软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(5):1031−1040 [doi: 10.3724/SP.J.1001.2011.03828]

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

高效的标准模型下基于身份认证密钥协商协议*

高志刚+, 冯登国

(中国科学院 软件研究所 信息安全国家重点实验室,北京 100190)

Efficient Identity-Based Authenticated Key Agreement Protocol in the Standard Model

GAO Zhi-Gang+, FENG Deng-Guo

(State Key Laboratory of Information Security, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

+ Corresponding author: E-mail: zhigang2005@is.iscas.ac.cn

Gao ZG NN, Feng DG. Efficient identity-based authenticated key agreement protocol in the standard model. *Journal of Software*, 2011,22(5):1031−1040. http://www.jos.org.cn/1000-9825/3828.htm

Abstract: This paper proposes an efficient Identity-Based authenticated key agreement protocol based on Waters' Identity-Based Encryption scheme and gives a detail security analysis with provable security techniques in the standard model. It is more efficient than other similar protocols, and provides known-key security and forward secrecy. And it also resists key-compromise impersonation and unknown key share attacks. Moreover, this protocol is extended to satisfy the requirement that the session key should be escrowed by the Private Key Generation (PKG) center, and is given a key confirmation property with a secure message authentication code algorithm.

Key words: authentication; key agreement; identity-based; provable security; standard model

摘 要: 在 Waters 的基于身份加密方案的基础上提出了一种高效的基于身份认证密钥协商协议,并在标准模型下证明了该协议的安全性.与目前已有的同类协议相比,该协议具有更高的效率和更弱的安全假设,并具有已知密钥安全和前向安全性等安全性质,同时能够抵抗未知密钥共享和密钥泄露伪装攻击.在该协议基础上,构造了防止用户密钥生成中心获取会话密钥的协议,以满足需要防止密钥托管的应用需求,并采用安全的消息认证码算法为该协议增加了密钥确认过程.

关键词: 认证;密钥协商;基于身份;可证明安全;标准模型

中图法分类号: TP309 **文献标识码**: A

当两个处于开放网络中的实体需要通信时,需要采用对通信信道进行加密的方法建立安全信道以保证会话的安全性.早期一般采用预共享密钥的方式,通过对称加密技术建立安全信道,然而这种方式容易受到重放攻击的威胁,如果共享密钥是简单的口令,则还容易受到猜测攻击的影响.相对于早期的共享会话密钥协议,会话密钥协商协议具有更高的安全性,并能抵抗重放攻击和猜测攻击.最早也最为著名的现代密钥协商协议是 Diffie 和 Hellman 在文献[1]中提出的 Diffie-Hellman 密钥交换协议,然而该协议由于没有对通信双方进行认证,因此存在中间人攻击.该问题的基本解决办法是为密钥协商协议增加对通信双方的相互认证.我们称增加了认

* 基金项目: 国家自然科学基金(60673083, 60803129); 江苏省网络与信息安全重点实验室资助项目(BM2003201); 国家发改委 2008 年下一代互联网业务试商用及设备产业化专项(CNGI-09-03-03)

收稿时间: 2009-06-18; 修改时间: 2009-10-20; 定稿时间: 2010-01-21

证功能的密钥协商协议为认证密钥协商协议.这类协议可以很好地解决在通信双方之间建立安全会话的需求.

认证密钥协商可以通过多种技术来实现.在本文中,我们集中关注于采用基于身份公钥密码体制和双线性映射的认证密钥协商协议.目前存在的这类认证密钥协商协议需要的交互轮数和信息量较小,具有较高的效率和很好的安全性,并且不需要建立和维护代价高昂的公钥基础设施(public key infrastructure,简称 PKI),易于实现和应用.自从 Shamir 在文献[2]中提出基于身份密码学的概念并构造了第一个基于身份签名方案,基于身份的加密、签名和密钥协商协议研究得到了迅速的发展.在基于身份认证密钥协商研究方面,国内外学者进行了深入的研究并提出了许多协议.由于效率较低,初期提出的采用双线性映射的基于身份的密钥建立协议不适合在实际应用系统中应用.实际上,有效的基于身份认证密钥协商协议直到 Boneh 和 Franklin[3]提出第一个有效的采用双线性映射的基于身份加密方案之后,才不断涌现,例如文献[4–8].尽管这类协议的效率问题得到解决,由于这类协议的安全性在较长一段时间并没有有效的方法进行安全证明,这也限制了这类协议在实际应用中的发展.Chen 和 Kudla(以下简称 CK)在文献[5]中提出第一个在随机预言机模型下的形式化证明方法.在文献[5]中,他们基于文献[6]构造了一个更有效的密钥协商协议,并采用他们提出的新方法进行了安全性证明.然而该证明方法存在一个缺陷,即不能响应 Reveal(即敌手通过该请求获取会话双方建立的会话密钥)请求,随后 CK 对他们的证明进行了更正,通过在一个弱化的 Bellare-Rogaway 模型中为协议增加一个内置的判定性函数,从而迫使攻击者泄露会话密钥的相关信息来达到可以响应 Reveal 请求的目标,并应用该方法重新对他们的协议进行了安全证明.Chen 在文献[9]中对这类协议进行了分析和示例证明.在国内的研究中,彭华熹在文献[10]中基于 CK[5]协议构造了在跨域环境中的三方认证密钥协商协议,并进行了安全性证明.

上述协议都是基于随机预言机模型的协议.由于构造安全随机函数比较困难,导致这类协议在实际的应用中的安全性得不到很好的保证,只能依赖于具体实现.近年来,在标准模型下可证明安全的基于身份加密方案研究取得了很大的发展,国内外学者提出了多种标准模型下有效的基于身份的加密方案,如文献[11–13].与此同时,标准模型下会话密钥协商协议也在不断发展.Wang 等人在文献[14]最先提出了一种标准模型下的基于身份的密钥协商协议,该协议基于 Gentry[13].然而,Liu 等人在文献[15]中提出了对 Wang 的非密钥托管协议中存在的恶意 PKG(private key generator)的攻击,同时 Wang 的协议基于一个非常强的困难假设 Augmented Bilinear Diffie-Hellman exponent assumption(q-ABDHE).Liu[15]同时提出了一个基于 Waters[9]的认证密钥协商协议,并采用类似于 Wang[14]中的方法提供了防止密钥托管的安全性质.然而该协议的效率较低,并且在证明过程中,Liu 等人并未考虑在攻击者的第 2 阶段攻击过程中,攻击者对他要挑战的 Oracle(随机预言机,代表参与协议运行的某个实体.由于在安全模型中实体需要对攻击者的各种请求做出合适的应答,因此该实体可以被看作一个预言机)参与的其他会话进行 Reveal 询问的情况.从直观上理解,当攻击者选定挑战会话之后,在自适应阶段为了获取更多与被挑战参与方相关的信息,必然会对挑战会话的参与方进行更多的询问,对于这类询问的处理可能导致攻击者发现模拟世界和现实世界的不同,因此在证明过程中必须对这类情况进行考虑.

在本文中,我们提出了一种基于身份的认证密钥协商协议.该协议与 Liu[15]的协议相比具有更高的效率,更易于在实际系统中应用.该协议的安全性基于判定性双线性 Diffie-Hellman 问题的困难性,并在标准模型下是可证明安全的.同时,为了满足一些应用环境中需要防止密钥托管的安全需求,我们基于基本协议构造了可以防止会话密钥在密钥生成中心(PKG)托管的协议.最后,我们采用一个安全的消息认证码算法为该协议增加了密钥确认过程.

本文首先简要介绍认证密钥协商协议相关工作及我们的文章的动机和创新点.第 1 节介绍相关的概念和定义.第 2 节描述我们的协议采用的认证密钥协商安全模型.第 3 节给出协议的具体构造.第 4 节对我们协议的安全性进行证明.第 5 节讨论协议的安全性和相关性质,并提出具有防止密钥托管性质的协议.第 6 节对我们的工作进行总结.

1 预备知识

首先,我们简要描述我们所需要使用到的双线性映射,更详细的信息参见文献[9].

定义 1(双线性映射). 选择群$\mathbb{G},\mathbb{G}_T$,其中$\mathbb{G}$的阶为 p,p 是一个大素数.g 是群$\mathbb{G}$的一个生成元,$e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$是从$\mathbb{G}$到$\mathbb{G}_T$上的一个映射,如果映射 e 满足以下 3 个条件,则称映射 e 是一个有效的从$\mathbb{G}$到$\mathbb{G}_T$上的双性映射:

1. 双线性:任意的 $a,b\in\mathbb{Z}_p$,满足 $e(g^a,g^b)=e(g,g)^{ab}$.
2. 非退化性:$(g,g)\neq 1$.
3. 可计算性:任意的 $u,v\in\mathbb{G}$,$e(u,v)$都是可以有效计算的.

我们的协议的安全性基于判定性双线性 Diffie-Hellman 假设(简称 DBDH).该假设的定义如下:

假设 1(判定性双线性 Diffie-Hellman 假设). 给定$(\mathbb{G},\mathbb{G}_T,g,g^a,g^b,g^c,Z)$,其中 $a,b,c\in\mathbb{Z}_p$,$Z\in\mathbb{G}_T$,判断等式 $Z=e(g,g)^{abc}$ 是否成立是困难的.

为了对协议的安全性进行分析,这里简要列举认证密钥协商协议所需要满足的一些性质,这些性质将会在之后的协议分析阶段使用到.

- 已知会话密钥安全性(known session key security,简称 KSK):一个会话密钥的泄露不能导致其他会话密钥的泄露.
- 前向安全性(forward secrecy,简称 FS):如果通信参与方中的一方或者多方的长期私钥的泄露不会导致他们之前已经建立的会话密钥的泄露,则称该协议具有前向安全性.基本的前向安全性仅能保证在所有参与方中一个参与方的长期密钥丢失并不影响之前的会话密钥安全性;如果通信双方的长期密钥都丢失却仍然保持该性质,则称协议达到了完全的前向安全性;如果在系统的主私钥丢失情况下仍保持该性质,则称协议达到了主密钥前向安全性.在下文我们使用 fs-s 标识基本的前向安全性,使用 fs-d 表示完全的前向安全性,使用 fs-m 表示主密钥前向安全性.
- 抵抗密钥泄露伪装攻击(key compromise impersonation resilience,简称 KCI):如果攻击者得到了一个实体 A 的私钥,则毫无疑问攻击者可以伪装成 A 与其他用户运行协议,但是不能使攻击者伪装成其他用户与 A 成功完成协议.
- 未知密钥共享安全性(unknown key share,简称 UKS):协议不能允许以下这种情况:用户 A 认为他与用户 B 建立了会话密钥 K,而实际上用户 A 与其他用户 C 建立了会话密钥 K.
- 会话密钥托管(session key escrow,简称 SKE):可信第三方可以通过监听协议双方在协议运行过程中的通信过程,并根据获取的消息恢复出该次协议运行产生的会话密钥.在某些安全要求很高的应用环境中,需要有可信第三方对于所有的回话过程进行监控.在这种情况下,协议应该具有会话密钥托管的性质,以保证可信第三方对通信的管理.然而在注重保护用户隐私的环境中,则需要防止会话密钥被第三方恢复,即需要防止会话密钥托管.

2 安全模型

在本文中,我们采用文献[9]中定义的安全模型来证明我们协议的安全性,在该模型中,会话的参与方被形式化为一个 Oracle,攻击者具有执行 Send,Reveal 和 Corrupt 请求的能力(具体定义在下面给出),在攻击游戏完成后,攻击者必须输出一个对会话密钥的猜测.在该模型中,我们定义 $\Pi_{i,j}^s$ 和 $\Pi_{j,i}^s$ 为第 s 次协议运行中的两个参与方,其中,i,j 表示系统中的第 i 和第 j 个用户.该安全模型描述如下:

在第 1 阶段中,攻击者可以任何次序执行以下询问:

Send$(\Pi_{i,j}^s,x)$. 敌手通过该条请求初始化一个会话或者向会话的参与方发送消息.$\Pi_{i,j}^s$ 收到消息 x 后执行该协议并输出一个消息 m,或者输出一个符号标识接受或者是拒绝该会话.如果 $\Pi_{i,j}^s$ 不存在,则根据输入消息 x 建立该参与方,如果 $x=\lambda$(λ是协议的安全参数),则该参与方为该会话的发起者;否则,该参与方为会话的响应者,并且消息 x 作为该参与方的输入.在这条消息中,要求 $i\neq j$,因为参与方不会与自己发起一次会话请求,这是符合实际情况的.

Reveal$(\Pi_{i,j}^s)$. 攻击者通过该请求获取会话密钥.如果 $\Pi_{i,j}^s$ 接受会话,则输出该参与方的会话密钥;否则,输出

终止符号⊥.

Corrupt(*i*). 攻击者通过该请求获取系统中第 *i* 个用户的私钥.

一旦攻击者决定第 1 阶段完成,则开始第 2 阶段.首先,攻击者选取一个新鲜的参与方$\Pi_{i,j}^{s}$,并执行一次*Test*($\Pi_{i,j}^{s}$)请求,获得该请求的输出消息.其中,新鲜性和*Test*($\Pi_{i,j}^{s}$)定义如下:

定义 2(新鲜参与方). 如果一个参与方$\Pi_{i,j}^{s}$满足以下条件,则称该参与方是新鲜的:(1) $\Pi_{i,j}^{s}$接受了会话;(2) $\Pi_{i,j}^{s}$未被打开,即没有接受 Reveal 询问;(3) $j\neq i$,并且 *j* 未接受 Corrupt 询问;(4) 如果存在与该会话匹配的对应参与方$\Pi_{i,j}^{s}$,则该参与方不能是被打开的,即没有接受 Reveal 询问.

Test($\Pi_{i,j}^{s}$). 如果$\Pi_{i,j}^{t}$是新鲜的,则挑战者通过公平的掷币协议选择 $b\in\{0,1\}$,如果 b=0,则输出会话密钥;否则,输出一个在密钥空间里随机选择的串.

攻击者接收到 *Test*($\Pi_{i,j}^{s}$)的输出之后,可以继续以任何次序请求第 1 阶段中的 3 种询问,但不能 Reveal 参与方$\Pi_{i,j}^{s}$或者与之相匹配的参与方$\Pi_{i,j}^{t}$(如果该参与方存在),并且不能 Corrupt 参与方 *j*(该限制是十分合理的,因为如果攻击者能够执行上述询问,那么敌手将能直接获得会话密钥).最终,攻击者必须输出对 *b* 的猜测 *b*′,如果 $b=b'$,则称攻击者赢得了该攻击游戏.攻击者的猜测优势定义为$Adv^{E}(k)=\left|2\Pr[b=b']-1\right|$(其中,*k* 是密钥空间参数,*E* 示攻击者).

在该攻击实验中,我们采用会话 ID 标识一次会话,会话 ID 的选取方式根据协议的不同而有相应的改变,但应能唯一标识一次协议执行.两个参与方$\Pi_{i,j}^{s}$和$\Pi_{i,j}^{t}$的会话相匹配,当且仅当他们的会话标识相同.

定义 3. 一个协议是安全的认证密钥协商协议,如果该协议满足以下条件:

(1) 在善意(在这里,我们所谓的善意是指攻击者忠实地传送消息,不修改协议传送的消息)的攻击者参与的会话过程中,参与方如果接受会话,则他们总是共享相同的会话密钥,并且该会话密钥在$\{0,1\}^{k}$上服从均匀分布;

(2) 对任意的多项式时间攻击者,他的猜测优势 $Adv^{E}(k)$都是可忽略的.

3 协议构造

我们的协议基于 Waters[11]的基于身份加密方案.我们提出的第 1 个协议(简称为协议 1,下同)包括系统建立、用户私钥抽取和密钥协商 3 个过程,其中,系统建立和用户私钥抽取过程与 Waters[11]类似.协议 1 的具体构造描述如下:

系统建立.选择阶为大素数 *p*(*p* 的长度由安全参数λ确定)的群和一个有效的从群$\mathbb{G}$映射到群$\mathbb{G}_1$的双线性映射 $e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_1$.随机选择 $\alpha\in\mathbb{Z}_p, g, g^2\in\mathbb{G}$,其中 *g* 是$\mathbb{G}$的一个生成元,设定 $g_1=g^{\alpha}$.系统随机选择 $u'\in\mathbb{G}$和一个 *n* 维向量 $U=(u_i)$其中 u_i是$\mathbb{G}$中随机选取的元素.同时,系统选择一个碰撞自由哈希函数 $H:\{0,1\}^{*}\to\{0,1\}^{k}$作为会话密钥生成函数,其中 *k* 是相应的对称加密算法需要的会话密钥的长度.系统的公开参数是$(g,g_1,e,u',U,H,\mathbb{G})$,系统的主密钥是 g_2^{α}.

用户私钥抽取.该过程为用户产生私钥.在该系统中用户的身份标识被表示为 *n* 位的字符串.对于标识为 *v* 的用户,设 v_k表示 *v* 中的第 *k* 位,设集合 $V\subseteq\{1,\ldots,n\}$是所有 v_k=1 的所有 *k* 的集合.用户 *v* 的私钥构造如下:

$$d_v=\left(g_2^{\alpha}\left(u'\prod_{k\in V}u_k\right)^{r},g^{r}\right),$$

其中,$r\in\mathbb{Z}_p$是密钥生成函数随机选择的整数.为了便于书写并不失一般性,我们设 $Q_v=u'\prod_{k\in V}u_k$ 表示用户身份 *v* 到群$\mathbb{G}$上的映射.

密钥交换.假设协议的参与方为 Alice(简称为 A)和 Bob(简称为 B),他们的身份(即公钥)为 Alice 和 Bob.他

们分别拥有对应的私钥 $d_A=(d_{A_1},d_{A_2})=\left(g_2^{\alpha}Q_A^{r_A},g^{r_A}\right),d_B=(d_{B_1},d_{B_2})=\left(g_2^{\alpha}Q_B^{r_B},g^{r_B}\right)$(其中,$r_A,r_B\in\mathbb{Z}_p$ 为密钥产生中心随机选取的整数).协议 1 的消息交互过程如图 1 所示,并详细描述如下:

1. Alice 随机选择 $x\in\mathbb{Z}_p$,计算 $T_A=\left(T_{A_1},T_{A_2}\right)=\left(Q_B^x,g^x\right)$ 并发送给 Bob.
2. Bob 收到 T_A 后,随机选择 $y\in\mathbb{Z}_p$,计算 $T_B=\left(T_{B_1},T_{B_2}\right)=\left(Q_A^y,g^y\right)$ 并发送给 Alice.
3. Alice 计算 $K_{AB}=e\left(d_{A_1},T_{B_2}g^x\right)e\left(d_{A_2}^{-1},T_{B_1}Q_A^x\right)=e\left(g_1,g_2\right)^{x+y},sk_A=H\left(A,B,T_A,T_B,K_{AB}\right)$;Bob 计算 $K_{BA}=e\left(d_{B_1},T_{A_2}g^y\right)e\left(d_{B_1},T_{A_2}g^y\right)e\left(d_{B_2}^{-1},T_{A_1}Q_B^y\right)=e\left(g_1,g_2\right)^{x+y},sk_B=H\left(A,B,T_A,T_B,K_{BA}\right)$.$sk_A$ 和 sk_B 是协商的会话密钥.

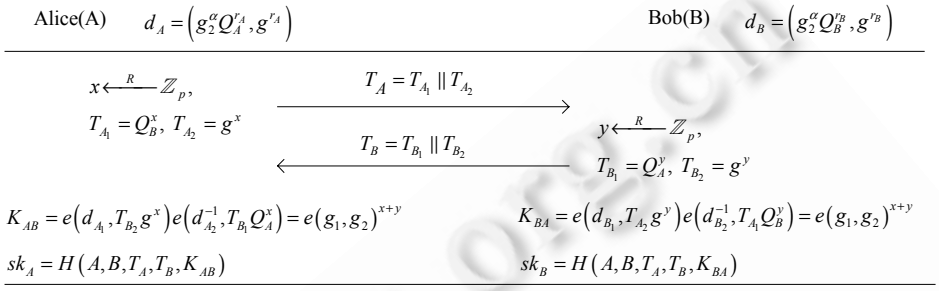

Fig.1 Identity-Based authenticated key agreement protocol

图 1 基于身份认证密钥协商协议

4 安全性

本节在第 2 节描述的安全模型中证明我们的协议的安全性.

定理 1. 如果 DBDH 困难假设成立,则协议 1 是安全的认证密钥协商协议(安全定义见定义 3).

证明:我们采用把攻击者对协议 1 的攻击能力规约到解决 DBDH 问题的方法来证明协议 1 的安全性.为使证明简便,我们定义会话的标识为 $T_A\|T_B$,两个会话相同当且仅当会话标识相同.

首先,我们证明协议 1 满足定义 3 中的第 1 个条件.由 K_{AB} 和 K_{BA} 的计算方法可知:

$$\begin{aligned}K_{AB}&=e\left(d_{A_1},T_{B_2}g^x\right)e\left(d_{A_2}^{-1},T_{B_1}Q_A^x\right)=e\left(g_2^{\alpha}Q_A^{r_A},g^yg^x\right)e\left(g^{-r_A},Q_A^yQ_A^x\right)\\&=\left(e\left(g_2^{\alpha}Q_A^{r_A},g\right)e\left(g^{-r_A},Q_A\right)\right)^{x+y}=\left(e\left(g_2^{\alpha},g\right)e\left(Q_A^{r_A},g\right)e\left(g,Q_A^{r_A}\right)^{-1}\right)^{x+y}=e\left(g_1,g_2\right)^{x+y},\\K_{BA}&=e\left(d_{B_1},T_{A_2}g^y\right)e\left(d_{B_2}^{-1},T_{A_1}Q_B^y\right)=e\left(g_2^{\alpha}Q_B^{r_B},g^xg^y\right)e\left(g^{-r_B},Q_B^xQ_B^y\right)\\&=\left(e\left(g_2^{\alpha}Q_B^{r_B},g\right)e\left(g^{-r_B},Q_B\right)\right)^{x+y}=\left(e\left(g_2^{\alpha},g\right)e\left(Q_B^{r_B},g\right)e\left(g,Q_B^{r_B}\right)^{-1}\right)^{x+y}=e\left(g_1,g_2\right)^{x+y}.\end{aligned}$$

由于 $K_{AB}=K_{BA}$,因此 Alice 和 Bob 协商的会话密钥 $sk_A=sk_B$.

其次,我们证明协议 1 满足定义 3 中的第 2 个条件.对于一个 DBDH 问题实例($\mathbb{G},\mathbb{G}_T,p,g,g^a,g^b,g^c,Z$),我们构造一个多项式时间模拟器 S(在本节中使用 S 代表模拟器),利用对协议 1 的攻击者 E(在本节中使用符号 E 代表攻击者)来解决该 DBDH 问题.假如存在能够成功攻击协议 1 的攻击者,我们可以证明 S 可以不可忽略的优势解决 DBDH 问题.首先,我们假设:(1) E 在该攻击实验中请求为 q_0 个用户产生私钥;(2) E 最多建立 q_1 次协议运行;(3) E 在第 1 阶段最多对 q_2 个用户执行 Corrupt 询问.S 选取 $J\in(0,q_1)$并保存在系统内部,则我们猜测 $\Pi_{i,j}^J$ 将会是 E 在 Test 询问中要挑战的会话.我们定义 $\Pi_{i,j}^s$ 和 $\Pi_{j,i}^s$ 为第 s 次协议运行中的两个参与方.其中,i 和 j 表示系统中的第 i 和第 j 个用户,他们的身份分别为 v_i 和 v_j.在下文中不引起混淆的情况下,我们把具有身份 v_i 和 v_j 的用户简写为 i 和 j.在上述假设的基础上,模拟器 S 的构造如下:

Setup(λ,n). 该步骤与文献[9]中的系统建立过程是相似的.在该系统中,用户的身份表示为 n 位的字符串.S

设置整数 $m=4(q_0-1)$,并随机选择 $h\in(0,n)$.S 选择 $x',y'\in(0,m)$和 n 维向量 $\vec{x}=(x_i)$, $\vec{y}=(y_i)$,其中,$x_i\in(0,m)$,$y_i\in\mathbb{Z}_p$.对于身份为 v 的用户,设$V\subseteq\{1,...,n\}$是所有满足 $v_k=1$ 的 k 的集合,S 定义函数$F(v)=\left((p-mh)+x'+\sum_{k\in V}x_k\right) \bmod p$, $J(v)=\left(y'+\sum_{k\in V}y_k\right) \bmod p$.$S$ 设置 $g_1=g^a$,$g_2=g^b$,$u'=g_2^{p-hm+x'}g^{y'}$,$U=(u_k)$,其中,$u_k=g_2^{x_k}g^{y_k}$,$k\in[1,n]$,并发送(g,g_1,g_2,e,p,u',U)给 E.

KG(v). KG(key generation)模拟用户私钥抽取过程.S 维护一个列表 $L_{KG}=(v,d_v,r,type)$,$r\in\mathbb{Z}_p$,其中,v 是用户标识,d_v 为对应的私钥,r 是 S 为用户 v 选择的随机数,$type\in\{0,1\}$为用户类型标识(其中,$type=1$ 表示 $F(v)=0 \bmod p$,即 S 不能计算该用户的私钥;$type=0$ 表示 $F(v)\neq 0 \bmod p$,S 能计算用户的私钥).对于用户 v 的私钥请求,S 查找列表,如果存在匹配的列表项,则返回对应的 d_v;否则,作如下处理:

- 如果 $F(v)=0 \bmod p$,则 S 无法为该用户产生私钥.在这种情况下,S 设置用户的私钥列表项为$(v,\perp,\perp,1)$.S 检查用户列表 L_{KG},如果列表中存在多个 $type=1$ 的列表项,或者列表长度等于 q_0 但不存在 $type=1$ 的列表项,则 S 终止模拟(Event 1).
- 如果 $F(v)\neq 0 \bmod p$,则随机选择 $r\in\mathbb{Z}_p$,计算 $d_v=\left(g_1^{\frac{-J(v)}{F(v)}}\left(u'\prod_{i\in V}u_i\right)^r, g_1^{\frac{-1}{F(v)}}g^r\right)$,并把$(v,d_v,r,0)$插入到列表中.

  注意,这里的私钥是一个合法的用户私钥,因为设 $r'=r-\frac{a}{F(v)}$,则有:

$$d_{v_1}=g_1^{\frac{-J(v)}{F(v)}}\left(u'\prod_{i\in V}u_i\right)^r=g_1^{\frac{-J(v)}{F(v)}}\left(g_2^{F(v)}g^{J(v)}\right)^r=g_2^a\left(g_2^{F(v)}g^{J(v)}\right)^{-\frac{a}{F(v)}}\left(g_2^{F(v)}g^{J(v)}\right)^r$$

$$=g_2^a\left(u'\prod_{i\in V}u_i\right)^{r-\frac{a}{F(v)}}=g_2^a\left(u'\prod_{i\in V}u_i\right)^{r'},$$

$$d_{v_2}=g_1^{-\frac{1}{F(v)}}g^r=g^{r-\frac{a}{F(v)}}=g^{r'}.$$

Send($\Pi_{i,j}^s$,M). S 维护一个列表 $L_2=(\Pi_{i,j}^s,r_i,M,M',K,sk)$其中,$M$ 是参与在会话过程中收到的消息,$r_i\in\mathbb{Z}_p$ 是模拟器为 $\Pi_{i,j}^s$ 选择的随机数,M'是 $\Pi_{i,j}^s$ 产生的消息,K 是计算的共享秘密,sk 是最后的会话密钥.K 和 sk 初始时设置为 $\perp$ 表示该值为空,同时,该列表可能会在 Reveal 询问中被更新.当 S 收到消息 M 时,作如下处理:

- 如果 $\Pi_{i,j}^s$ 已经存在,且为会话的发起者,则设置 M 为 $\Pi_{i,j}^s$ 接收到的消息并接受会话.
- 如果 $\Pi_{i,j}^s$ 不存在,则调用 *KG* 函数为参与方 i 生成对应的私钥.
- 如果 $M=\lambda$,则设置 i 为会话发起者;否则,设置 i 为会话的响应者,并且将 M 作为它的输入.
- 如果 $s\neq J$,S 随机选择 $r\in\mathbb{Z}_p$ 作为参与方 i 的随机数并计算$M=\left(\left(u'\prod_{k\in V_j}u_k\right)^r, g^r\right)$,更新 L_2 并返回 M.
- 如果 $s=J$,则 S 在列表 L_{KG} 中查找 v_j 对应的表项,如果 $type=0$,则终止模拟器(Event 2);否则,设置 $r=\perp$,计算 $M=\left(g^{c\cdot J(v_j)}, g^c\right)$,更新列表 L_2 并返回 M.
- 如果 i 为会话的响应者,则设置 $\prod_{i,j}^s$ 接受会话.

Corrupt(i). S 首先根据身份 v_i 查找列表 L_{KG},如果不存在相应的表项,则调用 *KG* 函数为它生成私钥.S 查找到相应的表项后,如果 $type=1$,则终止模拟器(Event 3);否则,返回对应的 d_{v_i}.

Reveal($\Pi_{i,j}^s$). S 从列表 L_2 中查找 $\prod_{i,j}^s$,如果未找到符合的表项,或者 $\Pi_{i,j}^s$ 未接受会话,则返回 $\perp$(同时,根据假设攻击者正确遵守了第 2 节的安全模型,即攻击者不 Reveal 它要挑战的会话);否则,作如下处理:

- 如果 $K\neq\perp$,则返回对应的 sk.
- S 在列表 L_{KG} 中查找 v_i 对应的表项,如果未找到,则返回 $\perp$.如果 v_i 对应的 $type=0$,则参与方 i 拥有合法的

用户私钥 (d_{v_1},d_{v_2}), S 根据输入消息 M 和它的随机数 $r_i\in\mathbb{Z}_p$ 计算 $K=e\left(d_{v_1},M_2g^x\right)e\left(d_{v_2}^{-1},M_1Q_v^x\right)$, 计算 $sk=H\left(v_i,v_j,\left(u'\prod_{j\in V_i}u_j\right)^{r_i}\middle\|g^{r_i},M,K\right)$ (如果 i 是会话发起者);否则,计算 $sk=H\left(v_j,v_i,M,\left(u'\prod_{j\in V_i}u_j\right)^{r_i}\middle\|g^{r_i},K\right)$, 更新列表并返回 sk.

- 如果 v_i 对应的 $type$=1,则由于模拟器不能计算参与方 i 的私钥,无法直接计算对应的会话密钥.S 首先在列表 L_2 中查找与该会话的会话 ID 相同的条目,如果找到匹配的项 $\left(\Pi_{m,n}^t,r_m,M,M',K,sk\right)$, 则计算 $K=e\left(d_{v_1},M_2g^x\right)e\left(d_{v_2}^{-1},M_1Q_v^x\right)$ 和 sk,更新列表并返回 sk;否则,随机选取 $K\in\mathbb{G}_1$ 并计算 sk,更新列表 L_2 并返回 sk.

Test($\Pi_{i,j}^s$). 当 E 决定结束第 1 阶段时,假设攻击者完全遵守第 2 节定义的安全模型,则攻击者选择一个新鲜的参与方 $\Pi_{i,j}^t$ 发起 Test 询问.S 收到询问请求后,作如下处理:

- 如果 $t\neq J$,或者 $t=J$ 但存在会话标识与 $\Pi_{i,j}^t$ 相同的会话,并且该会话已经被打开,则终止模拟器(Event 4);
- 否则,S 查找列表 L_2 获取 $\Pi_{i,j}^t$ 对应的会话随机数 r(由 Send 操作模拟过程可知, $\Pi_{i,j}^t$ 对应的类型 $type$=1), 计算 $Z\times e(g_2,g_1)^r$ 并返回给 E.

Guess. 一旦 E 决定完成询问,则输出它的猜测 μ.当 S 接收到 E 的猜测 μ 时,直接把 μ 作为 S 对 Z 的猜测.

下面,我们来分析在 E 成功的情况下 S 成功的概率.

引理 1. 如果 S 没有终止上述模拟游戏,则 E 无法区分模拟世界和真实世界.

证明:在上述的模拟游戏中的所有实体的输出都符合协议 1 的要求,同时实体的输出消息符合消息空间上的均匀分布.因此 E 无法觉察模拟世界和真实世界的不一致性. □

引理 2. 在 E 无法区分模拟世界和真实世界的情况下,Event 1 不发生的概率 $\Pr\left[\overline{\text{Event 1}}\right]\geqslant\frac{1}{8(n-1)(q_0-1)q_0q_1}$.

证明:Event 1 不发生,即 q_0 次密钥请求中有且仅有 1 次询问使得 $F(v)=0 \bmod p$.我们计算该事件发生概率的一个下限.对于任意顺序的 q_0 次密钥请求 $v_1,v_2,...,v_{q_0}$,

$$\begin{aligned}
\Pr\left[\overline{\text{Event 1}}\right]&=\Pr\left[\bigwedge_{i=1}^{q_0-1}F(v_i)\neq 0\wedge F\left(v_{q_0}\right)=0\right]\\
&=\left(1-\Pr\left[\bigwedge_{i=1}^{q_0-1}F(v_i)=0\right]\right)\Pr\left[F\left(v_{q_0}\right)=0\middle|\bigwedge_{i=1}^{q_0-1}F(v_i)\neq 0\right]\\
&\geqslant\left(1-\frac{q_0-1}{m(n-1)}\right)\Pr\left[F\left(v_{q_0}\right)=0\middle|\bigwedge_{i=1}^{q_0-1}F(v_i)\neq 0\right]\\
&=\left(1-\frac{q_0-1}{m(n-1)}\right)\frac{\Pr\left[F\left(v_{q_0}\right)=0\right]}{\Pr\left[\bigwedge_{i=1}^{q_0-1}F(v_i)\neq 0\right]}\Pr\left[\bigwedge_{i=1}^{q_0-1}F(v_i)\neq 0\middle|F\left(v_{q_0}\right)=0\right]\\
&\geqslant\frac{1}{m(n-1)}\left(1-\frac{q_0-1}{m(n-1)}\right)\left(1-\Pr\left[\bigwedge_{i=1}^{q_0-1}F(v_i)=0\middle|F\left(v_{q_0}\right)=0\right]\right)\\
&\geqslant\frac{1}{m(n-1)}\left(1-\frac{q_0-1}{m(n-1)}\right)^2\\
&\geqslant\frac{1}{m(n-1)}\left(1-\frac{2(q_0-1)}{m}\right).
\end{aligned}$$

引理 2 证明完毕. □

因为询问的顺序并不重要,所以我们可以通过上式计算 Event 1 不发生的概率.其中, $\Pr[F(v_i)=0]=\frac{1}{m(n-1)}, \forall i\in[1,q_0]$.应用条件概率公式,可以得到下限公式 $\frac{1}{m(n-1)}\left(1-\frac{2(q_0-1)}{m}\right)$.该概率的计算方法类似于文献[15].这里,我们取最优的情况,即 $m=4(q_0-1)$, 则 $\Pr[\overline{\text{Event 1}}]\geqslant\frac{1}{8(n-1)(q_0-1)}$.

最后,我们计算 S 成功的概率为

$$\begin{aligned}\Pr[S\text{ wins}]&=\Pr[\overline{\text{Event 1}}\wedge\overline{\text{Event 2}}\wedge\overline{\text{Event 3}}\wedge\overline{\text{Event 4}}\wedge\text{E wins}]\\&=\Pr[\text{E wins}\mid\overline{\text{Event 1}}\wedge\overline{\text{Event 2}}\wedge\overline{\text{Event 3}}\wedge\overline{\text{Event 4}}]\Pr[\overline{\text{Event 4}}\mid\overline{\text{Event 1}}\wedge\overline{\text{Event 2}}\wedge\overline{\text{Event 3}}]\\&\quad\Pr[\overline{\text{Event 3}}\mid\overline{\text{Event 1}}\wedge\overline{\text{Event 2}}]\Pr[\overline{\text{Event 2}}\mid\overline{\text{Event 1}}]\Pr[\overline{\text{Event 1}}]\\&=\varepsilon(k)\frac{1}{q_1}\frac{q_0-q_2}{q_0}\frac{1}{q_0}\Pr[\overline{\text{Event 1}}]\\&\geqslant\frac{q_0-q_2}{8(n-1)(q_0-1)q_0^2q_1}\varepsilon(k).\end{aligned}$$

定理 1 证明完毕. □

5 安全性与效率

通过上述的证明过程,在第 2 节的安全模型中我们可以看到,攻击者具有 3 种能力:获取用户私钥、获取会话密钥和修改协议的传输消息.在这种情况下,协议 1 是安全的,即可以证明协议 1 满足已知密钥安全并能抵抗密钥泄露伪装攻击和未知密钥共享攻击,同时具有完全的前向安全性.然而在 α 或者是 g_2^{α} 泄露的情况下,攻击者在获取运行协议双方的消息传输的情况下,可以通过计算 $K=e(g_2^{\alpha},T_{A_2}T_{B_2})$(其中 T_{A_2} 和 T_{B_2} 定义见第 3 节协议描述)来获取共享密钥,因此,基本协议 1 不具有主密钥安全性.

在第 5.1 节,我们在协议 1 的基础上进行增强,提出一个具有主密钥前向安全性的协议 2.在第 5.2 节,我们给出为协议 1 和协议 2 添加密钥确认过程的方法.

5.1 防止会话密钥托管

在本节,我们采用类似于 Wang[14]的方法为协议 1 增加主密钥前向安全性的性质,即避免协议 1 中会话密钥由用户私钥生成中心托管.

协议 2. 协议 2 中系统建立、用户私钥抽取和协议的前面两步与第 3 节所描述的协议 1 相同.协议 2 的具体流程如下:

1. 与协议 1 第 1 步相同.
2. 与协议 1 第 2 步相同.
3. Alice 计算 $K_{AB}=e(d_{A_1},T_{B_2}g^x)e(d_{A_2}^{-1},T_{B_1}Q_A^x)=e(g_1,g_2)^{x+y}$, $K'_{AB}=T_{B_2}^x$ 及会话密钥 $sk_A=H(A,B,T_A,T_B,K_{AB},K'_{AB})$;
   Bob 计算 $K_{BA}=e(d_{B_1},T_{A_2}g^y)e(d_{B_2}^{-1},T_{A_1}Q_B^y)=e(g_1,g_2)^{x+y}$, $K_{BA}{}'=T_{A_2}^y$, 并计算会话密钥 $sk_B=H(A,B,T_A,T_B,K_{BA},K'_{BA})$.

协议 2 的第 1 步和第 2 步与协议 1 是相同的.协议 2 与协议 1 的不同之处在于,最终的会话密钥生成过程中增加了 K'_{AB} 和 K'_{BA}. 由于 PKG 无法获得 Alice 和 Bob 选取的随机数 x 和 y,因此它无法计算 K'_{AB} 和 K'_{BA} (其中, K'_{AB} 和 K'_{BA} 的计算是一个 Diffie-Hellman 密钥交换过程,其安全性基于判定性 Diffie-Hellman 假设),保证了会话密钥只有 Alice 和 Bob 才能正确计算.

5.2 密钥确认

在实际的应用协议中,协议在进行认证密钥协商过程中,通常需要确认对方正确地计算出了会话密钥.当

然,我们必须假设通信双方都能接收到密钥确认消息,否则密钥确认就不可能顺利完成.比如,如果攻击者总是截获最后一条密钥确认消息,密钥确认就无法完成.在本节我们通过使用添加 MAC(消息认证码)的方法为协议 1 添加密钥确认性质.该方法类似于 Chen 在文献[9]中采用的方法.我们选择一种安全的 MAC 算法,并选择一个哈希函数$H:\mathbb{G}_1 \to \{0,1\}^k$,其中,$k$ 为对应的 MAC 算法的密钥空间长度参数.密钥确认过程如下(其中,系统建立和用户密钥产生的过程与协议 1 相同,K 是协议 1 和协议 2 中计算得出的共享会话密钥):

1. Alice→Bob: T_A.

2. Bob→Alice: $T_B, MAC_{H(K)}(2,\text{Alice},\text{Bob},T_A,T_B)$.

3. Alice→Bob: $MAC_{H(K)}(3,\text{Bob},\text{Alice},T_B,T_A)$.

在增加了密钥确认过程后,协议的安全性证明与第 4 节是类似的.同样地,该协议的安全性仍然建立在 DBDH 困难性假设之上.

5.3 安全性与计算复杂度的比较

如表 1 所示,我们的协议需要 2 次双线性映射计算,4 次群$\mathbb{G}$上的幂运算和 1 次群$\mathbb{G}_1$上的乘法运算.我们的协议与基于随机预言机模型的协议相比,在效率上差别较小,并且$Q_v = u'\prod_{i\in v} u_i$ 都是可以预先计算的,通信双方可以在通信之前预先计算好一部分信息并保存在系统缓存,以提高运算效率.与 Wang[14]的方案相比,我们的协议具有较弱的安全性假设,易于在实际中进行应用.与 Liu[10]的协议相比,我们的协议在效率上具有优势,比 Liu 的协议减少 1 次双线性映射计算,其次,不存在$\mathbb{G}_T$中的指数运算,仅有 1 次乘法运算,而 Liu 的协议中存在 1 次$\mathbb{G}_T$中的指数运算和 2 次乘法运算.

Table 1 Comparison on security properties and computation efficiency

表 1 安全性质与计算效率比较

Schemes	Security properties						Security model	Assumption	Computation cost
	ksk	fs-s	fs-d	fs-m	kci	uks			
Wang-1[14]	√	√	√	×	√	√	Standard	q-ABDHE	$P+S_1+3S_T$
Wang-2[14]	√	√	√	√	√	√	Standard	q-ABDHE	$P+S_1+5S_T$
Liu-1[15]	√	√	√	×	√	√	Standard	DBDH	$3P+3S_1+3S_T$
Liu-2[15]	√	√	√	√	√	√	Standard	DBDH	$3P+4S_1+3S_T$
Our Protocol 1	√	√	√	×	√	√	Standard	DBDH	$2P+4S_1+S_T$
Our Protocol 2	√	√	√	√	√	√	Standard	DBDH	$2P+5S_1+S_T$

P: Pairing computation S_1: Multiplication in $\mathbb{G}_1$ S_T: Multiplication in $\mathbb{G}_T$

6 总 结

在本文中,我们提出了一个在标准模型下可证明安全的基于身份认证密钥协商协议,并在标准模型下通过可证明安全技术对协议进行了分析和证明.该协议具有已知密钥安全、前向安全性和密钥控制等安全性质,并能抵抗密钥泄露伪装攻击和未知密钥共享攻击.与目前的其他类似协议相比,我们的协议具有更高的效率,更适于在实际的基于身份公钥系统中应用.此外,为了满足不需要密钥委托的应用环境,我们对基本协议进行扩展,构造了可以有效防止密钥托管的认证密钥协商协议.最后,我们采用一种安全的消息认证码算法为本文提出的基于身份的认证密钥协商协议增加了密钥确认过程.

References:

[1] Diffie W, Hellman M. New directions in cryptography. IEEE Trans. on Information Theory, 1976,22(6):644−654. [doi: 10.1109/TIT.1976.1055638]

[2] Shamir A. Identity-Based cryptosystems and signature schemes. In: Blakely GR, Chaum D, eds. Advances in Cryptology. LNCS 196, Heidelberg: Springer-Verlag, 1984. 47−53.

[3] Boneh D, Franklin M. Identity based encryption from the Weil pairing. In: Kilian J, ed. Advances in Cryptology-Crypto 2001. LNCS 2139, Heidelberg: Springer-Verlag, 2001. 213−229. [doi: 10.1007/3-540-44647-8_13]

[4] Cheng Z, Chen L. On security proof of McCullagh-Barreto's key agreement protocol and its variants. Report, 2005/201, 2005. http://eprint.iacr.org/2005/201 [doi: 10.1504/IJSN.2007.013178]

[5] Chen LQ, Kudla C. Identity based authenticated key agreement protocols from pairings. In: Proc. of the 16th IEEE Computer Security Foundations Workshop. Pacific Grove: IEEE Computer Society Press, 2003. 219−233. [doi: 10.1109/CSFW.2003.1212715]

[6] Smart NP. An identity based authenticated key agreement protocol based on the Weil pairing. Electronics Letters, 2002,38(13): 630−632. [doi: 10.1049/el:20020387]

[7] Cheng Z, Chen L, Comley R, Tang Q. Identity-Based key agreement with unilateral identity privacy using pairings. In: Chen K, Deng R, Lai X, Zhou J, eds. Information Security Practice and Experience. LNCS 3903, Heidelberg: Springer-Verlag, 2006. 202−213. [doi: 10.1007/11689522_19]

[8] Shim K. Efficient ID-based authenticated key agreement protocol based on the Weil pairing. Electronics Letters, 2003,39(8): 653−654. [doi: 10.1049/el:20030448]

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

[10] Peng HX. An identity-based authentication model for multi-domain. Chinese Journal of Computers, 2006,29(8):1271−1281 (in Chinese with English abstract).

[11] Waters B. Efficient identity-based encryption without random oracles. In: Cramer R, ed. Advances in Cryptology—EUROCRYPT 2005. LNCS 3494, Heidelberg: Springer-Verlag, 2005. 114−127. [doi: 10.1007/11426639_7]

[12] Boneh D, Boyen X. Secure identity based encryption without random oracles. In: Franklin M, ed. Advances in Cryptology—CRYPT 2004. LNCS 3152, Heidelberg: Springer-Verlag, 2004. 443−459. [doi: 10.1007/978-3-540-28628-8_27]

[13] Gentry C. Practical identity-based encryption without random oracles. In: Vaudenay S, ed. Advances in Cryptology—EUROCRYPT 2006. LNCS 4004, Heidelberg: Springer-Verlag, 2006. 445−464.

[14] Wang SB, Cao ZF, Kwang K, Choo R. Provably secure identity-based authenticated key agreement protocols without random oracles. Report, 2006/446, 2006. http://eprint.iacr.org/2006/446

[15] Liu ZH, Hu YP, Zhang XS, Ma H. New two-party identity-based authenticated key agreement protocol without random oracles. In: Lin DD, ed. Proc. of the 4th Int'l Conf. on Information Security and Cryptology. Beijing: Science Press, 2009. 78−91.

附中文参考文献:

[10] 彭华熹.一种基于身份的多信任域认证模型,计算机学报,2006,29(8):1271−1281.

高志刚(1982－),男,河南新密人,博士生,主要研究领域为网络和系统安全,身份鉴别技术.

冯登国(1965－),男,博士,研究员,博士生导师,主要研究领域为网络安全,人工智能.