张金辉[1,2]

(1.莆田学院 数学与金融学院，福建 莆田 351100；2.应用数学福建省高校重点实验室(莆田学院)，福建 莆田 351100；3.闽南师范大学 数学与统计学院，福建 漳州 363000)

摘要：针对文献[11]中提出的 CAKA 协议存在的无法认证对方身份和容易受到替换公钥攻击威胁的安全问题，给出了一种改进协议. 该协议改进了原协议中的 3 个步骤，使得参与协议的双方用户在执行协议过程中必须用到各自的全部私钥，并在协议双方发送的消息中加入各自的身份信息. 实验表明，该改进协议不仅能够克服原协议中的安全性问题，而且提高了计算效率. 因此该改进协议对基于无证书公钥系统构造的密钥协商协议具有良好的参考价值，同时也可为同类跨域密钥协商协议的分析与设计提供参考.

关键词：无证书；跨域认证；密钥协商协议；公钥密码

中图分类号：TP309 **文献标识码**：A

An improved certificateless cross-domain authentication key agreement protocol

LI Huimin[1,2]， LIANG Hongmei[3]， ZHANG Jinhui[1,2]

(1. *School of Mathematics and Finance*, *Putian University*, *Putian* 351100, *China*; 2. *Key Laboratory of Applied Mathematics of Fujian Province University* (*Putian University*), *Putian* 351100, *China*; 3. *School of Mathematics and Statistics*, *Minnan Normal University*, *Zhangzhou* 363000, *China*)

Abstract: Aiming at the security problems of CAKA protocol proposed in reference [11], which can not authenticate each othery's identity and will be threatened by replacement public key attack easily, this paper presents an improved protocol. The protocol improves the three steps in the original protocol, so that users on both sides of the protocol must use all their private keys in the process of executing the protocol, and add their identity information to the messages sent by both sides of the protocol. Experiments show that the improved protocol can not only overcome the security problem in the original protocol, but also improve the computational efficiency. Therefore, the improved protocol proposed in this paper has a good reference value for the key agreement protocol based on certificateless public key system, and can also provide a good reference for the analysis and design of similar cross domain key agreement protocols.

Keywords: certificateless; cross-domain authentication; key agreement protocol; public key cryptography

0 引言

随着无线网络的快速发展及其应用的日益普及，无线通信安全(特别是跨域通信安全)问题越来越受到人们的关注. 认证密钥协商(AKA)协议是一种基于公钥密码系统的密码学原语，它不仅能够使用

收稿日期：2021-10-25

基金项目：福建省自然科学基金(2020J01905)；福建省教育厅中青年教师教育科研项目(JAT200514)；莆田市科技计划项目(2021R4001-10)

作者简介：李慧敏(1986—)，女，硕士，讲师，研究方向为信息安全.

户在开放的网络环境下通过协商生成会话密钥,还可以使用户彼此认证双方身份.公钥密码系统主要包括基于目录公钥密码系统[1]、基于身份公钥密码系统[2]、基于证书公钥密码系统[3]和无证书公钥密码系统[4].由于无证书公钥密码系统能够克服传统公钥密码系统的证书管理问题和基于身份公钥密码系统的密钥托管问题,因此一些无证书密钥协商协议相继被一些学者提出[5-10],并被应用于一些需要跨域通信的场景中,如无线网状网络(WMN)、铁路运输管理信息系统、车联网 VANETs、Ad Hoc 网络和 5G 网络等[11-15].2016 年,Li 等[11]基于无证书公钥密码系统建立了一种应用于无线网状网络的无证书跨域密钥协商(CAKA)协议,该协议不仅具备无证书公钥密码系统的优点,而且能降低 Internet 服务提供者(ISP)的计算和通信开销;但本文对文献[11]中的密钥协商协议进行安全性分析后发现,其存在无法认证对方身份及易被替换公钥攻击的安全性问题,对此本文给出了原协议无法认证对方身份的具体原因和对原协议进行替换公钥攻击的具体步骤,并在文献[11]中的协议基础上给出了一种改进的密钥协商协议,同时通过实验验证了该协议的有效性.

1 相关理论

1.1 双线性对的定义

假设 q 是一个素数,G_1 是 q 阶加法群,G_2 是 q 阶乘法群,P 是 G_1 的生成元,则双线性对为如下映射 $e:G_1\times G_1\rightarrow G_2$,且满足下列关系:

1) 双线性.任意的 $P,Q,R\in G_1$,$n\in Z_q^*$ 均满足 $e(P+Q,R)=e(P,R)e(Q,R)$,$e(nP,Q)=e(P,nQ)=e(P,Q)^n$.

2) 非退化性.对于任意的 $P,Q\in G_1$,存在 $e(P,Q)\neq 1_{G_2}$.

3) 可计算性.对于任意的 $P,Q\in G_1$,都有一个有效算法来计算 $e(P,Q)\in G_2$.

1.2 困难性问题

本文协议的安全性主要涉及以下 3 类困难性问题[16]:

1) 计算 Diffie-Hellman 问题(CDHP).已知(P,aP,bP),对于任意的 $a,b\in Z_q^*$ 和 $P\in G_1$,计算 abP.

2) 双线性 Diffie-Hellman 问题(BDHP).给定 P、aP、bP、cP,对于任意未知的 $a,b,c\in Z_q^*$,计算 $e(P,P)^{abc}\in G_2$.

3) 离散对数问题(DLP).对任意的 $U\in G_1$,$V\in G_2$,计算 $a,r\in Z_q^*$ 满足 $U=aP$,$V=e(P,Q)^r$.

1.3 认证密钥协商协议的安全属性

假设A和B是执行AKA协议的两个已完成相互认证,并已建立用于安全通信会话的密钥网格实体(如网状客户端、网状路由器等),则 AKA 协议必备的安全属性为[17]:

1) 已知会话密钥安全.AKA 协议的每个执行过程都应生成一个唯一、独立的秘密会话密钥,这样即使一个密钥泄漏也不会影响其他会话密钥的安全性,从而避免会话密钥被攻击者用以冒充其他实体.

2) 前向安全性.A 和 B 之间的长期密钥如果被泄露,则不会对之前的会话密钥产生威胁.前向安全性通常分为完全前向安全性和主密钥前向安全性两类.完全前向安全性是指即使攻击者拥有 A 和 B 的私钥,也无法知道 A 和 B 之间以前使用的会话密钥;主密前向安全性是指即使攻击者获得了系统主密钥,也无法获得 A 和 B 之间以前的会话密钥.

3) 抗密钥泄露伪装.如果协议参与方 A 的长期密钥被泄露,则攻击者虽可以伪装成 A 参与会话,但无法伪装成其他人,即其他用户不会因为 A 的密钥被破解而受到影响.

4) 未知密钥共享安全.协议参与方如果要进行会话,需要先对双方的身份进行认证.

5) 抗密钥控制.当 A 和 B 需要建立会话密钥时,任何一方都不能生成和自己期望值一样的会话密钥.

2　文献[11]中的无证书跨域认证密钥协商协议及其安全性分析

2.1　文献[11]中的无证书跨域认证密钥协商协议

文献[11]中提出的无证书跨域认证密钥协商协议(简称CAKA协议)中规定，A和B之间需通过一轮消息交换完成A和B的相互认证，并由此建立一个会话密钥k. CAKA协议的具体执行步骤如下：

1) 建立系统参数. 利用CA(Certificate Authority)生成参数$(P,G_1,G_2,q,H_1,H_2,e(\cdot,\cdot))$并公开，其中$P$是$G_1$的生成元，素数$q$是$G_1$和$G_2$的阶数，$e(\cdot,\cdot)$是一个双线性映射，$H_1:\{0,1\}^*\times G_1\rightarrow G_1^*$和$H_2:G_2\times G_1\rightarrow\{0,1\}^l$是CA选择的两个安全的单向hash函数，$l$是对称加密算法中的会话密钥长度.

2) 生成域公钥. 在域D内，ISP选择$s_D\in Z_q^*$作为域主密钥，并将$p_D(p_D=s_DP)$作为D的域公钥. 下文中将用户A所属的域公钥记为p_{D_A}，将用户B对应的域公钥记为p_{D_B}.

3) 生成用户公钥/私钥. ISP将域公钥和域信息注册到CA，用户U随机选择秘密值$k_U\in Z_q^*$并计算$X_U=k_UP$，然后再将$p_U=\langle I_U,X_U\rangle$作为用户U的公钥，其中$I_U$是用户U的真实身份(如姓名或电子邮件地址). 这里假设每个网格用户在其域中具有唯一的标识.

用户U的私钥将由U和它的ISP通过以下两个步骤生成：

① 提取部分私钥. 首先计算$E_U=s_DQ_U$(其中$Q_U=H_1(I_U\|X_U)\in G_1$)，然后通过一个安全的途径将E_U发给U.

② 设置私钥. 用户U收到E_U后，判断$e(E_U,P)=e(Q_U,p_D)$是否成立. 如果等式成立，则E_U是正确的，并将用户U的私钥设置为$s_U=\langle k_U,E_U\rangle$.

系统完成上述的初始化后，用户A和用户B即可建立会话密钥并相互认证，其过程如图1所示.

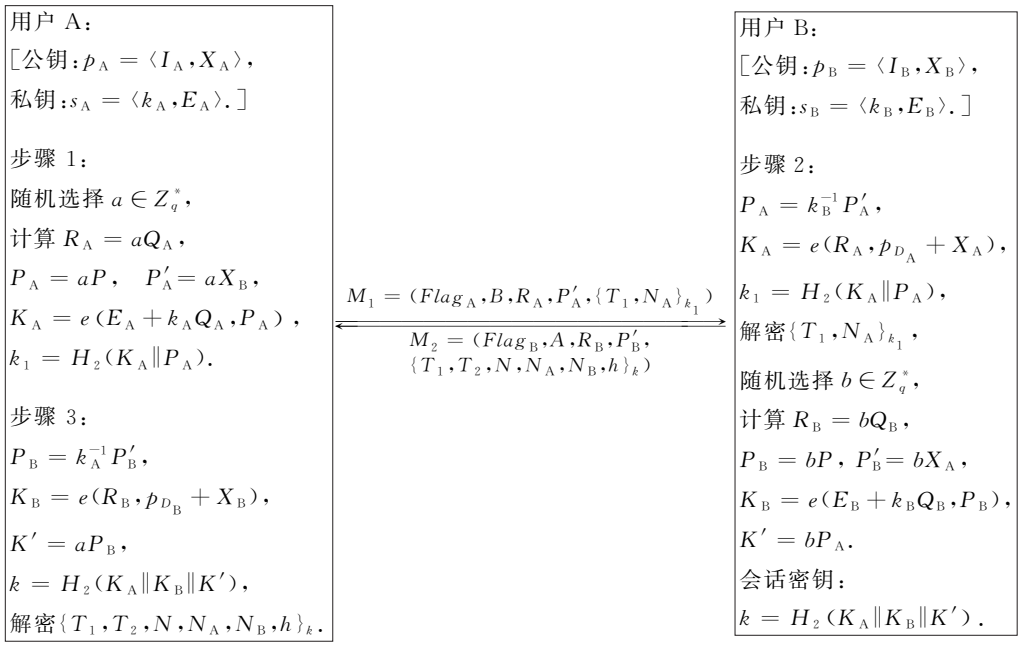

图1　CAKA协议交互图

2.2　文献[11]中的无证书跨域认证密钥协商协议的安全性问题

对CAKA协议进行安全性分析可得如下结果：

1) 无法验证另一方的身份. 在CAKA协议中，任何人可以通过发送者发送的消息来获取发送者的身份信息，冒充者可以假装为消息的原始发送者与另一方通信，进而使得该协议存在另一方身份无法认证的安全问题. 其原因是该协议在执行过程中要求按式(1)进行身份认证，并以此建立密钥.

$$K_A=e(E_A+k_AQ_A,P_A)=e(s_{D_A}Q_A+k_AQ_A,aP)=e((s_{D_A}+k_A)Q_A,aP)=$$
$$e((s_{D_A}+k_A)P,aQ_A)=e(R_A,P_{D_A}+X_A). \quad (1)$$

由式(1)可知 $K_A=e(R_A,P_{D_A}+X_A)$,但由于 P_{D_A} 和 X_A 是公开的,所以只要获得 R_A 就可以计算出 K_A.另外,由于 R_A 在协议执行过程的第1步中是以明文传输的,即任何人通过发送的信息均可获得 R_A,因此协议中的第1步无法实现认证对方身份的目的.

2)替换公钥攻击.由于CAKA协议是基于无证书公钥密码系统建立的,因此需要考虑对该协议的替换公钥攻击.本文对CAKA协议进行替换公钥攻击的具体步骤如下:

首先攻击者随机选取 $k_A^*\in Z_q^*$,并计算 $p_A^*=\langle I_A,X_A^*\rangle=\langle I_A,k_A^*P\rangle$;然后将用户A的公钥替换为 p_A^*,并执行如下步骤:

步骤1 首先随机选择 $a^*\in Z_q^*$,并计算 $R_A^*=a^*Q_A$, $P_A^*=a^*P$, $(P_A^*)'=a^*X_B$, $K_A^*=e(R_A^*,p_{D_A}+X_A^*)$, $k_1^*=H_2(K_A^*\|P_A^*)$;然后将第1个消息 $M_1=(Flag_{A^*},B,R_A^*,(P_A^*)',\{T_1,N_{A^*}\}_{k_1^*})$ 发送给B,其中 $Flag_{A^*}=\langle D_A,p_{D_A},p_A^*,Q_A\rangle$ 是标志用户A的标识符,T_1 是WMN系统时间,N_{A^*} 是一个随机数.

步骤2 B收到消息 M_1 后进行如下操作:① 计算 $P_A^*=k_B^{-1}(P_A^*)'$, $K_A^*=e(R_A^*,P_{D_A}+X_A^*)$ 和 $k_1^*=H_2(K_A^*\|P_A^*)$.② 对 $\{T_1,N_A\}_{k_1^*}$ 进行解密,如果 T_1 和 N_A 是新鲜的,则通过认证.③ 随机选择 $b\in Z_q^*$,并计算 $R_B=bQ_B$, $P_B=bP$, $(P_B^*)'=bX_A^*$, $K_B=e(E_B+k_BQ_B,P_B)$, $(K^*)'=bP_A^*$.④ 计算会话密钥 $k=H_2(K_A^*\|K_B\|(K^*)')$.⑤ 选择 $T_2=T_1+\Delta T$ 和 $N\in Z$,如果攻击者在时限 T_2 内重复访问 D_B 的次数小于 N,则用户B将 $(Flag_{A^*},Flag_B,P_A^*,P_B,T_1,T_2,N,h^*,Num)$ 添加到跨域身份验证列表中(CAL),其中 $h^*=H_2(Flag_{A^*}\|T_1\|T_2\|N\|k)$, $Flag_B$ 为标志用户B的标识符,Num 表示当前访问的数量(如果是第1次访问,则 $Num=1$).⑥ 随机选取 N_B,并将消息 $M_2=(Flag_B,A^*,R_B,(P_B^*)',\{T_1,T_2,N,N_{A^*},N_B,h^*\}_k)$ 发送给A.

步骤3 攻击者收到 M_2 后进行如下操作:① 验证域 D_B 的公钥 p_{D_B} 和用户B的公钥 p_B.② 验证通过后计算 $P_B=(k_A^*)^{-1}(P_B^*)'$, $K_B=e(R_B,p_{D_B}+X_B)$ 和 $(K^*)'=a^*P_B$.③ 获得会话密钥 $k=H_2(K_A^*\|K_B\|(K^*)')$.

由以上可知,攻击者按上述操作即可成功冒充用户A,然后与用户B进行交互并获取会话密钥.用户B是通过式(2)对消息发送者进行身份验证并建立会话密钥的,由式(2)可知上述攻击是可以实现的.

$$K_A^*=e(E_A+k_A^*Q_A,P_A^*)=e(s_{D_A}Q_A+k_A^*Q_A,a^*P)=e((s_{D_A}+k_A^*)Q_A,a^*P)=$$
$$e((s_{D_A}+k_A^*)P,a^*Q_A)=e(s_{D_A}P+k_A^*P,a^*Q_A)=e(p_{D_A}+X_A^*,R_A^*)=e(R_A^*,p_{D_A}+X_A^*). \quad (2)$$

3 改进的跨域认证密钥协商协议及其安全性分析

3.1 改进的跨域认证密钥协商协议

原协议之所以无法实现双方认证的目的和会受到替换公钥攻击是因为验证式(1)中没有用到用户的全部私钥(密钥生成中心生成的部分私钥和用户自己选的秘密值),攻击者可以通过发送的消息获取到发送者的身份信息.本文改进的协议中用户公私钥产生的方式与文献[11]一样,但对文献[11]协议中的交互认证和密钥协商的过程(3个步骤)进行了改进.改进方法为:用户A和B在执行协议的过程中必须使用全部私钥,且在用户A和B发送的消息中分别加入各自的身份信息,同时攻击者无法通过发送的消息获取发送者的身份信息.本文提出的跨域认证密钥协商协议中的系统初始化与文献[11]中的系统初始化相同,认证和会话密钥的建立过程如图2所示.

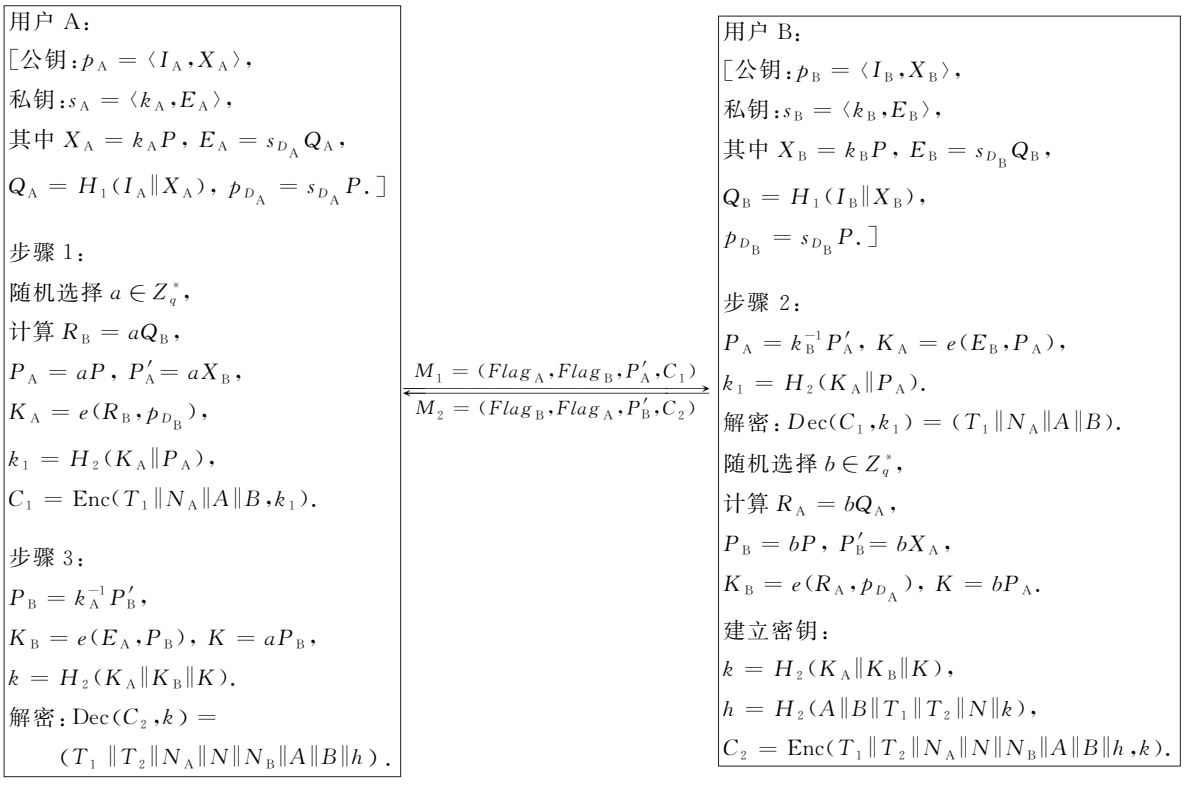

图 2　改进的交互认证和密钥协商过程

本文改进协议的交互认证和密钥协商过程的具体步骤如下：

步骤 1　首先用户 A 随机选择 $a\in Z_q^*$，并计算 $R_B=aQ_B$，$P_A=aP$，$P'_A=aX_B$，$K_A=e(R_B,p_{D_B})$，$k_1=H_2(K_A\|P_A)$ 和 $C_1=\mathrm{Enc}(T_1\|N_A\|A\|B,k_1)$；然后将第 1 个消息 $M_1=(Flag_A,Flag_B,P'_A,C_1)$ 发送给 B，其中 $Flag_A=\langle D_A,p_{D_A},p_A\rangle$ 和 $Flag_B=\langle D_B,p_{D_B},p_B\rangle$ 分别是表示标志用户 A 和用户 B 的标识符，T_1 是 WMN 系统时间，N_A 是随机数，C_1 表示利用 k_1 对消息 $(T_1\|N_A\|A\|B)$ 进行加密后的密文（C_1 对应的明文中加入了 A 和 B 的身份信息.）

注：该步骤将原协议步骤 1 中的 $K_A=e(E_A+k_AQ_A,P_A)$ 改为 $K_A=e(R_B,p_{D_B})$，并还需计算 $C_1=\mathrm{Enc}(T_1\|N_A\|A\|B,k_1)$. 另外，用户 A 发送给用户 B 的消息也由原方案中的 $M_1=(Flag_A,B,R_AP'_A,\{T_1,N_A\}_{k_1})$ 改为 $M_1=(Flag_A,Flag_B,P'_A,C_1)$.

步骤 2　用户 B 收到 M_1 后执行下列操作：① 验证域 D_A 的公钥 p_{D_A} 和用户 A 的公钥 p_A. 如果 p_{D_A} 和 p_A 无效，则 B 终止通信；否则，B 计算 $P_A=k_B^{-1}P'_A$，$K_A=e(E_B,P_A)$ 和 $k_1=\mathrm{H}_2(K_A\|P_A)$，并利用密钥 k_1 对 C_1 进行解密 $\mathrm{Dec}(C_1,k_1)=(T_1\|N_A\|A\|B)$，从而得到 T_1 和 N_A. 如果 T_1 和 N_A 是新鲜的，则 B 认为 M_1 是来自 A 的新消息. ② 随机选择 $b\in Z_q^*$，并计算 $R_A=bQ_A$，$P_B=bP$，$P'_B=bX_A$，$R_A=bQ_A$，$K_B=e(R_A,p_{D_A})$ 和 $K=bP_A$，由此再进一步计算即得计算会话密钥 $k(k=\mathrm{H}_2(K_A\|K_B\|K))$. ③ 选择 $T_2=T_1+\Delta T$ 和 N，N 表示用户 A 在时间限制 T_2 内可以重新访问域 D_B 的最大次数. 如果访问时刻仍然在 T_2 内且访问次数小于 N，则用户 B 将 $(Flag_A,Flag_B,P_A,P_B,T_1,T_2,N,h,Num)$ 添加到 CAL，其中 $h=H_2(A\|B\|T_1\|T_2\|N\|k)$，$Num$ 表示当前访问的次数，如果是第 1 次访问则 $Num=1$. ④ 随机选择一个 N_B，计算 $C_2=\mathrm{Enc}(T_1\|T_2\|N_A\|N\|N_B\|A\|B\|h,k)$，然后将消息 $M_2=(Flag_B,Flag_A,P'_B,C_2)$ 发送给 A.

注：该步骤将原协议步骤 2 中的 $K_A=e(R_A,p_{D_A}+X_A)$ 改为 $K_A=e(E_B,P_A)$，将 $K_B=e(E_B+k_BQ_B,P_B)$ 改为 $K_B=e(R_A,p_{D_A})$，这里的 $K_A=e(E_B,P_A)$ 与步骤 1 中的 $K_A=e(R_B,p_{D_B})$ 是相等的.

另外,还需计算$h=H_2(A\|B\|T_1\|T_2\|N\|k)$,$C_2=\mathrm{Enc}(T_1\|T_2\|N_A\|N\|N_B\|A\|B\|h,k)$,同时用户B发送给用户A的消息也由原协议中的$M_2=(Flag_B,A,R_B,P'_B,\{T_1,T_2,N,N_A,N_B,h\}_k)$改为$M_2=(Flag_B,Flag_A,P'_B,C_2)$.

步骤3 用户A收到M_2后执行如下操作:① 验证域D_B公钥p_{D_B}和用户B的公钥p_B.如果p_{D_B}和p_B无效,则A终止通信;否则,A计算$P_B=k_A^{-1}P'_B$,$K_B=e(E_A,P_B)$和$K=aP_B$,以此获得会话密钥$k=H_2(K_A\|K_B\|K)$.② 利用密钥k解密C_2,即$\mathrm{Dec}(C_2,k)=(T_1\|T_2\|N_A\|N\|N_B\|A\|B\|h)$.④ 由于随机数$N_A$是A自己选择的,所以可判断$N_A$是否新鲜,从而A可以确认该消息是否是用户B发送的密钥协商消息,进而完成对用户B的验证并取得会话密钥k.

注:该步骤将原协议步骤3中的$K_B=e(R_B,p_{D_B}+X_B)$改为$K_B=e(E_A,P_B)$,这里的K_B和步骤2中的$K_B=e(R_A,p_{D_A})$是相等的.

3.2 改进CAKA协议的正确性和安全性分析

3.2.1 协议的正确性分析

协议的正确性可由下式验证:

$$K_A=e(R_B,p_{D_B})=e(aQ_B,s_{D_B}P)=e(aP,s_{D_B}Q_B)=e(P_A,E_B)=e(E_B,P_A),$$

$$K_B=e(R_A,p_{D_A})=e(bQ_A,s_{D_A}P)=e(bP,s_{D_A}Q_A)=e(P_B,E_A)=e(E_A,P_B),$$

$$K=bP_A=baP=abP=aP_B.$$

由上式易知,本文提出的协议是正确的.

3.2.2 协议的安全性分析

1)已知会话密钥的安全性.由图2可以看出,会话密钥是由用户A和用户B通过随机选择$a,b\in Z_q^*$和$H_2(\cdot)$共同确定的,只有取得k_B和E_B的指定用户B才能计算出P_A和K_A,进而得到k_1和消息$(T_1\|N_A\|A\|B)$.另外,只有当$a\neq a'$或$b\neq b'$时,$k=H_2(K_A\|K_B\|K)=H_2(e(E_B,P_A)\|e(E_A,P_B)\|abP)$才不等于$H_2(e(E'_B,P'_A)\|e(E'_A,P'_B)\|a'b'P)$.这是因为$a$和$b$分别是用户A和B随机选择的,$k$可以看作是均匀分布在$\{0,1\}^l$上的随机输出.因此,即使攻击者能够得到$k$,但根据hash函数的单向性和循环乘法群中的DLP假设可知攻击者获知a和b的概率可以忽略不计.由以上可知,泄露其中一个会话密钥不会影响其他会话密钥的安全性.

2)前向安全性.假设用户A的长期私钥$s_A=\langle k_A,E_A\rangle$被敌手A′得到,此时可能出现当一个用户伪装成一个CAKA请求者或一个跨域AKA接收者时(如图2中的用户A),A′可以截取之前的对话信息并计算$K_A(K_A=e(E_B,P_A))$和$K_B(K_B=e(E_A,P_B))$,但无法计算得到密钥$k(k=H_2(K_A\|K_B\|K))$.因为根据G_1中的DLP和CDHP假设,敌手无法从P_A获得a或从P_B获得b,从而无法计算$K=abP$.因此,即使用户A或用户B的私钥被泄露,先前会话密钥也不会被泄露,由此可知前向安全性是可靠的.

3)抗密钥泄露伪装.假设敌手获得了用户A的长期私钥$s_A(s_A=\langle k_A,E_A\rangle)$,这时敌手虽然可以模拟用户A发起CAKA请求或伪装AKA接收者,但无法从交互中获取其他用户的长期私钥,即即使用户A的私钥被泄露,其他用户私钥的安全性也不会受到影响.

4)未知密钥共享安全.在改进的CAKA协议中由于使用了指定验证者的技术,会话密钥只能由CAKA请求者和接收者计算,任何其他第三方都不能强迫用户A与其他用户共享密钥,除非双方都执行图2中的CAKA协议.这是因为只有指定的接收者B才能获得$P_A(P_A=aP)$、$k_1(k_1=H_2(K_A\|P_A))$、会话密钥$k(k=H_2(K_A\|K_B\|K))$和对消息M_1的解密,而M_1的解密需要隐式身份验证.文献[18]已证明隐式认证特性隐含未知密钥共享的弹性.

5)抗密钥控制.由于会话密钥$k(k=H_2(K_A\|K_B\|K)=H_2(e(E_B,P_A)\|e(E_A,P_B)\|abP))$是由随机数$a,b\in Z_q^*$和$H_2(\cdot)$共同确定的,因此请求者和接收者都不能控制$k$为预选值.另外,虽然请求者可

以通过改变随机数 a 来选择一个理想的散列值，但由于 a 或 b 的微小改变都会较大改变 hash 函数的输出，即产生雪崩效应，因此请求者无法控制 k 值.

6）抗中间人攻击. 抗中间人（MITM）攻击是协议两方最容易受到的一种攻击. 假设最常见的敌手 A′ 以不可检测的方式对密钥交换协议发起 MIMT 攻击. 在发动 MIMT 攻击时，敌手 A′ 截获用户 A 发送给用户 B 的数据，或者可以假设敌手 A′ 更强大，其掌握了随机选择的数 $a'\in Z_q^*$，但是敌手 A′ 不知道用户 A 的全部私钥，其计算 $R_B=a'Q_B$，$P'_A=aP$，$P''_A=aX_B$，$K'_A=e(R_B,p_{D_B})$，$k'_1=H_2(K'_A\|P'_A)$，$C'_1=\mathrm{Enc}(T'_1\|N'_A\|A\|B,k'_1)$，发送 $M'_1=(Flag_A,Flag_B,P''_A,C'_1)$ 给用户 B. 用户 B 遵照协议发送 $M_2=(Flag_B,Flag_A,P'_B,C_2)$ 给用户 A，此时，敌手 A′ 可以随意截获该数据，但是由于敌手 A′ 在不知道用户 A 的私钥（即不知道 k_A 和 E_A）的情况下无法计算出 $P_B=k_A^{-1}P'_B$ 和 $K_B=e(E_A,P_B)$，从而无法计算得到 K 和 k，所以只有指定的客户端才能正确地对加密的消息进行解密. 因此，敌手 A′ 充当中继节点，无法获取会话密钥或私钥.

在无证书公钥系统下，由于替换公钥攻击是针对无证书方案的一种基本攻击，所以 MITM 攻击也有可能由 ISP 或获得 ISP 主密钥的敌手 A_1 或 A_2 发起，其中敌手 A_1 可以随意更改客户端的公钥，但不能访问系统主密钥；敌手 A_2 可以掌控系统主密钥，但不能替换客户端的公钥[19]. 如文献[18]所述，抵抗替换公钥攻击的一种方法是绑定用户的公钥和私钥，本文采用的方法是将用户 A 的身份 I_A 和固定公钥 X_A 与部分私钥绑定，即 $E_A=s_{D_A}H_1(I_A\|X_A)$. 因此，敌手在不知道私钥的情况下不能从替换的公钥中获得部分私钥 E_A，即使敌手 A_1 可以替换公钥 $X'_A=k'_AP$，$Q'_A=H_1(I_A\|X'_A)$，$R_A=a'Q'_A$ 并成功假扮用户 A，但在 CDHP 的假设下，他仍然无法根据 $a'bP$、P'_B 计算出正确的 P_B. 对于敌手 A_2，他可以访问域主密钥 s_D，但不能替换客户端的公钥，所以即使敌手 A_2 知道部分私钥 E_A，他仍然不能在不知道 s_A 的情况下伪装用户 A 来计算 K_A. 因此，两种类型的敌手都无法在不知道两个客户端完整私钥的情况下计算出会话密钥，从而说明本文改进的 CAKA 协议可以抵御 MITM 攻击.

3.3　改进 CAKA 协议的效率分析

本文通过计算协议涉及的主要密码运算[20] 的个数对本文改进的协议与文献[11]中的协议进行对比分析，计算中分别用 T_m、T_p 和 T_a 表示 G_1 中的点乘运算、双线性对运算和加法运算，用 T_e 表示 AES（Advanced Encryption Standard）对称加密运算，用 T_h 表示哈希运算 H_2，计算结果见表 1. 使用 PBC 库（版本 0.5.14）在 64 位、2.4 GHz 基于 Intel Core i7-5500U 处理器、4 GB 主内存、Windows 7 系统的电脑上测试所有这些计算，各运算的执行时间见表 2.

表 1　两个协议涉及的主要密码运算个数

协议	用户 A 执行协议所需密码运算的个数					用户 B 执行协议所需密码运算的个数				
	T_e	T_m	T_p	T_h	T_a	T_e	T_m	T_p	T_h	T_a
文献[11]中的协议	1	6	2	2	2	1	6	2	1	2
本文改进的协议	1	5	2	2	0	1	5	2	2	0

表 2　运算执行时间　　ms

T_e	T_m	T_p	T_h	T_a
30.400	8.006	16.064	0.600	0.038

为了更好的比较两种协议的性能，根据表 1 和表 2 计算出了两个协议中用户 A 和用户 B 的执行时间及协议总的执行时间，见图 3. 由图 3 可以看出，本文改进的协议不仅解决了文献[11]中存在的安全问题，而且还提高了效率. 其中用户 A 的执行时间提高了 7.23%，用户 B 的执行时间提高了 6.73%，协议总执行时间提高了 6.98%.

4 结论

对本文提出的改进的无证书跨域密钥协商协议进行实验表明,该协议不仅解决了文献[11]中存在的无法验证双方身份问题和容易受到替换公钥攻击的安全问题,而且还提高了协议的执行效率.本文的改进方法还可为同类跨域密钥协商协议的设计提供良好的参考价值.本文在研究中仅考虑了两个用户在跨域情景下的密钥协商协议,今后我们将对跨域环境下的多方密钥协商协议进行研究,从而实现跨域环境下的多方安全通信.

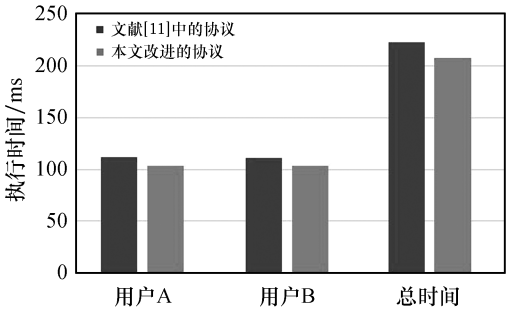

图3 两种协议的执行时间

参考文献:

[1] GUTMANN P. PKI: It's not dead, just resting[J]. Computer, 2002,35(8):41-49.

[2] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Workshop on the Theory and Application of Cryptographic Techniques. Berlin-Heidelberg: Springer, 1984:47-53.

[3] GENTRY C. Certificate-based encryption and the certificate revocation problem[C]//Advanes in Cryptology: EUROCRYPT 2003, LNCS: 2656. Berlin: Springer-Verlag, 2003:272-293.

[4] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin-Heidelberg: Springer, 2003:452-473.

[5] 周彦伟,杨波,张文政.一种改进的无证书两方认证密钥协商协议[J].计算机学报,2017,40(5):1181-1190.

[6] 顾兆军,刘东楠.基于身份的无证书双线性对密钥协商方案[J].中国民航大学学报,2019,37(1):55-59.

[7] 曾润智,王立斌.一种高效的无证书认证密钥交换协议[J].密码学报,2019,7(4):421-429.

[8] 许盛伟,任雄鹏,陈诚,等.可证安全的无证书两方认证密钥协商协议[J].密码学报,2020,7(6):886-898.

[9] 马骁,施运梅,宋莹,等.一种无证书的跨域量子密钥协商协议[J].太赫兹科学与电子信息学报,2020,18(6):1098-1102.

[10] TAO F S, SHI T, LI S J. Provably secure cross-domain authentication key agreement protocol based on heterogeneous signcryption scheme[C]//2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). Chongqing: IEEE, 2020,1:2261-2266.

[11] LI Y P, CHEN W F, CAI Z P, et al. CAKA: A novel certificateless-based cross-domain authenticated key agreement protocol for wireless mesh networks[J]. Wireless Network, 2016,22(8):2523-2535.

[12] LIU X, MA W. CDAKA: A provably-secure heterogeneous cross-domain authenticated key agreement protocol with symptoms-matching in TMIS[J]. Journal of Medical Systems, 2018,42(8):135.

[13] ZHOU Y S, LONG X W, CHEN L J, et al. Conditional privacy-preserving authentication and key agreement scheme for roaming services in VANETs[J]. Journal of Information Security and Applications, 2019,47:295-301.

[14] 曹震震,顾小卓,顾梦鹤.面向Ad Hoc网络的无证书认证组密钥协商协议[J].计算机应用,2019,39(2):476-482.

[15] LUO M, WU J Y, LI X J. Cross-domain certificateless authenticated group key agreement protocol for 5G network slicings[J]. Telecommunication Systems, 2020,74(4):437-449.

[16] BONEH D, FRANKLIN M. Identity-based encryption from the weil pairing[J]. SIAM Journal on Computing, 2003,32(3):586-615.

[17] WANG S B, CAO Z F, CHENG Z H, et al. Perfect forward secure identity-based authenticated key agreement protocol in the escrow mode[J]. Science in China Series F: Information Sciences, 2009,52(8):1358-1370.

[18] SHI Y, 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.

[19] HUANG X Y, MU Y, SUSILO W, et al. Certificateless signatures: new schemes and security models[J]. The Computer Journal, 2012,55(4):457-474.

[20] 李发根,吴威峰.基于配对的密码学[M].北京:科学出版社,2014:42.