Journal of Computer Applications
计算机应用,2013,33(5):1353 - 1356
ISSN 1001-9081
CODEN JYIIDU
2013-05-01
http://www.joca.cn

文章编号:1001 - 9081(2013)05 - 1353 - 04
doi:10.3724/SP.J.1087.2013.01353

独立网络中新的双方密钥协商协议

李海峰[1*],蓝才会[2],左为平[1],马海云[1]
(1.天水师范学院 物理与信息科学学院,甘肃 天水 741001; 2.西北师范大学 数学与信息科学学院,兰州 730070)
(*通信作者电子邮箱 hfli78@163.com)

摘 要:现有的密钥协商协议大多研究同一密钥生成中心(KGC)下的安全会话,即参与者的参数都由同一 KGC 提供。为了实现处于不同 KGC 中的参与者的安全会话,采用椭圆曲线设计方案提出了一种新的基于身份的双方认证密钥协商协议,新协议实现了两个具有独立参数的 KGC 中参与者的安全密钥协商。还利用改进的 Blake-Wilson 模型对新协议的安全性进行了严格的形式化证明。通过分析表明该新协议不但具有足够的安全性,而且还具备计算量小、效率高的特点,因而,可用于对能耗要求高的轻量级设备中。

关键词:密钥协商;独立网络;椭圆曲线;密钥生成中心;可证明安全
中图分类号:TP309.7 **文献标志码**:A

New two-party key agreement protocol in separate networks

LI Haifeng[1*], LAN Caihui[2], ZUO Weiping[1], MA Haiyun[1]
(1. *College of Mathematics Physics and Information Science, Tianshui Normal University, Tianshui Gansu* 741001, *China*;
2. *College of Mathematics and Information Science, Northwest Normal University, Lanzhou Gansu* 730070, *China*)

Abstract: There is much research about key agreement focus on the secure communication in the same Key Generation Center (KGC), i.e. all the parameters of different participants should be provided by one KGC. To realize the secure communication between two users in different KGCs, adopting elliptic curve cryptography algorithm, a new two-party ID-based key agreement protocol was proposed. This new scheme realized key agreement protocol in separate networks between two participants. Then the improved Blake-Wilson model was used to prove the security of the scheme. After being analyzed, the new protocol was proved to be secure, efficient and of lower computational cost. Therefore, the new scheme will be compatible with low-power and lightweight devices.

Key words: key agreement; separate network; elliptic curve; Key Generation Center (KGC); provable security

0 引言

在公钥密钥体制中,每个参与者都拥有一个私钥和一个对应的公钥。这一领域的主要问题是如何在用户身份(Identity,ID)与其公钥之间建立联系,一种常见的方法是在 ISO/IEC 95948[1] 中定义的基于公钥基础设施(Public Key Infrastructure,PKI)的手段。在这种解决办法中,一个称之为证书中心(Certificate Authority,CA)的可信第三方向参与者颁布一张用参与者私钥签名的证书,证书中包含了该参与者的 ID 和公钥信息。然而,由于这种方法成本甚高,基于身份的密码学(ID-Based Cryptography,IBC)应运而生。

1984 年,Shamir 首次提出了 IBC 的概念[2]。在一个 IBC 系统中,参与者的 ID 作为它的公钥,私钥则由称为密钥生成中心(Key Generation Center,KGC)的可信第三方产生。IBC 与传统的基于证书的密码体制相比的优势在于,前者并不要求第三方为每个参与者生成一个证书,因为在 IBC 中的公钥就是参与者的 ID。

2001 年,Boneh 等[3]利用双线性对提出了首个基于身份的加密方案。之后,学者们提出了大量利用双线性对构造的基于身份的认证密钥协商协议[4-7]。在传统的基于身份的加密方案中,参与者从一个 KGC 中获取各自的私钥。在一个简单的组织中,一个独立的 KGC 就可以支撑组织中参与者私钥的分配,但当多个组织存在时,由单一 KGC 来为不同组织的成员生成私钥显然不现实;另外,类似于文献[7]中假设不同的 KGC 使用相同系统参数也是不合理的。因此有必要研究不同 KGC 使用不同系统参数的问题。2005 年,Lee 等[8]提出了首个解决这一问题的双方和三方的基于身份的认证密钥协商协议。随后,Kim 等[9]改进了该协议,弥补了一个安全漏洞。

协议的高效性是研究的另一方面,根据文献[10 - 11]的研究结果,一个双线性对运算相当于三个模乘运算(在相同的乘法域中)。在低能耗的设备如掌上电脑(Personal Digital Assistant,PDA)、手机环境中,使用双线性对运算显然能耗是比较高的。为了解决这一问题,学者们又提出了利用椭圆曲线密钥体制(Elliptic Curve Cryptography,ECC)构造基于身份的密码方案的思路[12-14]。

本文沿着这一研究路线,提出了一种新的利用椭圆曲线构造的基于身份的认证密钥协商方案。新方案的最大特点就是其可用于对于能耗和存储要求高的轻量级设备,而独立网络的特点使得不同网络中的参与者可以分享协商的会话密钥

收稿日期:2012-11-27;**修回日期**:2013-01-04。
基金项目:国家自然科学基金资助项目(61163038);甘肃省自然科学基金资助项目(3ZS051-A25-042);天水师范学院科研项目(TSE0810)。
作者简介:李海峰(1978 -),男,河北安国人,讲师,硕士,主要研究方向:密码学; 蓝才会(1977 -),男(余族),江西永丰人,博士,主要研究方向:信息安全、密码学; 左为平(1976 -),男,甘肃甘谷人,讲师,硕士,主要研究方向:密码学; 马海云(1974 -),男(回族),甘肃徽县人,副教授,硕士,主要研究方向:软件工程、密码学。

以用于随后的安全通信。

1 基础知识

本章介绍本文用到的基础知识，包括椭圆曲线和椭圆曲线中计算 Diffie-Hellman（computational Diffie-Hellman，CDH）问题，用于基于身份的密钥协商协议的安全模型——CCS 模型。

1.1 椭圆曲线

设 F_p 是阶为 p 的有限域，则在 F_p 上的椭圆曲线的 Weierstrass 形式定义为 $E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$，这里 $a_1, a_2, a_3, a_4, a_6 \in F_p$。

椭圆曲线的 CDH 问题是指：对于 $a, b \in_R \mathbf{Z}_p^*$，给定 $P, aP, bP \in G$，计算 $abP \in G$ 是困难的。

1.2 安全模型

现在回顾由著名的 BW（Blake-Wilson）模型[15] 改进而来的 CCS 模型。在该模型中，每个参与者都被模拟成概率多项式时间图灵机，可以同时执行多项式次数的协议。假设协议中的两个参与者为 i 和 j，则记双方运行的第 s 次会话为 Π_{ij}^s。

本文通过一个挑战者（Challenger）和敌手 E 之间的游戏（Game）定义双方认证密钥协商协议的安全性。在该游戏中，M 被允许进行下面的预言机查询（Oracle query），并且，这些查询是无序的：

Send(Π_{ij}^s, x)：当收到消息 x 后，Π_{ij}^s 执行协议并回复消息，或者回复是否执行该会话。如果 Π_{ij}^s 不存在，收到该消息后，系统将作为发起者创建这一会话（当 $x = \lambda$）；否则则作为响应者。在本文中，要求 $i \neq j$，也就是不允许参与者与自己发起会话，这一假设在实际中是合理的。

Reveal(Π_{ij}^s)：如果 Π_{ij}^s 未被接受，则返回 $\perp$；否则返回会话密钥。

Corrupt(i)：参与者 i 将回复其的私钥。

在游戏的某些时刻，敌手 E 可以向一个新鲜的（Freshness，见定义 1）会话 Π_{ij}^s 进行 Test 查询。这时，Π_{ij}^s 通过投掷一枚硬币 $b \in \{0,1\}$ 来回答此查询：若投币结果为 0，那么它返回协商得到的会话密钥；否则返回密钥空间 $\{0,1\}^k$ 上的一个随机值。这里，k 表示会话密钥的比特长度。

在游戏的最后，E 输出 $b' \in \{0,1\}$ 作为对 b 的判断，若 $b = b'$，则称敌手 E 赢得了此游戏。

定义 1 新鲜性。如果满足如下条件，则称 Π_{ij}^s 是新鲜的：

1）Π_{ij}^s 已经被接受；

2）Π_{ij}^s 未被进行 Reveal 查询；

3）参与者 $j \neq i$ 未被进行 Corrupt 查询；

4）不存在 Π_{ji}^t，对应于 Π_{ij}^s。

定义 2 协议的安全性。在该模型下，敌手 E 攻击协议的优势定义为 $Adv^E(k) = |2\Pr[b = b'] - 1|$。对于任意的概率多项式时间敌手，如果其赢得上述游戏的优势是可以忽略的，则称该协议是安全的。

2 新的基于 ECC 的密钥协商方案

新协议共由三个算法构成：系统初始化算法、参与者密钥生成算法和会话密钥协商算法。

2.1 系统初始化

在新方案中，有 n 个不同的 KGC，并且这些 KGC 不共享系统参数。因此，每个 KGC 都执行如下操作：

1）随机选择一个素数 $p^{(i)}$ 并确定一个四元数组 $\{F_{p^{(i)}}, E^{(i)}/F_{p^{(i)}}, G^{(i)}, P^{(i)}\}$；

2）选择一个安全的 Hash 函数：$\{0,1\}^* \times G^{(i)} \rightarrow \mathbf{Z}_{p^{(i)}}^*$；

3）随机选择其主密钥 $x^{(i)} \in_R \mathbf{Z}_{p^{(i)}}^*$ 并计算系统公钥：$P_{\text{pub}}^{(i)} = x^{(i)}P^{(i)}$；

4）公布系统参数 $\{F_{p^{(i)}}, E^{(i)}/F_{p^{(i)}}, G^{(i)}, P^{(i)}, P_{\text{pub}}^{(i)}, H_1^{(i)}\}$。

2.2 参与者密钥生成

每个 KGC 将通过如下方式为参与者生成密钥：

1）选择一个随机数 $r_U \in_R \mathbf{Z}_{p^{(i)}}^*$，计算 $R_U = r_UP^{(i)}$ 和 $h_U = H_1^{(i)}(ID_U, R_U)$；

2）计算 $s_U = r_U + h_Ux^{(i)}$。

KGC 将参与者 U 的私钥 s_U 通过安全信道发送给 U。U 可以通过验证等式来辨别私钥的真伪性：$s_UP^{(i)} = R_U + H_1^{(i)}(ID_U, R_U)P_{\text{pub}}^{(i)}$。

2.3 会话密钥协商

两个独立 KGC 中的参与者 A 和 B 可以通过如下步骤完成密钥协商：

1）$A \rightarrow B$：$\{ID_A, T_A^{(1)}, T_A^{(2)}, R_A\}$。

A 选择两个随机数 $a^{(1)} \in_R \mathbf{Z}_{p^{(1)}}^*$ 和 $a^{(2)} \in_R \mathbf{Z}_{p^{(2)}}^*$，计算 $T_A^{(1)} = a^{(1)}P^{(1)}$，$T_A^{(2)} = a^{(2)}P^{(2)}$，并将 $\{ID_A, T_A^{(1)}, T_A^{(2)}, R_A\}$ 发送给参与者 B。

2）$B \rightarrow A$：$\{ID_B, T_B^{(1)}, T_B^{(2)}, R_B\}$。

B 选择两个随机数 $b^{(1)} \in_R \mathbf{Z}_{p^{(1)}}^*$ 和 $b^{(2)} \in_R \mathbf{Z}_{p^{(2)}}^*$，计算 $T_B^{(1)} = b^{(1)}P^{(1)}$，$T_B^{(2)} = b^{(2)}P^{(2)}$，并将 $\{ID_B, T_B^{(1)}, T_B^{(2)}, R_B\}$ 发送给参与者 A。

3）收到 B 发来的消息后，A 计算 $K_A^{(1)} = s_AT_B^{(1)}$，$K_A^{(2)} = a^{(2)}T_B^{(2)}$。这里 $P_B^{(2)} = s_BP^{(2)} = R_B + H_1^{(2)}(ID_B, R_B)P_{\text{pub}}^{(2)}$。最后，$A$ 利用一个类似于 SHA-2 的单向函数计算会话密钥：

$$K_{AB} = H\{ID_A, ID_B, T_A^{(1)}, T_A^{(2)}, T_B^{(1)}, T_B^{(2)}, a^{(1)}T_B^{(1)}, a^{(2)}T_B^{(2)}, K_A^{(1)}, K_A^{(2)}\}$$

4）收到 A 发来的消息后，B 计算 $K_B^{(1)} = b^{(1)}P_A^{(1)}$，$K_B^{(2)} = s_BT_A^{(2)}$。这里 $P_A^{(1)} = s_AP^{(1)} = R_A + H_1^{(1)}(ID_A, R_a)P_{\text{pub}}^{(1)}$。最后，$B$ 利用一个类似于 SHA-2 的单向函数计算会话密钥：

$$K_{BA} = H\{ID_A, ID_B, T_A^{(1)}, T_A^{(2)}, T_B^{(1)}, T_B^{(2)}, b^{(1)}T_A^{(1)}, b^{(2)}T_A^{(2)}, K_B^{(1)}, K_B^{(2)}\}$$

3 安全性分析

本章重点讨论新协议的安全性。

定理 1 如果 CDH 问题是困难的，且 Hash 函数 H 是一个随机预言机，则新协议是安全的。

证明 显然，新协议是满足安全性的第一个条件的。这是因为，两个预言机（Oracle）都计算出了相同的会话密钥：$K_A^{(1)} = s_AT_B^{(1)} = s_Ab^{(1)}P^{(1)} = b^{(1)}P_A^{(1)} = K_B^{(1)}$，$K_A^{(2)} = s_BT_A^{(1)} = s_Ba^{(1)}P^{(1)} = a^{(1)}P_B^{(1)} = K_A^{(1)}$。因此会话密钥 K_{AB} 和 K_{BA} 也是相同的。

现在证明新协议也满足安全性定义中的第二个条件。反证地，假设敌手 E 将以一个不可忽略的概率 ε 猜对对 Test 查询的回复是真实的还是随机的，也就是说，敌手可以赢得这个游戏，除了敌手外，这里将展示如何构造一个模拟者 S 可以以一个不可忽略的概率 $\varepsilon(k)$ 解决 CDH 问题。也就是说，给定 $(aP, bP) \in G$，S 可以计算得到 $cP \in G$，使得 $c = ab \bmod p$。

假设 S 和 E 之间的游戏涉及 $n_{\text{kgc}}(k)$ 个独立的 KGC，每个 KGC 可以支持 $n_u(k)$ 个使用者，而每个使用者可能同时参与

$n_s(k)$ 个会话,这里 k 是一个安全参数。如前所述,本文提出的新协议是在独立 KGC 中的参与者之间的密钥协商,所以本协议中定义每个参与者 $i \in \{1,2,\cdots,n_u(k)\}$ 都归属于不同的 $KGC_k \in \{1,2,\cdots,n_{kgc}(k)\}$。对应地,定义 $\Pi^s_{i(k),j(l)}$ 为参与者 $i^{(k)}$ 和 $j^{(l)}$ 的第 s 次会话。S 和 E 将进行如下交互:

setup:S 向敌手 E 模拟系统的初始化过程并定义每个 KGC 的公开参数。S 随机选择 $k,l \in \{1,2,\cdots,n_{pub}(k)\}$,$k,l \in \{1,2,\cdots,n_u(k)\}$ 以及 $s \in \{1,2,\cdots,n_s(k)\}$,然后将 $\{F_p, E/F_p, G, P, P^{(k)}_{pub}, H_1^{(k)}\}$ 作为系统中 KGC_k 的公开参数。随后,S 计算参与者 U_i 的长期私钥 $s_i^{(k)}$。最后,S 形成一个元素为 $(ID_i^{(k)}, s_i^{(k)})$ 的列表 $L_{PrivateKeys}$,列表的规则如下:

1) 如果 $i = I$ 且 $l = k$,则将 $(ID_l^{(k)}, \perp)$ 置于列表中;

2) 否则,S 随机选择 $r_i^{(k)} \in \mathbf{Z}_p^*$ 并计算 $R_i^{(k)} = r_i^{(k)} P^{(k)}$, $h_i^{(k)} = H_i^{(k)}(ID_i^{(k)}, R_i^{(k)})$, $s_i^{(k)} = r_i^{(k)} + r_i^{(k)} x^{(k)}$,然后将 $(ID_i^{(k)}, s_i^{(k)})$ 放入列表中。

Corrupt$(ID_i^{(k)})$:S 遍历列表 $L_{PrivateKeys}$,如果 $ID_i^{(k)}$ 不在列表中,则计算私钥并将其补充到列表中。随后,S 验证 $s_i^{(k)}$ 是否等于 $\perp$,如果不相等,则 S 相应敌手 E,否则放弃这一游戏(事件 1)。

Send$(\Pi^s_{i(k),j(l)}, M_1, M_2)$:$S$ 为每个预言维持一个列表 L_{Send}:

1) 如果 $\Pi^t_{i(k),j(l)} \neq \Pi^s_{I(K),J(L)}$,$S$ 将按照协议流程对待 E。

2) 否则,S 将 $\{ID_J^{(L)}, T_J^{(K)} = bP, T_J^{(L)}, R_J^{(L)}\}$ 返回给 E 并将 $r_J^{(K)} = \perp$ 存入 L_{Send}。

Reveal$(\Pi^t_{i(k),j(l)})$:保存一份格式为 $\{\Pi^t_{i(k),j(l)}, ID_i^{(k)}, ID_j^{(l)}, X_{i(k)}^{(1)}, X_{i(k)}^{(2)}, Y_{j(l)}^{(1)}, Y_{j(l)}^{(2)}, SK^t_{i(k),j(l)}\}$ 的列表 L_{Reveal}。为了回应敌手 E 的请求,S 首先遍历 L_{Reveal},如果之前已经被请求过,S 将列表中的回复给敌手,否则按照如下方式回复:

1) 从 L_{Reveal} 中查找到预言 $\Pi^t_{i(k),j(l)}$ 的对应数组。

2) 如果 $\Pi^t_{i(k),j(l)}$ 没有被接受,则返回 $\perp$;如果 $\Pi^t_{i(k),j(l)} = \Pi^s_{I(K),J(L)}$,则 S 退出该游戏;如果 $\Pi^t_{i(k),j(l)} \neq \perp$,则返回 $SK^t_{i(k),j(l)}$(事件 2)。

3) 否则,S 遍历 L_H:

① 如果 $\{ID_i^{(k)}, ID_j^{(l)}, X_{i(k)}^{(1)}, X_{i(k)}^{(2)}, Y_{j(l)}^{(1)}, Y_{j(l)}^{(2)}\}$ 不在列表中,随机选择一个值 $SK^t_{i(k),j(l)}$ 返给 E 并将 $\{\Pi^t_{i(k),j(l)}, ID_i^{(k)}, ID_j^{(l)}, X_{i(k)}^{(1)}, X_{i(k)}^{(2)}, Y_{j(l)}^{(1)}, Y_{j(l)}^{(2)}, SK^t_{i(k),j(l)}\}$ 保存在列表 L_H 中。

② 否则(也就是说,$\{ID_i^{(k)}, ID_j^{(l)}, X_{i(k)}^{(1)}, X_{i(k)}^{(2)}, Y_{j(l)}^{(1)}, Y_{j(l)}^{(2)}\}$ 在列表中),执行如下步骤:

a) 如果 L_H 中存在 $\{\Pi^t_{i(k),j(l)}, ID_i^{(k)}, ID_j^{(l)}, X_{i(k)}^{(1)}, X_{i(k)}^{(2)}, Y_{j(l)}^{(1)}, Y_{j(l)}^{(2)}, Z_{1u}, Z_{2u}, K_{1u}, K_{2u}, h_u\}$,则 S 将 h_u 返给 E,并更新列表 L_{Reveal}。

b) 如果 L_H 中存在 $\{--, ID_i^{(k)}, ID_j^{(l)}, X_{i(k)}^{(1)}, X_{i(k)}^{(2)}, Y_{j(l)}^{(1)}, Y_{j(l)}^{(2)}, Z_{1u}, Z_{2u}, K_{1u}, K_{2u}, h_u\}$,则 S 随机选择一个值 $SK^t_{i(k),j(l)}$ 返给 E,并更新列表 L_{Reveal}。

c) 如果 L_H 中存在 $\{\perp, ID_i^{(k)}, ID_j^{(l)}, X_{i(k)}^{(k)}, X_{i(k)}^{(l)}, Y_{j(l)}^{(k)}, Y_{j(l)}^{(l)}, Z_{1u}, Z_{2u}, K_{1u}, K_{2u}, h_u\}$,则 S 验证 $Z_{1u} \in G^{(k)}$, $Z_{2u} \in G^{(l)}$, $e(X_{i(k)}^{(k)}, Y_{j(l)}^{(k)}) = e(Z_{1u}, P^{(k)})$, $e(X_{i(k)}^{(l)}, Y_{j(l)}^{(l)}) = e(Z_{2u}, P^{(l)})$, $K_{1u} \in G^{(k)}$, $K_{2u} \in G^{(l)}$, $e(P_i^{(k)}, Y_{j(l)}^{(k)}) = e(K_{1u}, P^{(k)})$, $e(P_j^{(l)}, Y_{j(k)}^{(l)}) = e(K_{2u}, P^{(l)})$。

(a) 如果上述验证顺利通过,则 S 将 h_u 返给 E,并用 $\{\Pi^t_{i(k),j(l)}, ID_i^{(k)}, ID_j^{(l)}, X_{i(k)}^{(1)}, X_{i(k)}^{(2)}, Y_{j(l)}^{(1)}, Y_{j(l)}^{(2)}, Z_{1u}, Z_{2u}, K_{1u}, K_{2u}, h_u\}$ 替换列表 L_H 中的 $\{\perp, ID_i^{(k)}, ID_j^{(l)}, X_{i(k)}^{(k)}, X_{i(k)}^{(l)}, Y_{j(l)}^{(k)}, Y_{j(l)}^{(l)}, Z_{1u}, Z_{2u}, K_{1u}, K_{2u}, h_u\}$。随后,$S$ 更新列表 L_{Reveal}。

(b) 否则,S 随机选择一个值 $SK^t_{i(k),j(l)}$ 返给 L_{Reveal},并用 $\{--, ID_i^{(k)}, ID_j^{(l)}, X_{i(k)}^{(1)}, X_{i(k)}^{(2)}, Y_{j(l)}^{(1)}, Y_{j(l)}^{(2)}, Z_{1u}, Z_{2u}, K_{1u}, K_{2u}, h_u\}$ 替换列表 L_H 中的 $\{\perp, ID_i^{(k)}, ID_j^{(l)}, X_{i(k)}^{(k)}, X_{i(k)}^{(l)}, Y_{j(l)}^{(k)}, Y_{j(l)}^{(l)}, Z_{1u}, Z_{2u}, K_{1u}, K_{2u}, h_u\}$。

$H(ID_i^{(k)}, ID_j^{(l)}, X_{i(k)}^{(1)}, X_{i(k)}^{(2)}, Y_{j(l)}^{(1)}, Y_{j(l)}^{(2)}, Z_{1u}, Z_{2u}, K_{1u}, K_{2u})$:$S$ 保存一份格式为 $\{\perp, ID_i^{(k)}, ID_j^{(l)}, X_{i(k)}^{(k)}, X_{i(k)}^{(l)}, Y_{j(l)}^{(k)}, Y_{j(l)}^{(l)}, Z_{1u}, Z_{2u}, K_{1u}, K_{2u}, h_u\}$ 的列表 L_{Reveal}。为了回应敌手 E 的请求,S 首先遍历 L_H,如果之前已经被请求过,S 将列表中的回复给敌手,否则按照如下方式回复:

1) 如果 $\{ID_i^{(k)}, ID_j^{(l)}, X_{i(k)}^{(1)}, X_{i(k)}^{(2)}, Y_{j(l)}^{(1)}, Y_{j(l)}^{(2)}\}$ 不在列表中,则 S 随机选择一个值 h_u 返给 E,并将 $\{\perp, ID_i^{(k)}, ID_j^{(l)}, X_{i(k)}^{(1)}, X_{i(k)}^{(2)}, Y_{j(l)}^{(1)}, Y_{j(l)}^{(2)}, Z_{1u}, Z_{2u}, K_{1u}, K_{2u}, h_u\}$ 保存在列表 L_H 中。

2) 否则,S 验证 $Z_{1u} \in G^{(k)}$, $Z_{2u} \in G^{(l)}$, $e(X_{i(k)}^{(k)}, Y_{j(l)}^{(k)}) = e(Z_{1u}, P^{(k)})$, $e(X_{i(k)}^{(l)}, Y_{j(l)}^{(l)}) = e(Z_{2u}, P^{(l)})$, $K_{1u} \in G^{(k)}$, $K_{2u} \in G^{(l)}$, $e(P_i^{(k)}, Y_{j(l)}^{(k)}) = e(K_{1u}, P^{(k)})$, $e(P_j^{(l)}, Y_{j(k)}^{(l)}) = e(K_{2u}, P^{(l)})$。

① 如果上述验证顺利通过,则 S 将 $SK^t_{i(k),j(l)}$ 返给 E,并将 $\{\Pi^t_{i(k),j(l)}, ID_i^{(k)}, ID_j^{(l)}, X_{i(k)}^{(k)}, X_{i(k)}^{(l)}, Y_{j(l)}^{(k)}, Y_{j(l)}^{(l)}, Z_{1u}, Z_{2u}, K_{1u}, K_{2u}, h_u = SK^t_{i(k),j(l)}\}$ 保存在列表 L_H 中。

② 否则,S 随机选择一个值 h_u 返给 E,并将用 $\{--, ID_i^{(k)}, ID_j^{(l)}, X_{i(k)}^{(1)}, X_{i(k)}^{(2)}, Y_{j(l)}^{(1)}, Y_{j(l)}^{(2)}, Z_{1u}, Z_{2u}, K_{1u}, K_{2u}, h_u\}$ 保存在列表 L_H 中。

Test$(\Pi^t_{i(k),j(l)})$:如果 $\Pi^t_{i(k),j(l)} \neq \Pi^s_{I(K),J(L)}$,放弃该游戏。否则,$S$ 随机选择一个值 sk 返给 E(事件 3)。

Output:敌手 E 输出其的猜测 $b' \in \{0,1\}$。

现在,模拟器 S 可以按照如下步骤解决 CDH 问题:

预言 $\Pi^s_{I(K),J(L)}$ 分享的 Test 询问的秘密值是:

$$(K^{(K)})^s_{I(K)J(L)} = s_I^{(K)} T_J^{(K)} = (a + x^{(K)})bP = abP + bx^{(K)}P = abP + x^{(K)} T_J^{(K)}$$

显然,S 可以通过从游戏初始化阶段获得 KGC_K 的私钥 $x^{(K)}$,然后利用查询 L_{Send} 得到的 $T_J^{(K)}$ 计算出密钥的 $x^{(K)} T_J^{(K)}$ 部分。然而,S 可以从 L_H 中随机选择一个 K_u 并计算 $Q = K_u - x^{(K)}(M_1)^s_{I(K)J(L)}$。因此,如果下述条件都满足,则有 $Q = abP$:

1) 事件 1,2,3 都没有发生;2) $(K^{(k)})^s_{I(K)J(L)}$ 不在 L_H 中;3) $K_u = (K^{(k)})^s_{I(K)J(L)}$。

这时,$\Pr[Q = abP] = \Pr[\text{事件}\bar{1}, \text{事件}\bar{2}, \text{事件}\bar{3}] \cdot \Pr[(K^{(k)})^s_{I(K)J(L)} \in L_H] \cdot \Pr[K_u = (K^{(k)})^s_{I(K)J(L)}] = \dfrac{1}{n_u(K) n_s(K) n_{pub}(K)} \cdot \Pr[(K^{(k)})^s_{I(K)J(L)} \in L_H] \cdot \dfrac{1}{n_H(K)}$。

这里,$n_H(K)$ 是列表 L_H 的元素个数。为了计算上述概率,应该算出 $\Pr[K_u = (K^{(k)})^s_{I(K)J(L)}]$。假设敌手 E 成功赢得游戏,则:

$$\begin{aligned}\Pr[A] = {} & \Pr[A \mid (K^{(K)})^s_{I(K)J(L)} \notin L_H] \\ & \Pr[(K^{(K)})^s_{I(K)J(L)} \notin L_H] + \\ & \Pr[A \mid (K^{(K)})^s_{I(K)J(L)} \in L_H] \\ & \Pr[(K^{(K)})^s_{I(K)J(L)} \in L_H] = \\ & \Pr[A \mid (K^{(K)})^s_{I(K)J(L)} \notin L_H]\end{aligned}$$

$$(1-\Pr[(K^{(K)})^{s}_{I(K)J(L)} \in L_H]) + \Pr[A \mid (K^{(K)})^{s}_{I(K)J(L)} \in L_H]$$
$$\Pr[(K^{(K)})^{s}_{I(K)J(L)} \in L_H] = \Pr[A \mid (K^{(K)})^{s}_{I(K)J(L)} \notin L_H] + \Pr[(K^{(K)})^{s}_{I(K)J(L)} \in L_H] - \Pr[A \mid (K^{(K)})^{s}_{I(K)J(L)} \notin L_H]$$
$$\Pr[(K^{(K)})^{s}_{I(K)J(L)} \in L_H] \leqslant \frac{1}{2} + \frac{1}{2}\Pr[(K^{(K)})^{s}_{I(K)J(L)} \in L_H]$$

所以,$\Pr[A] \leqslant \frac{1}{2} + \frac{1}{2}\Pr[(K^{(K)})^{s}_{I(K)J(L)} \in L_H]$。

另一方面,

$$\Pr[A] \geqslant \Pr[A \mid (K^{(K)})^{s}_{I(K)J(L)} \notin L_H]\Pr[(K^{(K)})^{s}_{I(K)J(L)} \notin L_H] = \Pr[A \mid (K^{(K)})^{s}_{I(K)J(L)} \notin L_H](1-\Pr[(K^{(K)})^{s}_{I(K)J(L)} \in L_H]) = \frac{1}{2} - \frac{1}{2}\Pr[(K^{(K)})^{s}_{I(K)J(L)} \in L_H]$$

因此,有$|2\Pr[A]-1| \leqslant \Pr[(K^{(K)})^{s}_{I(K)J(L)} \in L_H]$。

进一步地,由于$\varepsilon(k) = Adv^{E}(k) = |2\Pr[A]-1|$,从而$\Pr[(K^{(K)})^{s}_{I(K)J(L)} \in L_H] \geqslant \varepsilon(k)$。

综上分析,模拟器 S 解决 CDH 问题的概率

$$\Pr[abP = K_u - x^{(K)}(M_1)^{s}_{I(K)J(L)}] = \frac{1}{n_u(k)n_s(k)n_{pub}(k)n_H(k)}\Pr[(K^{(K)})^{s}_{I(K)J(L)} \in L_H] \geqslant \varepsilon(k)\frac{1}{n_u(k)n_s(k)n_{pub}(k)n_H(k)}。$$

由于 $\varepsilon(k)$ 是一个不可忽略的概率,因此模拟器解决 CDH 问题的概率也是不可忽略的。这明显与本文前面的假设矛盾。因此,定理得证。

4 结语

本文提出了一种新的基于身份的认证密钥协商协议。新协议实现了两个具有独立参数的 KGC 下的参与者之间的安全密钥协商。随后,本文在随机预言模型下对新协议的安全性进行了严格的形式化证明。由于方案采用了椭圆曲线机制,因此可广泛地用于能耗要求高的轻量级设备中,而不同 KGC 下实现密钥协商的性质可使处于不同组织的参与者协商会话密钥进行安全会话。

参考文献:

[1] ISO/IEC 9594-8: (the 4th ed). Information technology Open Systems Interconnection-The Directory: Public-key and attribute certificate frameworks[S]. Geneva, Switzerland: ISO, 2001.

[2] SHAMIR A. Identity-based cryptosystems and signature schemes [C]// Processing of CRYPTO 1984, LNCS 196. Berlin: Springer-Verlag, 1984: 47 - 53.

[3] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairings[C]// Advances in Cryptology-Crypto 2001, LNCS 2139. Berlin: Springer, 2001: 213 - 229.

[4] YI X. Efficient ID-based key agreement from Weil pairing[J]. IEE Electronics Letters, 2003, 39(2): 206 - 208.

[5] 刘雪艳, 张强, 王彩芬. Ad Hoc 网络中基于身份的簇密钥协商机制[J]. 计算机应用, 2012, 32(8): 2258 - 2327.

[6] 李志敏, 徐馨, 李存华. 一个基于身份的非交互可否认源认证协议[J]. 计算机应用, 2012, 32(2): 465 - 471.

[7] 舒剑. 高效的强安全的基于身份认证密钥协商协议[J]. 计算机应用, 2012, 32(1): 95 - 98.

[8] LEE H, KIM D, KIM S, *et al*. Identity-based key agreement protocols in a multiple PKG environment[C]// ICCSA 2005: International Conference on Computational Science and its Applications, LNCS 3483. Berlin: Springer-Verlag, 2005: 877 - 886.

[9] KIM S, LEE H, OH H. Enhanced ID-based authenticated key agreement protocols for a multiple independent PKG environment [C]// Proceedings of the ICICS'05, LNCS 3783. Berlin: Springer, 2005: 323 - 336.

[10] BARRETO P, KIM H, LYNN B, *et al*. Efficient algorithms for pairing-based cryptosystems[C]// Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer, 2002: 354 - 368.

[11] BARRETO P S L M, LYNN B, SCOTT M. On the selection of pairing-friendly groups[C]// SAC 2003: Selected Areas in Cryptography, LNCS 3006. Berlin: Springer, 2003: 17 - 25.

[12] 唐宏斌, 刘心松. 鲁棒且高效的远程认证及密钥协商协议[J]. 计算机应用, 2012, 32(5): 1381 - 1384.

[13] 王明辉, 王建东. 对 TAKASIP 协议的分析和改进[J]. 计算机应用, 2012, 32(2): 468 - 471.

[14] CAO X F, KOU W D, FAN K. An identity-based authenticated key agreement protocol without bilinear pairing[J]. Journal of Electronics and Information Technology, 2009, 31(5): 1241 - 1244.

[15] BLAKE-WILSON S, JOHNSON D, MENEZES A. Key agreement protocols and their security analysis[C]// Processings of the 6th IMA International Conference on Cryptography and Coding, LNCS 1355. Berlin: Springer-Verlag, 1997: 30 - 45.

(上接第 1323 页)

[4] LIANG J J, WU D. A new smooth support vector machine[C]// AICI'10: Proceedings of the 2010 International Conference on Artificial Intelligence and Computational Intelligence: Part I. Berlin: Springer-Verlag, 2010: 266 - 272.

[5] 朱燕飞, 伍建平, 李琦, 等. MISO 系统的混合核函数 LS-SVM 建模[J]. 控制与决策 2005, 20(4): 417 - 425.

[6] 谭泗桥, 袁哲明, 柏连阳, 等. 基于局部核函数与全局核函数支持向量回归优化小样本 QSAR 建模[J]. 分子科学学报 2009, 25(3): 158 - 162.

[7] 薛欣, 贺国平. 基于多个混合核函数的 SVM 决策树算法设计[J]. 计算机工程与应用, 2007, 43(8): 142 - 144.

[8] LAM K C, YU C Y. A multiple kernel learning-based decision support model for contractor pre-qualification [J]. Automation in Construction, 2011, 20(5): 531 - 536.

[9] DORIGO M, GAMBARDELLA L M. Ant colony system: a cooperative learning approach to the traveling salesman problem[J]. IEEE Transactions on Evolutionary Computation, 1997, 1(1): 53 - 66.

[10] DORIGO M, STUTZLE T. Ant colony optimization [M]. Cambridge: MIT Press, 2004.

[11] HUANG M. Improved ant colony algorithm in the distribution of reactive power compensation device and optimization [J]. Procedia Engineering, 2010, 7: 256 - 264.

[12] 张恒喜, 郭基联, 朱家元, 等. 小样本多元数据分析方法及应用[M]. 西安: 西北工业大学出版社, 2002.