软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(11):2843−2852 [doi: 10.3724/SP.J.1001.2011.03942]

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

无证书两方密钥协商方案*

刘文浩[1+], 许春香[2]

[1](杭州师范大学 信息科学与工程学院,浙江 杭州 310012)

[2](电子科技大学 计算机科学与工程学院,四川 成都 611731)

Two Party Certificateless Key Agreement Schemes

LIU Wen-Hao[1+], XU Chun-Xiang[2]

[1](School of Information Science and Engineering, Hangzhou Normal University, Hangzhou 310012, China)

[2](School of Computer Science and Engineering, University of Electronic Science and Technology, Chengdu 611731, China)

+ Corresponding author: E-mail: whl819_819@163.com

Liu WH, Xu CX. Two party certificateless key agreement schemes. *Journal of Software*, 2011,22(11): 2843−2852. http://www.jos.org.cn/1000-9825/3942.htm

Abstract: A pairing-free certificateless two party key agreement scheme (CL-KA) is proposed. This work is able demonstrates all existing CL-KA schemes (except for Lippold's scheme) are insecure in the eCK model. The scheme is secure in the eCK model as long as each party has at least one uncompromised secret. The scheme has proven to be secure in the random oracle model (ROM), assuming that the computational Diffie-Hellman assumption hold even if the key generation centre (KGC) learns the ephemeral secrets of both parties, or reveal secret values/replace public keys, but not both. The scheme eliminates pairing computation. It achieves efficiency in computational cost when compared with all the other known certificateless key agreement schemes. The scheme is more suitable for the restricted bandwidth of the communication environment, such as ad hoc networks, wireless sensors, and so on.

Key words: key agreement; two party protocol; certificateless; without bilinear pairing

摘 要: 给出了一个无双线性对的无证书两方密钥协商方案,并演示了这些不安全无证书方案存在的攻击.只要每方至少有 1 个未泄露的秘密值,该方案在最强的安全模型下就是安全的.即使密钥生成中心知道双方的临时私钥或显示双方的秘密值/替换公钥(但不能同时),但只要计算 Diffie-Hellman 假设成立,该方案在随机预言机模型下也被证明是安全的.该方案消除了对运算,与其他无证书密钥协商方案相比,该方案是已知无证书安全协商方案中计算复杂度最低的.该方案尤其适合于带宽受限的通信环境中使用,如 Ad Hoc 网络、无线传感器网络等.

关键词: 密钥协商;两方协议;无证书;无双线性对

中图法分类号: TP309 **文献标识码**: A

在传统的基于公钥证书的密码体制下,用户的公钥由证书权威机构颁发证书来认证,公钥证书的管理过程复杂且代价极高.为了简化证书的管理过程,1984 年,Shamir[1]首次提出了基于身份的密码体制.在基于身份的密

* 基金项目: 国家高技术研究发展计划(863)(2009AA01Z415)
收稿时间: 2010-05-24; 修改时间: 2010-08-13; 定稿时间: 2010-09-10

码体制中,使用能够唯一代表用户身份的公开信息(如电话号码或邮箱等)来代表用户的公钥,用户的公钥不再需要证书权威机构颁发证书认证.基于身份的密码体制克服了公钥证书复杂性管理,但由于用户的私钥由可信密钥生成中心(key generation center,简称 KGC)产生,基于身份的密码体制带来了密钥托管新问题.Al-Riyami 和 Paterson[2]在 2003 年的亚密会上第一次提出了无证书公钥密码学概念.它解决了基于身份密码学中用户密钥托管问题,并保持了用户公钥不需使用公钥证书来认证的优点.2005 年,他们又提出了关于无证书的一个普遍构造与有效方案[3].然而,文献[3]中并没有给出无证书密钥协商的安全模型和安全证明.随后,一些研究者相继提出了不同的无证书两方认证密钥协商协议[4−7],但是这些协议都不能抵抗密钥泄露伪装攻击和临时私钥泄露产生的攻击.Zhang 和 Swanson 分别在文献[8]和文献[9,10]中详细分析了对上述方案产生的攻击.基于 LaMcchia 等人[11]提出的扩展 CK(extended Canetti-Krawczyk,简称 eCK)安全模型(eCK 安全模型介绍详见文献[11]),Swanson 定义了无证书两方认证密钥协商协议的安全模型.基于 Swanson[7]提出的安全模型,Lippold[12]提出了无证书两方认证密钥协商协议的一个更强安全模型,并给出了一个可证安全无证书认证协议.它是一个可证安全无证书认证密钥协商协议,但由于该协议使用了 10 次双线性对运算和 5 次指数运算,计算复杂度较高.到目前为止,所有已知的无证书密钥协商方案都采用了双线性对操作,比较指数运算和点乘运算,在有限域中,双线性对运算仍然是比它们更为耗时的运算.按照文献[13],执行一个 512 位 Tate pairing 需要花费 20ms,而一个 1 024 位素数指数操作却只需要 8.80ms.运行一次双线性双线性对操作的时间至少是椭圆曲线上点乘运算的 21 倍[14].因此,无双线性对运算的计算复杂度会更低.

基于身份的协议有一个难以解决的难题——KGC 形成的中间人攻击.如果 KGC 知道了通信中用户的临时私钥,它就可以计算出最终的会话密钥,形成攻击.但在一个安全性很好的无证书密钥协商协议中,只要通信中每方的长期私钥未被泄露,即使 KGC 知道通信中每个用户的临时私钥,它也无法计算出最终的会话密钥.因此,无证书密码学解决了基于基于身份密码学中难以解决的难题.一个好的协议必须满足安全性好,同时效率尽可能高的条件.基于上述无证书方案中要么存在安全漏洞,要么效率不理想的事实,我们对适用于无证书环境的扩展 CK 安全模型作了新的注解,并利用无证书签名技术提出了一个无证书两方密钥协商方案.该方案能够同时满足:(1) 无用户密钥托管,KGC 具有前向安全性;(2) 无密钥泄露伪装攻击(抗 KCI 攻击);(3) 会话时用户临时私钥泄露也不会产生攻击.该方案只需要 1 轮通信,消除了对运算.与 Lippold[12]等人的协议相比,该方案明显降低了计算复杂度.

在无证书密码学方案中,通信中的每方都有 3 个秘密值,分别为 KGC 生成的用户部分私钥、用户自己生成的长期私钥、会话时用户选择的随机临时值(临时私钥).在文献[4–7]的方案中,若攻击者知道了每个用户的两个秘密值就能计算出最终的会话密钥,形成攻击.这就是上述无证书协商方案不安全的根本原因.而在新方案中,即使密钥生成中心(KGC)获得了用户的临时私钥或用户的长期私钥/替换用户的公钥(但不能同时),它也是很安全的.也就是说,每个用户只要有 1 个秘密值未泄露,那么新方案就是安全的,除非敌手能攻破基于底层的计算性 Diffie-Hellman 困难问题(computational diffie-hellman problem,简称 CDHP)和离散对数困难问题(discrete logarithm problem,简称 DLP).一个密钥协商方案如果在越强的敌手攻击模型和越弱的困难性假设下是安全的,该方案就越是很安全的.为了更有条理地分析新方案的安全性和更简洁地演示对文献[4–7]中方案产生的攻击,在最强的敌手攻击模型下(每方只保留一个秘密值,允许敌手获得其他 4 个秘密值),在基于很弱的困难性假设(如 CDH 和 DL 假设)的情况下,我们对文献[9]中的强安全类型重新进行了科学的分类(前者分两类,新方案分为 3 类).

本文第 1 节叙述双线性映射性质和有关困难问题及假设.第 2 节陈述无证书密钥协商安全属性及强安全模型.第 3 节提出一个高效、安全的无证书两方密钥协商方案.第 4 节详细证明新方案的安全性.在第 5 节,使用我们定义的 3 种密钥协商安全类型,简洁地演示目前已知无证书方案在 eCK 模型下产生的各种攻击.第 6 节对比分析新方案与其他无证书方案的优劣情况.第 7 节得出本文的结论.

1 有关困难问题及其假设

计算性 Diffie-Hellman 问题(computational diffie-hellman problem,简称 CDHP):设 G 是阶为 q 的一个加法循环群,P 是它的一个生成元,给定 $aP,bP\in G$,对任意未知 $a,b\in Z_q^*$,计算 abP.

在概率多项式时间内(probabilistic polynomial time,简称 PPT),算法 A 在解决 CDH 问题的优势定义如下:

$$Adv^{CDH}(A)=\Pr[A(aP,bP)=abP \mid a,b\in Z_q^*].$$

CDH 假设:对任意 PPT 算法 A,$Adv^{CDH}(A)$是可以忽略的.

离散对数问题(discrete logarithm problem,简称 DLP):设 G 是阶为 q 的一个循环群,P 是它的一个生成元,给定 $P,aP\in G$,对任意未知 $a\in Z_q^*$,计算 a.

在概率多项式时间内算法 A 在解决 DLP 问题的优势定义如下:

$$Adv^{DLP}(A)=\Pr[A(P,aP)=a \mid a\in Z_q^*].$$

DLP 假设:对任意 PPT 算法 A,$Adv^{DLP}(A)$是可以忽略的.

2 安全模型

2006 年,LaMacchia 等人在文献[11]中为密钥协商方案提出了一个较强的安全模型(被称为 eCK 模型).Georg 等人在文献[12]中陈述了 Swanson[9]模型的一个加强版本(都是基于 eCK 模型).

设 $\Pi_{i,j}^t$ 是用户 i 和 j 和第 t 次会话,如果会话 $\Pi_{i,j}^t$ 和 $\Pi_{j,i}^k$ 有相同的伙伴标识 $PID=(ID_i,ID_j)$,则这两个会话被认为是匹配的会话.安全模拟为游戏,该游戏分为两个阶段.在游戏的第 1 阶段,攻击者 M 允许发生如下查询:

- Send($\Pi_{i,j}^t,x$):如果会话 $\Pi_{i,j}^t$ 不存在,它将被创建一个发起者(如果 x 为空集,则发起者为用户 i;否则,用户 j 是应答者).接到消息 x 后,协议被执行.当用户 i 已经接收和发送协议指定的最后信息后,它输出一个决定接收或拒绝接收会话的标识.
- Reveal mater key:系统的主私钥 s 允许被敌手 M 访问.
- Session key reveal($\Pi_{i,j}^t$):如果会话没有被接收,就返回结束标志⊥;否则,它将返回会话密钥.
- Reveal ID-based secret(i):用户 i 应答其基于身份的私钥(例如 $sH_1(ID_i)$).
- Reveal secret value(i):用户 i 应答它对应于其公钥的秘密值 x_i.如果用户 i 被询问以前的公钥替换查询,则它返回⊥.
- Replace public key(i,pk):攻击者 M 选择自己的公钥 pk 来替换无证书公钥 x_iP.用户 i 将使用新的公钥 pk 来进行通信和计算.
- Reveal ephemeral key($\Pi_{i,j}^t$):在会话时,用户 i 用它的短暂私钥来应答敌手查询.

完成初始化阶段后,敌手允许发起“Test”查询,对于新鲜的会话定义如下:

定义 1(新鲜的会话). 一个会话被认为是新鲜的,假设它满足:(1) $\Pi_{i,j}^t$ 已经接受;(2) $\Pi_{i,j}^t$ 没有发生“Session key reveal($\Pi_{i,j}^t$)”查询;(3) 在会话中没有任何用户被完全腐化(也就是用户的长期私钥、短暂私钥及基于身份的部分私钥没有完全被敌手获得);(4) 与 $\Pi_{i,j}^t$ 匹配的伙伴 $\Pi_{j,i}^k$ 也没有被完全腐化.

- Test($\Pi_{i,j}^t$):输入的会话 $\Pi_{i,j}^t$ 必须是新鲜的.在这种查询中,挑战者随机选择 $b\in\{0,1\}$.如果 b=0,则它返回会话密钥给敌手 M;否则,它返回一个随机比特串.

在完成“Test”查询后,M 继续被允许做以上查询.最后它终止,输出它猜想的一个比特值 b',若被选择的“Test($\Pi_{i,j}^t$)”会话是新鲜的且满足 $b'=b$,则 M 在游戏中获胜.

敌手在游戏中获胜的优势定义为 $Adv_M(k)=|\Pr[b'=b]-1/2|$.如果在 PPT 内不存在敌手以不可忽略的优势 $Adv_M(k)$在游戏中获胜,则该协议被认为是安全的.

设计的安全协议应该能够同时满足:(1) 无用户密钥被托管,KGC 具有前向安全性;(2) 无密钥泄露伪装攻

击(抗 KCI 攻击);(3) 会话时用户临时私钥泄露也不会产生中间人攻击.针对安全协议的基本要求,我们重新定义了 3 种类型的密钥协商安全.

定义 2(类型 I 密钥协商安全). 如果两用户部分私钥泄露,只要其他两个密钥中的 1 个安全,在概率多项式时间内攻击者没有不可忽略的优势在游戏中获胜,则称为类型 I 密钥协商安全.

如果能够满足此类型的安全,则说明该协议具有无密钥托管,同时 KGC 具有前向安全的特性.

定义 3(类型 II 密钥协商安全). 如果两用户长期私钥泄露,只要其他两个密钥中的 1 个安全,在概率多项式时间内攻击者没有不可忽略的优势在游戏中获胜,则称为类型 II 密钥协商安全.

如果能够满足此类型的安全,则表明该方案具有前向安全的特性.

定义 4(类型 III 密钥协商安全). 如果两用户临时私钥泄露,只要其他两个密钥中的 1 个安全,在概率多项式时间内攻击者没有不可忽略的优势在游戏中获胜,则称为类型 III 密钥协商安全.

此类型的安全,主要是防止会话时用户临时私钥被泄露产生的攻击.如果某协议有这种类型的安全,则说明该协议满足已知会话临时信息安全的特性.

3 新的无证书密钥协商方案

(1) 系统参数建立

输入安全参数 k,产生两个大素数 p,q,且 $q|p-1$.P 为椭圆曲线上的循环群 G 中任意一阶为 q 的生成元,选择安全 Hash 函数:

$$H_1:\{0,1\}^*\times G\to Z_q^*, H_2:\{0,1\}^*\to Z_q^*, H:\{0,1\}^*\times\{0,1\}^*\times G^7\to\{0,1\}^k.$$

KGC 随机选择系统主密钥 $x\in Z_q^*$,计算 $y=xP$,系统公开参数(p,q,P,y,H_1,H_2,H),保密 x.

(2) 用户密钥生成

给定用户身份 ID_i,KGC 随机选择 $r_i\in Z_q^*$,计算 $R_i=r_iP, D_i=r_i+xH_1(ID_i,R_i)$,通过安全渠道返回 D_i 给用户 i,并作为其部分私钥.$R_i=r_iP$ 作为用户 i 的部分公钥,并公开 R_i.

用户 ID_i 随机选择 $x_i\in Z_q^*$ 作为其长期私钥,生成对应的私钥(x_i,D_i),计算 $X_i=x_iP$,生成公钥(X_i,R_i),X_i 可以放在公共目录树上.用户 ID_i 可以通过计算等式 $R_i+H_1(ID_i,R_i)y=D_iP$ 是否成立来判断 KGC 分配给自己的部分私钥是否有效.

(3) 身份认证和密钥协商

用户 A 随机选取 $a\in Z_q^*$,计算 $T_A=aP, h_1=H_1(ID_B,R_B), h=H_2(T_A\|ID_A\|m), s=a/(x_A+D_A+h)$,生成签名$(h,s)$(Schnorr 签名的一种变体),并发送消息$(ID_A,h,s)$给用户 B.

用户 B 收到消息(ID_A,h,s)后,计算 $P_A=R_A+H_1(ID_A,R_A)y, h_2=H_1(ID_A,R_A), T_A'=s(X_A+R_A+h_2y+hP)=aP=T_A$,若 $H_2(T_A'\|ID_A\|m)=h$ 成立,则用户 B 通过了对用户 A 的身份验证.

用户 B 随机选取 $b\in Z_q^*$,计算 $T_B=bP$,发送消息(T_B,ID_B)给用户 A,并计算:

$$K_{B1}=x_B(X_A+P_A+T_A)=x_B(x_AP+P_A+aP),$$
$$K_{B2}=D_B(X_A+P_A+T_A)=D_B(x_AP+P_A+aP),$$
$$K_{B3}=b(X_A+P_A+T_A)=b(x_AP+P_A+aP).$$

当用户 A 收到消息后,计算 $P_B=R_B+H_1(ID_B,R_B)y$,计算:

$$K_{A1}=(x_A+D_A+a)X_B=(x_A+D_A+a)x_BP=K_{B1}=K_1,$$
$$K_{A2}=(x_A+D_A+a)P_B=K_{B2}=K_2,$$
$$K_{A3}=(x_A+D_A+a)T_B=(x_A+D_A+a)bP=K_{B3}=K_3.$$

最终会话密钥:

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

4 安全证明

为了证明新方案是安全的,我们首先要证明完成最终会话密钥使用的签名技术具有不可伪造性.在此基础上,新方案按照敌手发生攻击的可能方式划分为 9 种情况进行分析和证明.参照文献[14]中定义的敌手类型,无证书签名方案面临着两种类型的敌手攻击:

类型 1(A_1):攻击者可查询用户公钥或替换合法用户公钥,但不知道系统主密钥;

类型 2(A_2):攻击者可获得系统主密钥,但不能替换合法用户的公钥或查询用户公钥.

无证书签名通用方案及其安全模型介绍见文献[15]中描述.

4.1 签名不可伪造性证明(参考了文献[15]中的证明方法)

定理 1(类型 1 攻击下的不可伪造性). 在 ROM 中,若存在一个(*EUF-CLSC-CMA*)敌手 A_1 能够在概率多项式时间内以ε的优势在游戏中获胜(假设最多进行 q_i 次 H_i 查询,i=1,2),那么存在一个可区分者 Q 能够在概率多项式时间内以 $\varepsilon/(q_1^2 q_2)$ 的优势解决 DL 困难问题.

证明:设 Q 是一个 DL 困难问题的解决者,困难问题的输入为(P,uP),其目标是计算出 u.Q 设置 y=uP,并以 A_1 为子程序并充当(*EUF-CLSC-CMA*)游戏中的挑战者.游戏开始后,Q 发送(p,q,P,y,H_1,H_2)给 A_1,哈希函数 H_1,H_2 看成随机预言机.假设 A_1 在如下的各种查询中均不同:

H_1 查询:Q 维持一个列表 L_1,开始时,该列表被初始化为空表.当 Q 收到 A_1 对 $H_1(ID_i,R_i)$查询时,若列表 L_1 中存在(ID,R,h_1),返回相应的值给 A_1.否则, Q 随机选择新的 $h_1 \in Z_q^*$,并将(ID,R,h_1)加入列表 L_1 中.

H_2 查询:Q 维持一个列表 L_2,开始时,该列表为空表.当 Q 收到 A_1 对 $H_2(m||ID||T)$查询时,若列表 L_2 中存在(m,ID,T,h_2),返回相应的值给 A_1.否则, Q 随机选择 $c\in\{0,1\}$,其中 Pr[c=1]=δ.当 c=0 时,随机选择新的 $h_2 \in Z_q^*$,将 h_2 传给 A_1,把(m,ID,T,h_2,c)加入列表 L_2 中;当 c=1 时,令 h_1=⊥,返回⊥给 A_1.

部分私钥提取查询:Q 维持一个列表:L_D,开始时,该列表为空表.若列表 L_D 中存在(ID,D,R),则返回相应的值给 A_1.否则,Q 随机选择 $D,h_1 \in Z_q^*$,计算 R=DP–yh_1,将(ID,D,R)加入列表 L_D,(ID,R,h_1)加入列表 L_1,将(R,D)传给 A_1.

私钥提取查询:若列表 L_{SK} 中存在(ID,D,x),则返回相应的值给 A_1;否则,Q 查询列表 L_D 得到 D,随机选择 $x \in Z_q^*$,把(ID,D,x)加入列表 L_{SK}.

公钥提取查询:Q 维持一个列表 L_{PK},开始时,该列表被初始化为空表.若列表 L_{PK} 中存在(ID,R,X),则返回相应的值给 A_1;否则.Q 先查询列表 L_D 和 L_{SK},计算 X=xP,将(ID,R,X)加入列表 L_{PK},并返回(R,X)给 A_1.若列表 L_D 和 L_{SK} 中不存在(ID,R,X),则查询列表 L_2:若 c=1,Q 随机选择 $r, x \in Z_q^*$,计算 R=rP,X=xP,将(ID,R,X,c)加入列表 L_{PK},并返回(R,X);若 c=0,则运行部分私钥提取查询,得到(R,D),Q 随机选择 $x \in Z_q^*$,将(ID,D,x),(ID,R,X,c)分别加入列表 L_{SK} 和 L_{PK},并返回(R,X).

公钥替换:用新的公钥 R'替换掉原来的 R 参与计算.

签名查询:Q 先在列表 L_{PK} 查询(ID_B,R_B,X_B,c),若 c=1,则放弃查询,否则查询列表(ID_A,D_A,x_A),随机选 $a \in Z_q^*$,计算 T=aP, $h_1' = H_1(ID_A, R_A)$,h=$H_2(T||ID_A||m)$,s=a/(x_A+D_A+h),返回消息σ=(h,s)给 A_1.

校验签名查询:Q 先在列表 L_{PK} 查询 ID_A:① 若存在,且 c=0,则在列表 L_1 中查询 (ID_A, R_A, h_1'),计算 $T' = s(R_A + X_A + h_1'y + hP)$.若 $H_2(T'||ID_A||m)$=h 成立,则返回“通过验证”,否则终止模拟;② 若存在,且 c=1,则在 L_1 中查询 (ID_A, R_A, h_1'),若存在(m,ID_A,T',h)∈L_2,返回“通过验证”,否则终止模拟;③ 如果列表 L_{PK} 中不存在,那么在列表 L_1 中查询 (ID_A, R_A, h_1'),若存在(m,ID_A,T',h)∈L_2,则返回“通过验证”,否则终止模拟.

经过概率多项式次数上述查询后,A_1 随机选择 $a, s^* \in Z_q^*$,计算 T=aP,h^*=$H_2(ID_A||T||m)$, $h_1' = H_1(ID_A, R_A)$,输出对 m 的有效伪签名σ^*=(h^*,s^*).若伪造签名成功,则 Q 输出 $u = (a - s^*(r_A + x_A + h^*))/h_1's^*$ 作为解决 DL 困难问题的回答;否则,Q 没有解决 DL 困难问题.若 A_1 对 ID_A 进行过部分私钥或私钥查询,则 Q 失败,它不做这种查询的概率为 $1/q_1 \times 1/(q_1 - 1) > 1/q_1^2$;若 A_1 对 T'进行过 H_2 查询,则 Q 失败,它不作这种查询的概率大于 $1/q^2$.因此,Q 解决

DL 困难问题的优势 $Adv^{EUF\text{-}CMA}(A_1) \geqslant 1/q_1^2 q_2$. □

定理 2(类型 2 攻击下的不可伪造性). 在 ROM 中,若存在一个(*EUF-CLSC-CMA*)敌手 A_2 能够在概率多项式时间内以 ε 的优势在游戏中获胜(假设最多进行 q_i 次 H_i 查询,i=1,2),那么存在一个可区分者 Q 能够在概率多项式时间内以 $1/(q_1^2 q_2)$ 的优势解决 DL 困难问题.

证明:假设 Q 是一个 DL 困难问题的解决者,其困难问题输入为(P,vP),其目标是计算出 v.首先,Q 设置 $y=uP$,Q 以 A_1 为子程序并充当(*EUF-CLSC-CMA*)游戏中的挑战者.游戏开始后,Q 发送(p,q,P,y,H_1,H_2)给 A_2,A_2 知道系统主密钥 u,但不能进行公钥替换攻击,其他条件及目标均同定理 1 中给定的.

A_2 可以进行定理 1 中的除“校验签名”和“公钥替换”之外的所有查询.

校验签名查询:Q 先在列表 L_{PK} 查询 ID_A:① 若存在,且 c=0,则在列表 L_1 中查询 (ID_A, R_A, h_1'),计算 $T' = s(R_A + X_A + h_1' y + hP)$.若 $H_2(T'||ID_A||m)=h$ 成立,则返回“通过验证”,否则终止模拟;② 若存在,且 c=1,则在 L_1 中查询 (ID_A, R_A, h_1'),若存在$(m, ID_A, T', h) \in L_2$,则返回“通过验证”,否则终止模拟.③ 如果列表 L_{PK} 中不存在,那么在列表 L_1 中查询 (ID_A, R_A, h_1'),若存在$(m, ID_A, T', h) \in L_2$,则返回“通过验证”,否则终止模拟.

经过概率多项式次数上述查询后,A_2 随机选择 $a, s^* \in Z_q^*$,计算 $T=aP$,$h^*=H_2(ID_A||T||m)$,$h_1' = H_1(ID_A, R_A)$,输出对 m 的有效伪签名 $\sigma^*=(h^*, s^*)$,Q 知道系统主密钥 u.若伪造签名成功,则 Q 输出 $r_A = (a - s^*(uh_1' + x_A + h^*))/s^*$ 作为解决 DL 困难问题的回答;否则,Q 没有解决 DL 困难问题.若 A_2 对 ID_A 进行过部分私钥或私钥查询,则 Q 失败,它不做这种查询的概率至少是 $1/q_1^2$;若 A_2 对 T'进行过 H_2 查询,则 Q 失败,它不做这种查询的概率大于 $1/q^2$.因此,Q 解决 DL 困难问题的优势 $Adv^{EUF\text{-}CMA}(A_2) \geqslant 1/q_1^2 q_2$. □

4.2 新方案安全性证明(参考了文献[12]中的证明方法)

现在将新方案中敌手发生的攻击方式划分为 9 种情况分别进行分析和证明.

在游戏开始前,挑战者 Q 试图猜想“测试会话”;游戏结束后,Q 随机选择两个指数 $I,J \in \{1,\ldots,n\}$,$I \neq J$ 表示对于 H_1 的第 I 次和第 J 次查询是随机可区分的查询.Q 正确选择 I,J 的概率是 $(1/n)\times(1/n-1) > 1/n^2$.$Q$ 选择 $t \in \{1,\ldots,m\}$,猜想测试预言 $\Pi_{I,J}^t$ 正确的概率至少是 $1/mn^2$;若 Q 没有正确猜想到测试会话,那么 Q 将终止游戏(令 n 是敌手 M 发生可区分 H_1 查询的最大次数,m 是任意一个用户与其他用户发生会话次数的最大值).

为了借助敌手 M 解决 CDH 困难问题,挑战者 Q 将猜想敌手不知道的相应的测试会话中的部分密钥.如果敌手查询的目标是下面禁止元素中的任意一个,那么 Q 将终止游戏;否则,游戏正常进行.为了简化证明,令 a,b 分别表示用户 I 和用户 J 的临时私钥,x_A, x_B 分别表示用户 I 和用户 J 的长期私钥,D_A, D_B 分别表示用户 I 和用户 J 的基于身份的部分私钥.我们将敌手 M 划分为 9 种情况来讨论:

(1) M 不知道 x_A, x_B;
(2) M 不知道 a, b;
(3) M 不知道 x_A, b;
(4) M 不知道 a, x_B;
(5) M 不知道 x_B(也不能替换其公钥 $x_B P$),也不知道 D_A;
(6) M 不知道 x_A(也不能替换其公钥 $x_A P$),也不知道 D_B;
(7) M 不知道 D_A, b;
(8) M 不知道 a, D_B;
(9) M 不知道 D_A, D_B.

在以上 9 种情况中,情况(1)~情况(4)和情况(9)这几种情况是很重要的.因为情况(1)提供了抗临时私钥泄露给 KGC 或临时私钥和基于身份的部分私钥全部泄露给敌手而产生的攻击,情况(2)提供了抗密钥泄露伪装攻击(KCI 攻击),情况(3)、情况(4)提供了抗临时私钥泄露给替换一个合法用户的公钥且腐化另一个合法用户基于身份的公钥的敌手而产生的攻击,情况(9)提供了抗临时私钥泄露给替换两个合法用户公钥的敌手而产生的攻击.现在详细分析情况(1)~情况(4)和情况(9)这几种情况的安全证据.

情况(1):挑战者 Q 想利用敌手 M 的帮助来解决 CDH 困难问题.Q 输入(uP,vP),它的目标是计算出 uvP.在游戏最后,Q 设用户 ID_I,ID_J 的无证书公钥分别为 uP,vP,Q 通过计算 $e(uP,vP)=e(uvP,P)$是否成立来判断敌手 M 对 H 随机预言查询是否有效.若该等式成立,则 Q 终止游戏,并返回 uvP 作为它解决 CDH 困难问题的答案.Q 成功解决 CDH 困难问题的概率是 $Adv_Q^{CDH}(k) \geqslant Adv_M(k)/9mn^2$. 为“$H$ 查询”所需的其他秘密值必须在 Q 的控制下,Q 才能计算所有的其他元素值(x_Ax_BP,K_1,K_2,K_3).若 M 是类型 2 敌手,则在游戏开始时,Q 将系统主密钥 x 发送给敌手,敌手就能为任何用户生成基于其身份的部分私钥.进行“测试查询”时,M 允许替换用户 ID_I,ID_J 的无证书公钥.如果 M 替换了其他用户的公钥且询问“显示查询”,那么 Q 首先利用对运算为 H 预言机做匹配查询检查,若没有找到匹配的查询,则 Q 从 H 的域内随机产生一个值 r,将 r 加到列表 L_2 中,并返回 r 给敌手 M;若 Q 后来询问“H 查询”包含正确的 x_Ax_BP 和无证书公钥 x_AP,x_BP,那么 Q 能够通过使用对操作完成列表 L_2 中表述的项目.

情况(2):挑战者 Q 想利用敌手 M 的帮助来解决 CDH 困难问题.Q 输入(uP,vP),它的目标是计算出 uvP.在游戏最后,Q 设用户 ID_I,ID_J“测试查询”中的临时公钥分别为 uP,vP,Q 通过计算 $e(uP,vP)=e(uvP,P)$是否成立来判断敌手 M 对 H 随机预言查询是否有效.若该等式成立,则 Q 终止游戏,并返回 uvP 作为它解决 CDH 困难问题的答案.Q 成功解决 CDH 困难问题的概率是 $Adv_Q^{CDH}(k) \geqslant Adv_M(k)/9mn^2$.由于 M 允许替换任何用户的无证书公钥,Q 使用情况(1)中陈述的方法来决定如何应答“显示查询”和“H 查询”.

情况(3)和情况(4):由于情况(3)和情况(4)是对称情形,所以 Q 成功解决 CDH 困难问题的概率相同.现在只分析情况(3),挑战者 Q 想利用敌手 M 的帮助来解决 CDH 困难问题.Q 输入(uP,vP),它的目标是计算出 uvP.在游戏最后,Q 设用户 ID_I 的无证书公钥为 $x_AP=uP$,用户 ID_J 在会话 $\Pi_{I,J}^t$ 中的临时公钥为 $bP=vP$,若 M 是类型二敌手,则 Q 在游戏开始时就将系统主密钥 x 发送给 M.与情况(1)、情况(2)类似,Q 通过计算 $e(P,bx_AP)=e(uP,vP)$是否成立来判断敌手 M 对 H 随机预言查询是否有效.若该等式成立,则 Q 终止游戏,并返回 uvP 作为它解决 CDH 困难问题的答案.Q 成功地解决 CDH 困难问题的概率是 $Adv_Q^{CDH}(k) \geqslant Adv_M(k)/9mn^2$. Q 使用情况(1)中陈述的方法来处理替换身份为 ID_I 以外的其他无证书密钥.

将情况(3)中的 b 换成 D_B 就变成了情况(6),将情况(4)中的 a 换成 D_A 就变成了情况(5),它们的处理方式与情况(3)类似,Q 成功解决 CDH 困难问题的概率也是 $Adv_Q^{CDH}(k) \geqslant Adv_M(k)/9mn^2$.

将情况(2)中的 b 换成 D_B 就变成了情况(8),将情况(2)中的 a 换成 D_A 就变成了情况(7),它们的处理方式与情况(2)类似,Q 成功解决 CDH 困难问题的概率也是 $Adv_Q^{CDH}(k) \geqslant Adv_M(k)/9mn^2$.

由于敌手不知道 D_A,D_B,它无法计算出 D_AD_BP,除非敌手能攻破基于底层的 CDH 困难问题.情况(9)的处理及分析类似于情况(7)、情况(8),Q 成功解决 CDH 困难问题的概率也是 $Adv_Q^{CDH}(k) \geqslant Adv_M(k)/9mn^2$.

5 协议总结

下面的所有协议,KGC 有主私钥 $s \in Z_q^*$,系统主公钥 $Pub=sP$,系统公共参数(e,q,P,Pub,G,G_2)和一些密钥获取函数:

$$H:\{0,1\}^* \to Z_q^*, H':G_2 \to Z_q^*, h:\{0,1\}^* \to G, h':\{0,1\}^* \times G \to G, h'':G_2 \times G \to \{0,1\}^k, kdf_{MT}:G_2 \times G \times G \to \{0,1\}^k,$$

$$kdf_{L_i}:G_2 \to \{0,1\}^k, kdf_{Shao}:G_2 \times \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^k, kdf_{Wang}:\{0,1\}^* \times \{0,1\}^* \times G_2 \times G \times G \to \{0,1\}^*.$$

P_i:表示用户 i 的公钥(如 P_A 表示用户 A 的公钥);Q_i:表示 i 的身份 ID_i 映射到群 G 上的元素.每个用户有临时私钥(用户 A、用户 B 的临时私钥分别用 $a,b \in Z_q^*$ 表示)和长期私钥 $x_i \in Z_q^*$ 以及由 KGC 生成的部分私钥 $S_i \in G$.用户 A 随机选择 $a \in Z_q^*$,并把 T_A 发给用户 B;用户 B 随机选择 $b \in Z_q^*$,并把 T_B 发给用户 A.表 1~表 3 分别列出了本文提到的无证书密钥协商方案的相关信息.X_i 表示用户 i 的全部私钥.

Table 1 Parameters for user i

表 1 用户 i 的有关参数

Scheme	P_i	Q_i	S_i	X_i
AP[2]	x_iP,x_iPub	$h(ID_i)$	sQ_i	x_iS_i
MT[4]	x_iP	$h(ID_i)$	sQ_i	$(s+x_i)Q_i$
WCW[6]	x_iP	$h(ID_i)$	sQ_i	(x_i,S_i)
Shao[7]	x_iP	$h'(ID_i,P_i)$	sQ_i	(x_i,S_i)
SL[5]	$E(P,x_iP)$	$H(ID_i)$	$(Q_i+s)^{-1}P$	x_iS_i

Table 2 Shared key computation

表 2 用户 A 与用户 B 共享的密钥计算

Scheme	T_i		Shared key K
AP[2]	T_A	aP	$e(X_B,T_A)e(X_A,T_B)$
	T_B	bP	$e(Q_B,x_BPub)^ae(X_A,T_B)$
MT[4]	T_A	aP	$e(Q_B,Pub+P_B)^ae(Q_A,Pub+P_A)^b$
	T_A	bP	$e(Q_B,Pub+P_B)^ae(X_A,T_B)$
WCW[6]	T_A	aP	$e(Q_A,Q_B)^s$
	T_B	bP	$e(S_A,Q_B)$
Shao[7]	T_A	aP_B	$H'(e(Q_A,Q_B)^s)abP$
	T_B	bP_A	$H'(e(S_A,Q_B))ax_A^{-1}(\mathrm{mod}\,q)T_B$
SL[5]	T_A	aQ_B	$P_A^bP_B^a$
	T_B	bQ_A	$e(T_B,X_A)P_B^a$

Table 3 Session key computation (K denotes the shared key from Table 2)

表 3 最终的会话密钥(K 表示表 2 中计算得到的共享密钥)

Scheme	Session key
AP[2]	$h''(K\|\|abP)$
MT[4]	$kdf(K\|\|abP\|\|x_Ax_BP)$
WCW[6]	$kdf(ID_A,ID_B,K,ax_BP,bx_AP)$
Shao[7]	$kdf(K\|\|ID_A\|\|ID_B)$
SL[5]	$kdf(K)$

各种无证书协议是否会产生攻击,主要看通信中的每方在只保留 1 个未泄露秘密的情况下,任何人是否能够顺利计算出最终的会话密钥.如果能,则表示该协议存在攻击;否则表明该协议在扩展 eCK 模型中是安全的.根据我们前面定义的 3 种安全类型来分析下面各种协议是不安全的:

Al-Riyami 和 Paterson(AP)协议产生的攻击.当 KGC 作为敌手知道临时私钥 a,b 时就会计算出 $K=e(Q_B,x_BPub)^a(S_A,x_AP)^b=e(S_B,x_BP)^ae(S_A,x_AP)^b$ 和 abP.因此,敌手在知道 S_A,S_B,a,b 的情况下就能计算出最终的会话密钥 $h''(K\|abP)$.因此,AP 协议不能抵抗临时私钥泄露产生的攻击.

MT 协议产生的攻击.当敌手知道临时私钥 a,b 时,它就能计算出 $K=e(Q_B,Pub+P_B)^ae(Q_A,Pub+P_A)^b$ 和 abP;如果再知道 x_A 或 x_B,它就能顺利求出最终的会话密钥 $kdf(K\|abP\|x_Ax_BP)$.因此,MT 协议不能抵抗临时私钥泄露产生的攻击和因某一方的长期私钥泄露产生的密钥泄露伪装(KCI)攻击.

WCW 协议产生的攻击.当 KGC 作为敌手知道临时私钥 a,b 时就会计算出 $K=e(Q_A,Q_B)^s,abP,ax_BP$ 和 bx_AP,它也就能顺利计算出最终的会话密钥 $kdf(ID_A,ID_B,K,ax_BP,bx_AP)$,产生攻击.因此,此协议具有密钥托管,且不具有 KGC 前向安全性,也不满足已知临时信息安全特性.另外,如果敌手知道 a,b,D_A,x_B 或 a,b,x_A,D_B,它就能计算出 $K=e(Q_A,Q_B)^s,bx_AP=x_AbP,ax_BP=x_BaP$,因此,它在知道两方临时私钥和另一方长期私钥的情况下就能计算出最终的会话密钥,产生 KCI 攻击和临时私钥泄露攻击.

Shao 协议产生的攻击.当敌手知道 S_A 或 S_B 以及临时私钥 a 或 b 时,就会计算出 $K=H'(e(Q_A,Q_B)^s)abP$.因此,只要敌手知道任何一方的部分私钥和任何一方的临时私钥都会计算出最终的会话密钥,产生因临时私钥泄露攻击和 KCI 攻击.

SL 协议产生的攻击.当敌手知道 a,b,x_A,x_B 时,它就能计算出 $K=e(bP,x_AP)e(aP,x_BP)=g^{ax_B+bx_A}$,也就能计算

出最终的会话密钥 $kdf(K)$,形成 KCI 攻击和中间人攻击.

Xia 协议产生的攻击.当敌手知道临时私钥 a,b 时,它就能计算出 $K=e(Q_B,Pub+P_B)^a e(Q_A,Pub+P_A)^b$ 和 abP.根本不需要知道 x_A 或 x_B,它就能顺利求出最终的会话密钥 $kdf(K||ax_BP||bx_AP||abP||A||B)$.因此,该方案会因临时私钥泄露产生中间人攻击.当敌手知道 b,x_B 时,可用 $P_E=x_EP-sP$ 来替换用户 B 的公钥 P_B,敌手在不知道 a 的情况下仍然能顺利计算出 $K=e(Q_B,x_BP)^a e(Q_A,Pub+P_A)^b=e(Q_B,aP)^{x_E} e(Q_A,Pub+P_A)^b$,敌手也能顺利计算出最终的会话密钥 $kdf(K||ax_BP||bx_AP||abP||A||B)$,因替换用户 B 的公钥而产生 KCI 攻击.

6 性能比较

新方案和文献[12]中的方案都只需 1 轮通信,传输带宽与文献[12]等同.新方案消除了双线性对操作,到目前为止,它是已知无证书安全认证协议中计算复杂度最低的.在安全方面,我们主要考虑方案是否满足:(1) 抗 KCI 攻击;(2) 前向安全;(3) KGC 前向安全性;(4) 已知会话临时信息安全.文献[1,3–6]中的方案都没有安全模型,而且都存在 KCI 攻击和 MA 攻击,尽管文献[12]和我们的方案一样不存在攻击,但它比我们方案多了 10 次双线性对运算.因此,新方案比本文提到的其他方案有明显优势(见表 4).

Table 4 Comparison of efficiency and security properties

表 4 效率及安全性比较

Protocol	Pairing	Exponentiation	Multiplication	KCI	FS	KGC-FS	MA
AP[2]	4	1	1	×	×	×	×
MT[4]	2	1	2	×	×	×	×
SL[5]	1	1	1	×	×	×	×
WCW[6]	1	0	3	×	×	×	×
Shao[7]	1	1	2	×	×	×	×
Georg[12]	10	5	5	√	√	√	√
New scheme	0	0	5	√	√	√	√

在表 4 中,KCI 表示“密钥泄露伪装攻击”,FS 表示“前向安全”,KGC-FS 表示“密钥生成中心前向安全”,MA 表示“因临时私钥泄露产生的攻击”.

7 结 论

我们演示了上述无证书密钥协商方案在 eCK 模型下存在的主要攻击问题,重新科学地定义了无证书密钥协商方案的 3 种安全类型,为以后设计安全的无证书密钥协商方案提供了简洁而有效的安全分析方法.新方案消除了对运算,它比同类其他无证书密钥协商方案具有更低的计算复杂度.只要 DL 和 CDH 假设成立,在每方只保留 1 个秘密值的情况下,新方案在文中定义的强安全模型中就是安全的.标准模型下无证书密钥协商方案将是一个开放性问题.

致谢 感谢评审专家的精心评审,感谢各位编辑的辛勤劳动.

References:

[1] Shamir A. Identity-Based cryptosystems and signature schemes. In: Proc. of the Crypto’84. LNCS 196, Berlin: Springer-Verlag, 1984. 47–53. [doi:10.1007/3-540-39568-7_5]

[2] Al-Riyami SS, Paterson K. Certificateless public key cryptography. In: Laih CS, ed. Advances in Cryptology——Asiacrypt 2003. LNCS 2894, Heidelberg: Springer-Verlag, 2003. 452–473. [doi: 10.1007/978-3-540-40061-5_29]

[3] Al-Riyami SS, Paterson KG. CBE from CL-PKE: A generic construction and efficient schemes. In: Vaudenay S, ed. Proc. of the PKC 2005. LNCS 3386, Berlin: Springer-Verlag, 2005. 398–415. [doi: 10.1007/978-3-540-30580-4_27]

[4] Mandt TK. Certificateless authenticated two-party key agreement protocols [MS. Thesis]. University of Gjovik, 2006.

[5] Wu CH, Chen ZX. A new efficient certificateless signcryption scheme. In: Proc. of the ISISE 2008. 2008. 661−664. [doi: 10.1109/ISISE.2008.206]

[6] Wang SB, Cao ZF, Wang LC. Efficient certificateless authenticated key agreement protocol form pairings. Wuhan University Journal of Natural Sciences, 2006,11(5):1278−1282. [doi: 10.1007/BF02829251]

[7] Shao ZH. Efficient authenticated key agreement protocol using self-certified public keys from pairings. Wuhan University Journal of Natural Sciences, 2005,10(1):267−270. [doi: 10.1007/BF02828666]

[8] Xia LQ, Wang SB, Shen JJ, Xu GM. Breaking and repairing the certificateless key agreement protocol from ASIAN 2006. Wuhan University Journal of Natural Sciences, 2008,13(5):562−566. [doi: 10.1007/s11859-008-0510-9]

[9] Swanson CM. Security in key agreement two-party certificateless schemes [MS. Thesis]. University of Waterloo, 2009.

[10] Swanson C, Jao D. A study of two-party certificateless authenticated key agreement protocols. In: Proc. of the INDOCRYPT 2009. LNCS 5922, Berlin, Heidelberg: Springer-Verlag, 2009. 57−71. [doi: 10.1007/978-3-642-10628-6_4]

[11] LaMacchia B, Lauter K, Mityagin A. Stronger security of authenticated key exchange. Technical Report, 2006/073, 2006.

[12] Lippold G, Boyd C, Nieto JG. Strongly secure certificateless key agreement. In: Proc. of the Pairing 2009. LNCS 5671, Berlin, Heidelberg: Springer-Verlag, 2009. 206−230. [doi: 10.1007/978-3-642-03298-1_14]

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

[14] Chen L, Cheng Z, Smart NP. Identity-Based key agreement protocols from pairings. Int'l Journal of Information Secure, 2007,6(4):213−241. [doi: 10.1007/s10207-006-0011-9]

[15] Zhang L, Zhang FT. A method to construct a class of certificateless signature schemes. Chinese Journal of Computers, 2009,32(5):940−945 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2009.00940]

附中文参考文献:

[15] 张磊,张福泰.一类无证书签名方案的构造方法.计算机学报,2009,32(5):940−945. [doi: 10.3724/SP.J.1016.2009.00940]

刘文浩(1974－),男,湖北孝感人,博士,主要研究领域为信息安全,密码学.

许春香(1965－),女,博士,教授,博士生导师,主要研究领域为信息安全,密码学.