软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2016,27(Suppl.(2)):12−17

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

基于分层身份的网络密钥协商协议*

薛 天, 王小峰, 苏金树, 陈培鑫

(国防科学技术大学 计算机学院,湖南 长沙 410073)

通讯作者: 薛天, E-mail: xuetian@nudt.edu.cn

摘 要: 为保证开放网络环境下的安全通信,在现有基于身份密码体制的基础上,提出一种新的基于分层身份的网络密钥协商协议.新协议满足所有密钥协商的安全属性,计算效率全面领先目前已有协议,能够有效地解决传统公钥系统需要进行证书传递和验证的问题,且能满足大规模网络应用的需求.

关键词: 密钥协商;基于身份密码体制;基于分层身份加密;网络安全通信;双线性对

中文引用格式: 薛天,王小峰,苏金树,陈培鑫.基于分层身份的网络密钥协商协议.软件学报,2016,27(Suppl.(2)):12−17. http://www.jos.org.cn/1000-9825/16013.htm

英文引用格式: Xue T, Wang XF, Su JS, Chen PX. Hierarchical identity-based key agreement protocol of Internet. Ruan Jian Xue Bao/Journal of Software, 2016,27(Suppl.(2)):12−17 (in Chinese). http://www.jos.org.cn/1000-9825/16013.htm

Hierarchical Identity-Based Key Agreement Protocol of Internet

XUE Tian, WANG Xiao-Feng, SU Jin-Shu, CHEN Pei-Xin

(School of Computer Science, National University of Defense Technology, Changsha 410073, China)

Abstract: To ensure the communication security in a public network, a hierarchical identity-based key agreement protocol based on the present identity-based cryptosystem is proposed in this paper. The new protocol which is able to solve the problem of the certification transfering and verifying in the traditional public key cryptosystem efficiently achieves all of the known security attributes and can be achieved in the state-of-art speed which can meet the demand of large scale network applications.

Key words: key agreement; identity-based cryptosystem; hierarchical identity based encryption (HIBE); network secure communication; bilinear pairing

1 引 言

互联网、电子商务和电子政务的普及,在为社会经济发展带来巨大利益的同时,也带来了更加严峻的安全问题.在网络信息交互的应用环境中,公钥基础设施(public key infrastructure,简称 PKI)体系虽然从技术上可以解决网上认证、信息完整性和抗抵赖性等安全问题,但其安全保障是由证书来完成的,证书的管理和维护需要大量的处理资源和带宽资源,部署成本较高.

1984 年 Shamir 首次提出基于身份密码体制(identity-based cryptosystem,简称 IBC)的概念[1].其基本思想是将用户的身份与其公钥以最自然的方式绑定:用户的身份信息即为用户的公钥.在 IBC 系统内,用户的身份注册和私钥生成由一个可信的私钥生成器(private key generator,简称 PKG)完成.当一个用户使用另一个用户的公钥信息时,只需要知道该用户的身份信息,而无需再去获取和验证该用户的公钥证书,大大降低了密码系统中密钥管理的难度[2].2000 年 Sakai 最早提出了基于身份的签名(identity-based signature,简称 IBS)方案[3].2001 年 Boneh 和 Franklin 利用双线性配对设计出第一个真正实用的基于身份加密(identity-based encryption,简称 IBE)方案[4].2002 年 Smart 利用 Boneh 基于身份的加密方案,设计了第一个基于双线性对的认证密钥协商协议[5].之后,大量基于

* 收稿时间: 2015-05-31; 采用时间: 2016-01-05

身份的安全方案被陆续提出.

但是,单个 PKG 无法承担起大规模系统的身份注册与私钥生成任务[6],2002 年 Gentry 和 Silverberg 第一次提出了一个完整的建立在随机预言机模型下、双线性 Diffie-Hellman(BDH)假设基础上的基于身份的分层密码算法(hierarchical ID-based cryptography,简称 HIBC)[7].该方案将 PKG 的功能分为多层,包括一个根 PKG 和多层的域 PKG.根 PKG 只为域 PKG 生成私钥,并对其进行身份认证.域 PKG 在得到私钥之后又可以利用自己的私钥为下层的域 PKG 生成私钥,直至最终用户的上一层,而这一层的 PKG 往往处于用户的本地或局域网中,这就使得对用户的认证和密钥的传输都在本地进行.如果低层 PKG 的密钥泄露,只会影响其域内用户,而不影响高层 PKG 的安全性.本文认为,未来的安全通信领域将以 IBC 为基础,签名使用(H)IBS,加密使用(H)IBE,密钥协商使用(H)IBKA(identity-based key agreement).

密钥协商协议在网络安全通信中具有重要的基础性作用[8],本文以 Hu 等人提出的 HIBE 系统[9]为基础,提出了一种基于分层身份的密钥协商(HIBKA)机制,并给出其安全性证明.

2 预备知识

2.1 双线性映射

设 G_1 是由 g 产生的循环乘法群,它的阶是素数 p,G_2 是同阶的循环乘法群,映射 $e:G_1\times G_1\to G_2$ 是一个双线性映射,如果映射满足下面的条件:

(1) 双线性:对于所有的 $u,v\in G_1,a,b\in Z_p$,有 $e(u^a,v^b)=e(u,v)^{ab}$;

(2) 非退化性:存在 $e(g,g)\neq 1$,1 为 G_2 的单位元;

(3) 可计算性:对于所有的 u,v,存在一种有效的算法计算 $e(u,v)$.

2.2 难题假设

假设 1. CDH(computational Diffie-Hellman problem)问题.

G 为 q 阶椭圆曲线乘法循环群,q 为素数.随机选取 G 的生成元 g 以及 $a,b\in Z_q^*$,则对于给定的 g,g^a,g^b,计算 g^{ab} 是困难的.

假设 2. BDH(bilinear Diffie-Hellman)问题.

设 G_1,G_2 为两个具有素数 q 阶的点群,$e:G_1\times G_1\to G_2$ 为一个可采纳的双线性映射,g 为 G_1 的生成元,$a,b,c\in Z_q^*$,则对于给定的 g,g^a,g^b,g^c,计算 $e(g,g)^{abc}\in G_2$ 是困难的.

假设 3. 截断判定性 q-ABDHE(truncated decision q-augmented bilinear Diffie-Hellman exponent)问题.

已知一个有 $q+3$ 个元素的矢量 $(g',g'^{\alpha^{q+2}},g,g^{\alpha},g^{\alpha^2},...,g^{\alpha^q})\in G_1^{q+3}$ ($\alpha\in Z_p,p$ 为 G_1 的阶),元素 $Z\in G_2$ 作为输入,如果 $Z=e(g^{\alpha^{q+1}},g')$,输出 0,否则,输出 1.如果 $|Pr[B(g',g'^{\alpha^{q+2}},g,g^{\alpha},...,g^{\alpha^q},e(g^{\alpha^{q+2}},g'))=0]-Pr[B(g',g'^{\alpha^{q+2}},g,g^{\alpha},...,g^{\alpha^q},Z)=0]|\geqslant\varepsilon$,则称算法 B 以$\varepsilon$的优势解决了截断判定性 q-ABDHE 问题.这里的概率同生成元 g,g'在群 G_1 中的随机选取、α在 Z_p 中的随机选取、Z 在 G_2 中的随机选取以及算法 B 使用的随机比特有关.

3 新的 HIBKA 方案

本文基于文献[9]中提出的 HIBE 方案进行密钥协商,私钥安全性基于 q-ABDHE 假设.设 G 和 G^T 是 p 阶循环群,e 是双线性映射:$G\times G\to G_T$,消息空间是 G_T,身份空间是 Z_p,l 是指定为 HIBE 最大层的正整数.定义身份向量表示用户在层次结构中的位置,一个深度为 d 的分层身份 ID 是一个 d 元组 $ID=(ID_1,ID_2,\ldots,ID_d)$,如果 ID 是 ID' 的一个前缀,则身份为 ID 的 PKG 是身份为 ID'的 PKG(用户)的祖先.

3.1 协议描述

系统建立:PKG 从 G 中随机选取生成元 g,g_0,从 G 中随机选取 $g_2,g_3,h_1,h_2,...,h_l,u_1,u_2,\ldots,u_l$,从 Z_p 中随机选取α,γ,μ.设 $g_1=g^{\alpha},F(k)=u_kh_k^{-u}$,其中,$1\leqslant k\leqslant l,g_4=g_1g^{-u},g_5=g_2g_3^{-u}$,公共参数 $params=\{r,g_0,g,g_4,g_5,F(1),\ldots,F(l)\}$,主密钥是$\alpha,\mu$.

私钥生成:设 $ID=(ID_1,ID_2,...,ID_i)\in Z_p^i$, $1\leqslant i\leqslant l$,从 Z_p^* 选取随机指数 r_i,定义身份 ID 的私钥 $d_{ID}=(a_0,b_{i+1},\ldots,b_l)$,其中,

$$a_0=(g^{-r})^{(\alpha-u)}\cdot\left(\prod_{k=1}^{i}F(k)^{ID_k}\cdot g_5\right)^{r_i},$$

$$b_{i+1}=F(i+1)^{r_i},\ldots,b_l=F(l)^{r_i}.$$

这个私钥可以由根 PKG 生成,也可由其身份为$(ID_1,ID_2,\ldots,ID_{i-1})$的父节点生成,假设身份$(ID_1,ID_2,\ldots,ID_{i-1})$的私钥是 $(a_0',b_i',...,b_l')$,其随机指数为 r_{i-1}',为了得到身份$(ID_1,ID_2,\ldots,ID_i)$的私钥$(a_0,b_{i+1},...,b_l)$,首先从 Z_p 中随机选择 t,然后计算:

$$a_0=a_0'\cdot b_i'^{ID_i}\cdot\left(\prod_{k=1}^{i}F(k)^{ID_k}\cdot g_5\right)^{t},$$

$$b_{i+1}=b_{i+1}'\cdot F(i+1)^{t},$$

$$\cdots$$

$$b_l=b_l'\cdot F(l)^{t}.$$

这个私钥满足 $r_i=r_{i-1}'+t\in Z_p$,且关于 ID 在值域内是随机分布的.

密钥协商:设用户 A 和 B 在第 $i(1\leqslant i<l)$层有公共节点,A 的身份 $ID_A=(ID_1,ID_2,...,ID_i,ID_{i+1},...,ID_k)$,取随机指数为 r_k,私钥 $SK_A=(a_0,b_{k+1},...,b_l)$.$B$ 的身份 $ID_B=(ID_1,ID_2,...,ID_i,ID'_{i+1},...,ID'_m)$,取随机指数为 r_m,私钥 $SK_B=(a'_0,b'_{m+1},...,b'_l)$.

步骤 1. A 随机选取 $x\in Z_p^*$作为临时密钥,计算 X 并发送给 B.

$$X=[(a_0/(F(i+1)^{ID_{i+1}}...F(k)^{ID_k})^{r_k})^x,g_0^x]=[((g_0^{-r})^{\alpha-u}(F(1)^{ID_1}F(2)^{ID_2}...F(i)^{ID_i}\cdot g_5)^{r_k})^x,g_0^x].$$

步骤 2. B 随机选取 $y\in Z_p^*$作为临时密钥,计算 Y 并发送给 B.

$$Y=[(a_0'/(F(i+1)^{ID'_{i+1}}...F(m)^{ID'_m})^{r_m})^y,g_0^y]=[((g_0^{-r})^{\alpha-u}(F(1)^{ID_1}F(2)^{ID_2}...F(i)^{ID_i}\cdot g_5)^{r_m})^y,g_0^y].$$

步骤 3. A 根据 Y 计算共享秘密 S_A:

$$S_A=e((g_0^{-r})^{\alpha-u}\cdot(F(1)^{ID_1}F(2)^{ID_2}...F(i)^{ID_i}\cdot g_5)^{r_m})^y,(g^{r_k})^x)\cdot e(g_0^y,((g_4^r)^{r_k})^x).$$

B 根据 X 计算共享秘密 S_B:

$$S_B=e((g_0^{-r})^{\alpha-u}\cdot(F(1)^{ID_1}F(2)^{ID_2}...F(i)^{ID_i}\cdot g_5)^{r_k})^x,(g^{r_m})^y)\cdot e(g_0^x,((g_4^r)^{r_m})^y).$$

步骤 4. A 计算会话密钥 $SK_A=H(ID_A,ID_B,X,Y,S_A)$,$B$ 计算会话密钥 $SK_B=H(ID_A,ID_B,X,Y,S_B)$,其中,$H:\{0,1\}^*\rightarrow\{0,1\}^n$ 为输出为定长的 Hash 函数.

3.2 正确性证明

$$\begin{aligned}
S_A&=e(((g_0^{-r})^{\alpha-u}\cdot(F(1)^{ID_1}F(2)^{ID_2}...F(i)^{ID_i}\cdot g_5)^{r_m})^y,(g^{r_k})^x)\cdot e(g_0^y,((g_4^r)^{r_k})^x)\\
&=e(((g_0^{-r})^{\alpha-u})^y,(g^{r_k})^x)\cdot e(((F(1)^{ID_1}F(2)^{ID_2}...F(i)^{ID_i}\cdot g_5)^{r_m})^y,(g^{r_k})^x)\cdot e(g_0^y,((g_4^r)^{r_k})^x\\
&=e(((g_0^{-r})^{\alpha-u})^y,(g^{r_k})^x)\cdot e(g_0^y,(((g^{\alpha-u})^r)^{r_k})^x\cdot e(((F(1)^{ID_1}F(2)^{ID_2}...F(i)^{ID_i}\cdot g_5)^{r_m})^y,(g^{r_k})^x)\\
&=e(((F(1)^{ID_1}F(2)^{ID_2}...F(i)^{ID_i}\cdot g_5)^{r_m})^y,(g^{r_k})^x)\\
&=e(F(1)^{ID_1}F(2)^{ID_2}...F(i)^{ID_i}\cdot g_5,g)^{r_kxr_my}.\\
S_B&=e(((g_0^{-r})^{\alpha-u}\cdot(F(1)^{ID_1}F(2)^{ID_2}...F(i)^{ID_i}\cdot g_5)^{r_k})^x,(g^{r_m})^y)\cdot e(g_0^x,((g_4^r)^{r_m})^y)\\
&=e(((g_0^{-r})^{\alpha-u})^y,(g^{r_m})^y)\cdot e(((F(1)^{ID_1}F(2)^{ID_2}...F(i)^{ID_i}\cdot g_5)^{r_k})^x,(g^{r_m})^y)\cdot e(g_0^x,((g_4^r)^{r_m})^y\\
&=e(((g_0^{-r})^{\alpha-u})^y,(g^{r_m})^y)\cdot e(g_0^x,(((g^{\alpha-u})^r)^{r_m})^y\cdot e(((F(1)^{ID_1}F(2)^{ID_2}...F(i)^{ID_i}\cdot g_5)^{r_k})^x,(g^{r_m})^y)\\
&=e(((F(1)^{ID_1}F(2)^{ID_2}...F(i)^{ID_i}\cdot g_5)^{r_k})^x,(g^{r_m})^y)\\
&=e(F(1)^{ID_1}F(2)^{ID_2}...F(i)^{ID_i}\cdot g_5,g)^{r_kxr_my}\\
&=S_A.
\end{aligned}$$

□

4 安全性证明

密钥协商协议的安全属性基于对攻击者能力的假设,而攻击者的目的就是要攻破这些安全属性.下面对安全属性进行具体叙述[10],并证明本文提出的方案满足目前所有安全属性.

(1) 已知会话密钥安全性.

已知旧的会话密钥不会影响其他会话密钥安全性.

参与者每次进行密钥协商都会选取新的 x,y,故攻击者不能根据某次会话密钥计算其他的会话密钥.

(2) 前向安全性.

如果一方或多方参与实体的长期私钥泄露,攻击者不能有效计算旧的会话密钥,则称为部分前向安全性;如果所有参与实体的长期私钥泄露,攻击者仍然不能有效计算旧的会话密钥,则称为完美前向安全性.

如果双方的长期私钥 r_k,r_m 泄露给攻击者,攻击者并不知道临时私钥 x,y,故没有办法计算

$$e(F(1)^{ID_1}F(2)^{ID_2}...F(i)^{ID_i}\cdot g_5,g)^{r_m x r_k y}\ (S_A \text{ 或 } S_B),$$

不能得到共享密钥.

(3) PKG 前向安全性.

在基于身份的密钥协商协议中,攻击者即使获得私钥产生中心 PKG 的主密钥,仍然无法计算参与实体的会话密钥.

本文提出的密钥协商协议,其主密钥在计算过程中被消掉,故获得主密钥仍不能计算会话密钥.

(4) 抗密钥泄露伪装.

一个参与实体 A 的长期密钥泄露将使得攻击者可以伪装 A,但不应导致攻击者可以伪装成其他实体与 A 进行成功的密钥协商.

攻击者虽然得到 A 的长期密钥,但不能由长期密钥计算得到系统主密钥,故攻击者不能正确生成其他用户的私钥.倘若攻击者臆造主密钥,则协商过程中 $S_A\neq S_B$.

(5) 无密钥控制(密钥完整性).

会话密钥生成后,协议参与方必须对会话有相同的贡献,会话密钥值不受任何一方控制.

在 S_A,S_B 的计算过程中,$F,ID_i(1\leqslant i<l)$为已知量,r_k,x 由 A 产生,r_m,y 由 B 产生,A,B 所做贡献相同,在产生 SK_A,SK_B 的过程中,A,B 所做贡献也相同,故协议参与方有相同贡献且会话密钥值不受任何一方控制.

(6) 抗未知密钥共享.

一个参与实体 A 不应被强迫与一个实体 C 实现共享会话密钥,而实际上参与实体 A 却认为他是在和意定参与实体 B 完成密钥协商.

用户私钥产生过程中,用到主密钥和随机指数并且基于 q-ABDHE 问题,C 在冒充 B 的过程中不能正确产生 B 的私钥,故不能正常进行密钥协商.

(7) 消息独立性.

两方或多方参与会话密钥协商的实体交互的消息应是独立产生并交互的,不受其他方的制约和强迫.

在私钥产生过程中,双方随机指数 r_i 的选取满足随机分布,临时密钥 x,y 的选取是随机独立选取的,故本协议能满足消息独立性.

(8) 已知会话相关临时秘密信息安全性.

当参与实体在一次会话密钥协商过程中使用的临时秘密信息(临时密钥)泄露后(但长期私钥未泄露),不应影响到会话密钥的安全性.

本协议中,攻击者利用临时密钥不能计算出任何有用信息,且 $S_A(S_B)$ 由 r_k,r_m,x,y 共同决定,因此临时密钥泄露不影响本次通话的安全性,更不会影响其他通话的安全性.

综上所述,本文提出的新的密钥协商协议具有良好的安全性.

5 复杂度分析

对于一个密钥协商协议的考量,不能只关注其安全性,也要对其可行性进行分析.目前,标准模型下可证安全的 HIBKA 方案由文献[6]提出,现对本文提出的 HIBKA 方案进行复杂度分析并与文献[6]中的方案进行对比,见表 1.其中,E 代表指数运算,M 与 M_T 分别表示 G 和 G^T 上的乘法运算,P 表示双线性运算,k,m 为用户所处的层级,i 为双方共同祖先的层数,l 为系统总层级数,H 表示 Hash 运算.在文献[6]中总结的计算复杂度为近似值,本文采用精确值进行比较.

从表 1 中对比可以看出,本文提出的 HIBKA 协议在具有较高安全性的同时,运算效率也全面领先现有协议,并且在生成共享秘密的过程中复杂度为常数,因此具有较高的可行性.

Table 1 Comparison of protocol complexity

表 1 协议复杂度对比

协议执行阶段	曹等人的 HIBKA 方案	本文提出的 HIBKA 方案
私钥生成	$(l+2)\cdot E+(k+1)\cdot(E+M)$	$(l+3)E+(k+1)M$ (根 PKG), $(l+2)\cdot(E+M)$ (上层 PKG)
生成 X	$2(m-i)\cdot(E+M)+3E$	$(k-i)\cdot(E+M)+3E$
生成 Y	$2(k-i)\cdot(E+M)+3E$	$(m-i)\cdot(E+M)+3E$
生成 S_A	$(k-i+2)\cdot E+(k-i-1)\cdot M+3P+2M_T$	$5E+2P+M_T$
生成 S_B	$(m-i+2)\cdot E+(m-i-1)\cdot M+3P+2M_T$	$5E+2P+M_T$
生成 SK_A 与 SK_B	H	H

6 结束语

本文以 Hu 等人提出的 HIBE 系统为基础,提出了一种新的基于分层身份的密钥协商协议,用于大规模网络的安全通信.新协议能够较好地满足当前密钥协商所有的安全属性,且计算复杂度较低,具有较高的可行性.由于采用基于身份的公钥密码体制,相比于传统 PKI,不仅节省了建立和管理公钥基础设施的代价,而且避免了用户存储、管理和传输公钥证书等问题.在未来网络的安全通信领域,基于身份密码体制将表现出越来越明显的优势.

References:

[1] Shamir A. Identity-Based cryptosystems and signature schemes. Lecture Notes in Computer Science, 1984,196:47–53.

[2] Sun JM, Sun Y, Zhang SD, Pei QQ. Identity (ID)-Based authentication and the key agreement protocol. Journal of Xidian University (Natural Science), 2008,35(3) (in Chinese with English abstract).

[3] Boneh D, Franklin M. Identity-Based encryption from the Weil pairing. SIAM Journal on Computing, 2003,32(3):586–615.

[4] Paterson KG. ID-Based signatures from pairings on elliptic curves. Electronics Letters, 2002,38(18):1025–1026.

[5] Smart NP. An identity based authenticated key agreement protocol based on the Weil pairing. Electronics Letters, 2002,38(13): 630–632.

[6] Cao CL, Liu MQ, Zhang R,Yang YX. Provably secure authenticated key agreement protocol based on hierarchical identity. Journal of Electronics & Information Technology, 2014,(12) (in Chinese with English abstract).

[7] Gentry C, Silverberg A. Hierarchical ID-based cryptography. Lecture Notes in Computer Science, 2002,2501:548−566.

[8] Wang SB, Cao ZF, Dong XL. Provably secure identity-based authenticated key agreement protocols in the standard model. Chinese Journal of Computers, 2007,30(10) (in Chinese with English abstract).

[9] Hu X, Huang S, Fan X. Practical hierarchical identity based encryption scheme without random oracles. IEICE Fundamentals of Electronics, Communications and Computer Sciences, 2009,E92-A(6):1494–1499.

[10] Blake-Wilson S, Johnson D, Menezes A. Key agreement protocols and their security analysis. In: Proc. of the 6th IMA Int'l Conf. on Cryptography and Coding. LNCS 1355, Berlin: Springer-Verlag, 1997. 30–45.

附中文参考文献:

[2] 孙纪敏,孙玉,张思东,裴庆祺.基于 ID 的认证及密钥协商协议.西安电子科技大学学报(自然科学版),2008,35(3).

[6] 曹晨磊,刘明奇,张茹,杨义先.基于层级化身份的可证明安全的认证密钥协商协议.电子与信息学报,2014,(12).

[8] 王圣宝,曹珍富,董晓蕾.标准模型下可证安全的身份基认证密钥协商协议.计算机学报,2007,30(10).

薛天(1991－),男,河北唐山人,学士,主要研究领域为计算机网络与通信,信息安全.

苏金树(1962－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为计算机网络与通信,信息安全.

王小峰(1982－),男,博士,助理研究员,CCF 专业会员,主要研究领域为可信网络及系统,网络安全,分布智能数据处理.

陈培鑫(1987－),男,硕士,主要研究领域为基于身份加密,域间路由安全.