



(12) 发明专利申请

(10) 申请公布号 CN 104868993 A

(43) 申请公布日 2015. 08. 26

(21) 申请号 201510247662. 3

(22) 申请日 2015. 05. 15

(71) 申请人 河海大学

地址 211100 江苏省南京市江宁开发区佛城西路 8 号

(72) 发明人 陆阳 张全领 李继国 王刚

(74) 专利代理机构 南京经纬专利商标代理有限公司 32200

代理人 朱小兵

(51) Int. Cl.

H04L 9/08(2006. 01)

H04L 29/06(2006. 01)

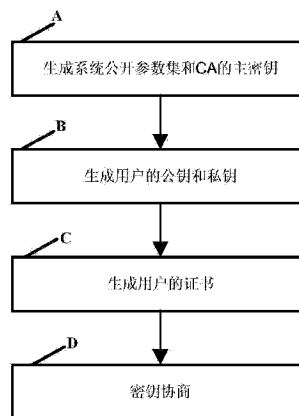
权利要求书2页 说明书6页 附图3页

(54) 发明名称

一种基于证书的两方认证密钥协商方法及系统

(57) 摘要

本发明公开了一种基于证书的两方认证密钥协商方法,包括以下步骤:生成证书中心 CA 的主密钥和系统公开参数集;根据所述系统公开参数集和用户的身份信息生成用户的公钥和私钥,所述用户包括会话发起方和会话响应方;根据所述系统公开参数集、证书中心 CA 的主密钥、用户的身份信息以及用户的公钥,生成用户的证书;根据所述系统公开参数集,会话发起方和会话响应方的身份信息、公钥、私钥、证书,生成两方共享的会话密钥。本发明还公开了一种基于证书的两方认证密钥协商系统,本发明所述技术方案不仅简化了用户证书的管理过程,提供了高效的隐认证机制,而且不存在密钥分发和密钥托管的问题,适用于开放网络环境。



1. 一种基于证书的两方认证密钥协商方法,其特征在于,包括以下步骤:

步骤 A、生成证书中心 CA 的主密钥和系统公开参数集;

步骤 B、根据所述系统公开参数集和用户的身份信息生成用户的公钥和私钥,所述用户包括会话发起方和会话响应方;

步骤 C、根据所述系统公开参数集、证书中心 CA 的主密钥、用户的身份信息以及用户的公钥,生成用户的证书;

步骤 D、根据所述系统公开参数集,会话发起方和会话响应方的身份信息、公钥、私钥、证书,生成两方共享的会话密钥。

2. 根据权利要求 1 所述的一种基于证书的两方认证密钥协商方法,其特征在于,所述步骤 A 具体过程如下:

步骤 101、证书中心 CA 根据设定的安全参数 $k \in \mathbb{Z}^+$, 选择一个 k 比特的大素数 q , 并生成一个 q 阶加法循环群 G_1 、一个 q 阶乘法循环群 G_2 以及定义在群 G_1 和群 G_2 上的双线性对 $e: G_1 \times G_1 \rightarrow G_2$; 其中 \mathbb{Z}^+ 是正整数集合, 双线性对 $e: G_1 \times G_1 \rightarrow G_2$ 是群 G_1 与自身的笛卡尔积 $G_1 \times G_1$ 到群 G_2 的映射, 即双线性对 $e: G_1 \times G_1 \rightarrow G_2$ 是指函数 $z = e(P_1, P_2)$, 其中 $P_1, P_2 \in G_1$ 为自变量, $z \in G_2$ 为因变量;

步骤 102、从加法循环群 G_1 中选择一个生成元 P 并在集合 \mathbb{Z}_q^* 中随机选择一个整数 s , 计算 $P_{pub} = sP$, 其中, 集合 $\mathbb{Z}_q^* = \{1, 2, \dots, q-1\}$;

步骤 103、定义三个哈希函数 $H_1: \{0, 1\}^* \times G_1 \rightarrow G_1$ 、 $H_2: \{0, 1\}^* \times \{0, 1\}^* \times G_1 \times \mathbb{Z}_q^* \rightarrow \mathbb{Z}_q^*$ 、 $H_3: \{0, 1\}^* \times \{0, 1\}^* \times (G_1)^6 \times G_2 \times (G_1)^3 \rightarrow \{0, 1\}^k$; 其中, H_1 是笛卡尔积 $\{0, 1\}^* \times G_1$ 到 G_1 的密码学哈希函数, H_2 是笛卡尔积 $\{0, 1\}^* \times \{0, 1\}^* \times G_1 \times \mathbb{Z}_q^*$ 到 \mathbb{Z}_q^* 的密码学哈希函数, H_3 是笛卡尔积 $\{0, 1\}^* \times \{0, 1\}^* \times (G_1)^6 \times G_2 \times (G_1)^3$ 到 $\{0, 1\}^k$ 的密码学哈希函数, $\{0, 1\}^*$ 表示长度不确定的二进制串的集合, $\{0, 1\}^k$ 表示长度为 k 比特的二进制串的集合, $(G_1)^3$ 和 $(G_1)^6$ 分别表示 3 个群 G_1 的笛卡尔积和 6 个群 G_1 的笛卡尔积, $\{0, 1\}^* \times G_1$ 表示 $\{0, 1\}^*$ 和群 G_1 的笛卡尔积, $\{0, 1\}^* \times \{0, 1\}^* \times G_1 \times \mathbb{Z}_q^*$ 表示 $\{0, 1\}^*$ 、 $\{0, 1\}^*$ 、群 G_1 和集合 \mathbb{Z}_q^* 的笛卡尔积, $\{0, 1\}^* \times \{0, 1\}^* \times (G_1)^6 \times G_2 \times (G_1)^3$ 表示 $\{0, 1\}^*$ 、 $\{0, 1\}^*$ 、 $(G_1)^6$ 、群 G_2 和 $(G_1)^3$ 的笛卡尔积;

步骤 104、根据步骤 101 至步骤 103, 生成证书中心 CA 秘密保存的主密钥为 $msk = s$ 和系统公开参数集 $params = \{k, q, G_1, G_2, e, P, P_{pub}, H_1, H_2, H_3\}$ 。

3. 根据权利要求 2 所述的一种基于证书的两方认证密钥协商方法,其特征在于,所述步骤 B 具体过程如下:

身份为 ID_U 的用户 U 在集合 \mathbb{Z}_q^* 中随机选择一个整数 x_U 作为自己的私钥, $SK_U = x_U$; 然后计算并获得自己的公钥 $PK_U = x_U P$ 。

4. 根据权利要求 3 所述的一种基于证书的两方认证密钥协商方法,其特征在于,所述步骤 C 具体过程如下:

身份为 ID_U 的用户 U 把自己的身份信息 ID_U 和公钥 PK_U 提交给证书中心 CA, 证书中心 CA 计算 $Q_U = H_1(ID_U, PK_U)$, 生成用户 U 的证书 $Cert_U = msk Q_U = s Q_U$, 并把证书 $Cert_U$ 发送给用户 U 。

5. 根据权利要求 4 所述的一种基于证书的两方认证密钥协商方法,其特征在于,所述

步骤 D 的具体过程如下：

步骤 401、会话发起方 A 在集合 Z_q^* 中随机选择一个整数 a, 计算 $R_A = aP$ 和 $W_A = H_2(ID_A, ID_B, Cert_A, SK_A)P$, 其中, ID_A 是会话发起方 A 的身份信息, SK_A 是会话发起方 A 的私钥, $Cert_A$ 是会话发起方 A 证书, ID_B 是会话响应方 B 的身份信息; 然后将 (ID_A, R_A, W_A) 发送给会话响应方 B;

步骤 402、会话响应方 B 收到 (ID_A, R_A, W_A) 后, 会话响应方 B 在集合 Z_q^* 中随机选择一个整数 b, 计算 $R_B = bP$ 和 $W_B = H_2(ID_A, ID_B, Cert_B, SK_B)P$, 其中, SK_B 是会话响应方 B 的私钥, $Cert_B$ 是会话响应方 B 的证书; 然后将 (ID_B, R_B, W_B) 发送给会话发起方 A;

步骤 403、会话发起方 A 收到 (ID_B, R_B, W_B) 后, 会话发起方 A 依次计算

$K_{A_1} = e(R_B + Q_B, aP_{pub} + Cert_A)$, $K_{A_2} = SK_A PK_B + H_2(ID_A, ID_B, Cert_A, SK_A)W_B$, $K_{A_3} = aPK_B + SK_A R_B$ 和 $K_{A_4} = aR_B$, 其中, $Q_B = H_1(ID_B, PK_B)$; 然后计算并获得会话密钥 $K_{AB} = H_3(ID_A, ID_B, PK_A, PK_B, R_A, R_B, W_A, W_B, K_{A_1}, K_{A_2}, K_{A_3}, K_{A_4})$, 其中, PK_A 是会话发起方 A 的公钥, PK_B 是会话响应方 B 的公钥;

步骤 404、会话响应方 B 依次计算 $K_{B_1} = e(R_A + Q_A, bP_{pub} + Cert_B)$, $K_{B_2} = SK_B PK_A + H_2(ID_A, ID_B, Cert_B, SK_B)W_A$, $K_{B_3} = bPK_A + SK_B R_A$ 和 $K_{B_4} = bR_A$, 其中, $Q_A = H_1(ID_A, PK_A)$; 然后计算并获得会话密钥 $K_{BA} = H_3(ID_A, ID_B, PK_A, PK_B, R_A, R_B, W_A, W_B, K_{B_1}, K_{B_2}, K_{B_3}, K_{B_4})$ 。

6. 一种基于证书的两方认证密钥协商系统, 其特征在于, 包括:

系统参数生成模块, 用于根据输入的安全参数生成证书中心 CA 的主密钥以及密码系统的公开参数集;

用户密钥生成模块, 用于根据系统参数生成模块生成的公开参数集, 以及用户的身份信息, 生成用户的公钥和私钥, 所述用户包括会话发起方和会话响应方;

证书生成模块, 用于根据系统参数生成模块生成的公开参数集和证书中心 CA 的主密钥、用户的身份信息和公钥, 生成用户的证书;

密钥协商模块, 用于根据系统参数生成模块生成的公开参数集、会话发起方和响应方的身份信息、用户密钥生成模块生成的会话发起方和响应方的公钥和私钥以及证书生成模块生成的会话发起方和响应方的证书, 生成会话两方共享的会话密钥。

7. 根据权利要求 6 所述的一种基于证书的两方认证密钥协商系统, 其特征在于, 所述密钥协商模块包括会话发起方单元和会话响应方单元; 其中,

所述会话发起方单元用于会话发起方计算会话密钥;

所述会话响应方单元用于会话响应方计算会话密钥。

一种基于证书的两方认证密钥协商方法及系统

技术领域

[0001] 本发明涉及信息安全中的密钥协商技术领域,特别是一种基于证书的两方认证密钥协商方法及系统。

背景技术

[0002] 密钥协商作为一个重要的密码学原语,它可以保证两个或多个用户在公开网络环境中通过交互信息建立一个共享的会话密钥,参与通信的用户通过共享的会话密钥来加解密通信数据从而保证网络通信的安全。认证密钥协商是一种带有认证功能的密钥协商,它能够对参与密钥协商双方的身份进行认证,从而能有效抵抗中间人攻击。认证密钥协商为开放网络环境下用户间的安全通信提供了认证性、机密性和完整性保护,进而能被用于构造更复杂的高层协议。国内外学者对认证密钥协商方法进行了深入的探讨和研究。但已有方法大多是在传统公钥密码体制下或基于身份密码体制下所提出的,因此这些方法要么存在复杂的证书管理问题,要么存在密钥分发和密钥托管的问题。而近期所提出的无证书认证密钥协商方法尽管有效解决了复杂的证书管理和密钥托管问题,但仍存在密钥分发的问题。因此,现有的认证密钥协商方法在开放网络环境下的应用将会受到限制。

[0003] 基于证书密码体制是 Gentry 在 2003 年所提出的一种新型公钥密码体制,该体制有机结合了基于身份密码体制和传统公钥密码体制的优点,并有效克服了这两种密码体制中存在的缺陷。基于证书密码体制的一个最大的特点是提供了一种高效的隐证书机制,即用户证书仅发送给证书持有人,并与其私钥相结合产生最终的解密密钥或签名密钥。基于该特点,基于证书密码体制不仅消除了证书状态的第三方查询问题,简化了传统公钥密码体制中复杂的证书管理过程,而且克服了基于身份密码体制中固有的密钥分发问题和密钥托管问题。因此,基于证书密码体制是一个性能优良,便于开放网络环境中应用的新型公钥密码体制。

发明内容

[0004] 本发明所要解决的技术问题是克服现有技术的不足而提供一种基于证书的两方认证密钥协商方法及系统,本发明将基于证书密码体制和认证密钥协商相结合,不仅简化了证书的管理过程,而且不存在密钥分发和密钥托管的问题,便于在开放网络环境中应用。

[0005] 本发明为解决上述技术问题采用以下技术方案:

[0006] 根据本发明提出的一种基于证书的两方认证密钥协商方法,包括以下步骤:

[0007] 步骤 A、生成证书中心 CA 的主密钥和系统公开参数集;

[0008] 步骤 B、根据所述系统公开参数集和用户的身份信息生成用户的公钥和私钥,所述用户包括会话发起方和会话响应方;

[0009] 步骤 C、根据所述系统公开参数集、证书中心 CA 的主密钥、用户的身份信息以及用户的公钥,生成用户的证书;

[0010] 步骤 D、根据所述系统公开参数集,会话发起方和会话响应方的身份信息、公钥、私

钥、证书,生成两方共享的会话密钥。

[0011] 作为本发明所述的一种基于证书的两方认证密钥协商方法进一步优化方案,所述步骤 A 具体过程如下:

[0012] 步骤 101、证书中心 CA 根据设定的安全参数 $k \in \mathbb{Z}^+$, 选择一个 k 比特的大素数 q , 并生成一个 q 阶加法循环群 G_1 、一个 q 阶乘法循环群 G_2 以及定义在群 G_1 和群 G_2 上的双线性对 $e: G_1 \times G_1 \rightarrow G_2$; 其中 \mathbb{Z}^+ 是正整数集合, 双线性对 $e: G_1 \times G_1 \rightarrow G_2$ 是群 G_1 与自身的笛卡尔积 $G_1 \times G_1$ 到群 G_2 的映射, 即双线性对 $e: G_1 \times G_1 \rightarrow G_2$ 是指函数 $z = e(P_1, P_2)$, 其中 $P_1, P_2 \in G_1$ 为自变量, $z \in G_2$ 为因变量;

[0013] 步骤 102、从加法循环群 G_1 中选择一个生成元 P 并在集合 Z_q^* 中随机选择一个整数 s , 计算 $P_{pub} = sP$, 其中, 集合 $Z_q^* = \{1, 2, \dots, q-1\}$;

[0014] 步骤 103、定义三个哈希函数 $H_1: \{0, 1\}^* \times G_1 \rightarrow G_1$ 、 $H_2: \{0, 1\}^* \times \{0, 1\}^* \times G_1 \times Z_q^* \rightarrow Z_q^*$ 、 $H_3: \{0, 1\}^* \times \{0, 1\}^* \times (G_1)^6 \times G_2 \times (G_1)^3 \rightarrow \{0, 1\}^k$; 其中, H_1 是笛卡尔积 $\{0, 1\}^* \times G_1$ 到 G_1 的密码学哈希函数, H_2 是笛卡尔积 $\{0, 1\}^* \times \{0, 1\}^* \times G_1 \times Z_q^*$ 到 Z_q^* 的密码学哈希函数, H_3 是笛卡尔积 $\{0, 1\}^* \times \{0, 1\}^* \times (G_1)^6 \times G_2 \times (G_1)^3$ 到 $\{0, 1\}^k$ 的密码学哈希函数, $\{0, 1\}^*$ 表示长度不确定的二进制串的集合, $\{0, 1\}^k$ 表示长度为 k 比特的二进制串的集合, $(G_1)^3$ 和 $(G_1)^6$ 分别表示 3 个群 G_1 的笛卡尔积和 6 个群 G_1 的笛卡尔积, $\{0, 1\}^* \times G_1$ 表示 $\{0, 1\}^*$ 和群 G_1 的笛卡尔积, $\{0, 1\}^* \times \{0, 1\}^* \times G_1 \times Z_q^*$ 表示 $\{0, 1\}^*$ 、 $\{0, 1\}^*$ 、群 G_1 和集合 Z_q^* 的笛卡尔积, $\{0, 1\}^* \times \{0, 1\}^* \times (G_1)^6 \times G_2 \times (G_1)^3$ 表示 $\{0, 1\}^*$ 、 $\{0, 1\}^*$ 、 $(G_1)^6$ 、群 G_2 和 $(G_1)^3$ 的笛卡尔积;

[0015] 步骤 104、根据步骤 101 至步骤 103, 生成证书中心 CA 秘密保存的主密钥为 $msk = s$ 和系统公开参数集 $params = \{k, q, G_1, G_2, e, P, P_{pub}, H_1, H_2, H_3\}$ 。

[0016] 作为本发明所述的一种基于证书的两方认证密钥协商方法进一步优化方案,所述步骤 B 具体过程如下:

[0017] 身份为 ID_U 的用户 U 在集合 Z_q^* 中随机选择一个整数 x_U 作为自己的私钥, $SK_U = x_U$; 然后计算并获得自己的公钥 $PK_U = x_U P$ 。

[0018] 作为本发明所述的一种基于证书的两方认证密钥协商方法进一步优化方案,所述步骤 C 具体过程如下:

[0019] 身份为 ID_U 的用户 U 把自己的身份信息 ID_U 和公钥 PK_U 提交给证书中心 CA, 证书中心 CA 计算 $Q_U = H_1(ID_U, PK_U)$, 生成用户 U 的证书 $Cert_U = msk Q_U = s Q_U$, 并把证书 $Cert_U$ 发送给用户 U 。

[0020] 作为本发明所述的一种基于证书的两方认证密钥协商方法进一步优化方案,所述步骤 D 的具体过程如下:

[0021] 步骤 401、会话发起方 A 在集合 Z_q^* 中随机选择一个整数 a , 计算 $R_A = aP$ 和 $W_A = H_2(ID_A, ID_B, Cert_A, SK_A)P$, 其中, ID_A 是会话发起方 A 的身份信息, SK_A 是会话发起方 A 的私钥, $Cert_A$ 是会话发起方 A 证书, ID_B 是会话响应方 B 的身份信息; 然后将 (ID_A, R_A, W_A) 发送给会话响应方 B ;

[0022] 步骤 402、会话响应方 B 收到 (ID_A, R_A, W_A) 后, 会话响应方 B 在集合 Z_q^* 中随机选择一个整数 b , 计算 $R_B = bP$ 和 $W_B = H_2(ID_A, ID_B, Cert_B, SK_B)P$, 其中, SK_B 是会话响应方 B 的私钥, $Cert_B$ 是会话响应方 B 的证书; 然后将 (ID_B, R_B, W_B) 发送给会话发起方 A;

[0023] 步骤 403、会话发起方 A 收到 (ID_B, R_B, W_B) 后, 会话发起方 A 依次计算

$K_{A_1} = e(R_B + Q_B, aP_{pub} + Cert_A)$, $K_{A_2} = SK_A PK_B + H_2(ID_A, ID_B, Cert_A, SK_A)W_B$, $K_{A_3} = aPK_B + SK_A R_B$ 和 $K_{A_4} = aR_B$, 其中, $Q_B = H_1(ID_B, PK_B)$; 然后计算并获得会话密钥 $K_{AB} = H_3(ID_A, ID_B, PK_A, PK_B, R_A, R_B, W_A, W_B, K_{A_1}, K_{A_2}, K_{A_3}, K_{A_4})$, 其中, PK_A 是会话发起方 A 的公钥, PK_B 是会话响应方 B 的公钥;

[0024] 步骤 404、会话响应方 B 依次计算 $K_{B_1} = e(R_A + Q_A, bP_{pub} + Cert_B)$, $K_{B_2} = SK_B PK_A + H_2(ID_A, ID_B, Cert_B, SK_B)W_A$, $K_{B_3} = bPK_A + SK_B R_A$ 和 $K_{B_4} = bR_A$, 其中, $Q_A = H_1(ID_A, PK_A)$; 然后计算并获得会话密钥 $K_{BA} = H_3(ID_A, ID_B, PK_A, PK_B, R_A, R_B, W_A, W_B, K_{B_1}, K_{B_2}, K_{B_3}, K_{B_4})$ 。

[0025] 一种基于证书的两方认证密钥协商系统, 包括:

[0026] 系统参数生成模块, 用于根据输入的安全参数生成证书中心 CA 的主密钥以及密码系统的公开参数集;

[0027] 用户密钥生成模块, 用于根据系统参数生成模块生成的公开参数集, 以及用户的身份信息, 生成用户的公钥和私钥, 所述用户包括会话发起方和会话响应方;

[0028] 证书生成模块, 用于根据系统参数生成模块生成的公开参数集和证书中心 CA 的主密钥、用户的身份信息和公钥, 生成用户的证书;

[0029] 密钥协商模块, 用于根据系统参数生成模块生成的公开参数集、会话发起方和响应方的身份信息、用户密钥生成模块生成的会话发起方和响应方的公钥和私钥以及证书生成模块生成的会话发起方和响应方的证书, 生成会话两方共享的会话密钥。

[0030] 作为本发明所述的一种基于证书的两方认证密钥协商系统进一步优化方案, 所述密钥协商模块包括会话发起方单元和会话响应方单元; 其中,

[0031] 所述会话发起方单元用于会话发起方计算会话密钥;

[0032] 所述会话响应方单元用于会话响应方计算会话密钥。

[0033] 本发明采用以上技术方案与现有技术相比, 具有以下技术效果:

[0034] (1) 本发明方法将基于证书密码体制和认证密钥协商相结合, 提供了高效的隐证书机制, 有效克服了已有认证密钥协商方法中存在的问题, 是一种非常适合于开放网络环境中应用的新型认证密钥协商方法;

[0035] (2) 由于用户仅在获得证书的情况下才能进行密钥协商, 因此会话发起者也就无须在发送会话消息前获取响应者的最新证书状态信息, 因此本发明不仅消除了基于传统 PKI 证书的认证密钥协商方法中对证书状态的第三方询问问题, 同时也简化了证书的撤销问题;

[0036] (3) 由于 CA 无法获知用户的私钥, 所以该方法解决了基于身份认证密钥协商方法中固有的密钥托管问题;

[0037] (4) 由于证书只是为了绑定用户公钥与用户身份之间的对应关系,可以公开地发送给用户,所以该方法也有效克服了基于身份认证密钥协商方法和无证书认证密钥协商方法中存在的密钥分发问题。

附图说明

[0038] 图 1 是本发明所述的一种基于证书的两方认证密钥协商方法的流程图。

[0039] 图 2 是依照本发明方法的基于证书的两方认证密钥协商系统执行的操作流程图。

[0040] 图 3 是本发明所述的基于证书的两方认证密钥协商系统的示意图。

具体实施方式

[0041] 下面结合附图对本发明的技术方案做进一步的详细说明：

[0042] 本发明所述基于证书的两方认证密钥协商方法可基于双线性对来实现,下面首先简要介绍双线性对的基本定义和它满足的性质。

[0043] 设 G_1 是一个阶为 q 的加法循环群, G_2 是一个阶为 q 的乘法循环群,并且 P 是群 G_1 的生成元,其中 q 是一个大素数。假设 G_1 和 G_2 这两个群上的 BDH 问题都是困难问题。如果定义在群 G_1 和群 G_2 上一个映射 $e:G_1 \times G_1 \rightarrow G_2$ 满足下面的三条性质,则称该映射为有效的双线性对。双线性对 $e:G_1 \times G_1 \rightarrow G_2$ 是群 G_1 与自身的笛卡尔积 $G_1 \times G_1$ 到群 G_2 的映射,即双线性对 $e:G_1 \times G_1 \rightarrow G_2$ 是指函数 $z = e(P_1, P_2)$, 其中 $P_1, P_2 \in G_1$ 为自变量, $z \in G_2$ 为因变量。

[0044] 双线性对应满足的三条性质为：

[0045] (1) 双线性. 对于任意的 $P_1, P_2 \in G_1$ 和 $a, b \in Z_q^*$, 有 $e(aP_1, bP_2) = e(P_1, P_2)^{ab}$ 。

[0046] (2) 非退化性. $e(P, P) \neq 1_{G_2}$, 其中 1_{G_2} 是群 G_2 的单位元。

[0047] (3) 可计算性. 对于任意的 $P_1, P_2 \in G_1$, 存在有效的算法计算 $e(P_1, P_2)$ 。

[0048] 其中,大素数 q 对于 BDH 问题而言不低于二进制表示的 160 比特,而对于大整数分解问题而言不低于二进制表示的 1024 比特。循环群的概念为:设 H 为群,如果存在一个元素 $P \in H$ 使得 $H = \{kP | k \in Z\}$, 则称 H 为加法循环群,称 P 是 H 的生成元;如果存在一个元素 $u \in H$ 使得 $H = \{u^k | k \in Z\}$, 则称 H 为乘法循环群,称 u 是 H 的生成元。若 H 为加法(乘法)循环群且生成元 $P(u)$ 的阶为 n , 即 n 是使得 $P(u)$ 的幂等于群 H 的单位元的最小正整数,则称 H 为 n 阶加法(乘法)循环群。简单来说,加法循环群是指该循环群的生成元能够以加法运算生成群中的所有元素,而乘法循环群是指该循环群的生成元能够以乘幂的方法生成群中的所有元素。此外, $Z_q^* = Z_q / \{0\} = \{1, 2, \dots, q-1\}$, 其中 Z_q 是指整数模素数 q 的剩余类,即 $Z_q = \{1, 2, \dots, q-1\}$ 。

[0049] 根据以上双线性对的描述,下面结合附图和实现例对本发明提出的一种基于证书的两方认证密钥协商方法进行进一步说明,但并不作为对本发明的限定。

[0050] 本发明所述方法设计的实体如下：

[0051] (1) 证书中心 CA:负责系统参数生成,即证书中心 CA 主密钥和系统公开参数集,并签发证书的可靠第三方；

[0052] (2) 会话发起方:会话的原始发起实体；

[0053] (3) 会话响应方:会话的响应实体。

[0054] 参照图附图 1 和附图 2, 图 1 是本发明所述的一种基于证书的两方认证密钥协商方法的流程图, 图 2 是依照本发明方法的基于证书的两方认证密钥协商系统执行的操作流程图。

[0055] 本发明所述方法的步骤具体描述如下:

[0056] 步骤 A, 生成证书中心 CA 的主密钥和系统公开参数集; 具体步骤如下:

[0057] 步骤 101: 证书中心 CA 根据设定的安全参数 $k \in Z^+$, 选择一个 k 比特的大素数 q , 并生成一个 q 阶加法循环群 G_1 和一个 q 阶乘法循环群 G_2 以及定义在群 G_1 和群 G_2 上的双线性对 $e: G_1 \times G_1 \rightarrow G_2$; 其中: Z^+ 是正整数集合, 双线性对 $e: G_1 \times G_1 \rightarrow G_2$ 是群 G_1 与自身的笛卡尔积 $G_1 \times G_1$ 到群 G_2 的映射, 即双线性对 $e: G_1 \times G_1 \rightarrow G_2$ 是指函数 $z = e(P_1, P_2)$, 其中 $P_1, P_2 \in G_1$ 为自变量, $z \in G_2$ 为因变量;

[0058] 步骤 102: 从加法循环群 G_1 中选择一个生成元 P 并在集合 Z_q^* 中随机选择一个整数, 并计算 $P_{pub} = sP$, 其中: 集合 $Z_q^* = \{1, 2, \dots, q-1\}$ 。

[0059] 步骤 103: 定义三个哈希函数 $H_1: \{0, 1\}^* \times G_1 \rightarrow G_1$ 、 $H_2: \{0, 1\}^* \times \{0, 1\}^* \times G_1 \times Z_q^* \rightarrow Z_q^*$ 、 $H_3: \{0, 1\}^* \times \{0, 1\}^* \times (G_1)^6 \times G_2 \times (G_1)^3 \rightarrow \{0, 1\}^k$; 其中: H_1 是笛卡尔积 $\{0, 1\}^* \times G_1$ 到 G_1 的密码学哈希函数, H_2 是 $\{0, 1\}^* \times \{0, 1\}^* \times G_1 \times Z_q^*$ 到 Z_q^* 的密码学哈希函数, H_3 是 $\{0, 1\}^* \times \{0, 1\}^* \times (G_1)^6 \times G_2 \times (G_1)^3$ 到 $\{0, 1\}^k$ 的密码学哈希函数, 整数 $k > 0$, k 表示系统安全参数的比特长度, $\{0, 1\}^*$ 表示长度不确定的二进制串的集合, $\{0, 1\}^k$ 表示长度为 k 比特的二进制串的集合, $(G_1)^3$ 和 $(G_1)^6$ 分别表示 3 个群 G_1 的笛卡尔积和 6 个群 G_1 的笛卡尔积, $\{0, 1\}^* \times G_1$ 表示 $\{0, 1\}^*$ 和群 G_1 的笛卡尔积, $\{0, 1\}^* \times \{0, 1\}^* \times G_1 \times Z_q^*$ 表示 $\{0, 1\}^*$ 、 $\{0, 1\}^*$ 、群 G_1 和集合 Z_q^* 的笛卡尔积, $\{0, 1\}^* \times \{0, 1\}^* \times (G_1)^6 \times G_2 \times (G_1)^3$ 表示 $\{0, 1\}^*$ 、 $\{0, 1\}^*$ 、 $(G_1)^6$ 、群 G_2 和 $(G_1)^3$ 的笛卡尔积。

[0060] 步骤 104: 根据步骤 101、步骤 102 及步骤 103 的执行结果, 生成 CA 秘密保存的主密钥为 $msk = s$ 和系统公开参数集 $params = \{k, q, G_1, G_2, e, P, P_{pub}, H_1, H_2, H_3\}$ 。

[0061] 步骤 B, 根据所述系统公开参数集, 用户身份信息, 生成用户的公钥和私钥对, 所述用户包括会话发起方和会话响应方; 具体步骤如下:

[0062] 步骤 105: 身份为 ID_U 的用户 U 在集合 Z_q^* 中随机选择一个整数 x_U 作为自己的私钥 $SK_U = x_U$ 。

[0063] 步骤 106: 计算并获得自己的公钥 $PK_U = x_U P$ 。

[0064] 步骤 C, 根据所述系统公开参数集, 证书中心 CA 的主密钥, 用户的身份信息, 用户的公钥, 生成用户的证书; 具体步骤如下:

[0065] 步骤 107: 身份为 ID_U 的用户 U 把身份信息 ID_U 和公钥 PK_U 提交给 CA。

[0066] 步骤 108: CA 计算 $Q_U = H_1(ID_U, PK_U)$, 生成用户 U 的证书 $Cert_U = mskQ_U = sQ_U$ 。

[0067] 步骤 109: CA 把证书 $Cert_U = sQ_U$ 发送给用户 U 。

[0068] 步骤 D, 根据所述系统公开参数集, 会话发起方和会话响应方的身份信息、公钥、私钥、证书, 生成两方共享的会话密钥; 具体步骤如下:

[0069] 步骤 110 : 会话发起方 A 在集合 Z_q^* 中随机选择一个整数 a, 计算 $R_A = aP$ 和 $W_A = H_2(ID_A, ID_B, Cert_A, SK_A)P$, 其中 ID_A 、 SK_A 和 $Cert_A$ 分别是会话发起方 A 的身份信息、私钥和证书, ID_B 是会话响应方 B 的身份信息。

[0070] 步骤 111 : A 发送 (ID_A, R_A, W_A) 给会话响应方 B。

[0071] 步骤 112 : 收到 (ID_A, R_A, W_A) 后, 会话响应方 B 在集合 Z_q^* 中随机选择一个整数 b, 计算 $R_B = bP$ 和 $W_B = H_2(ID_A, ID_B, Cert_B, SK_B)P$, 其中 SK_B 和 $Cert_B$ 分别是会话响应方 B 的私钥和证书。

[0072] 步骤 113 : B 发送 (ID_B, R_B, W_B) 给会话发起方 A。

[0073] 步骤 114 : 收到 (ID_B, R_B, W_B) 后, 会话发起方 A 依次计算 $K_{A_1} = e(R_B + Q_B, aP_{pub} + Cert_A)$, $K_{A_2} = SK_A PK_B + H_2(ID_A, ID_B, Cert_A, SK_A)W_B$, $K_{A_3} = aPK_B + SK_A R_B$ 和 $K_{A_4} = aR_B$, 其中, $Q_B = H_1(ID_B, PK_B)$; 然后计算并获得会话密钥 $K_{AB} = H_3(ID_A, ID_B, PK_A, PK_B, R_A, R_B, W_A, W_B, K_{A_1}, K_{A_2}, K_{A_3}, K_{A_4})$, 其中 PK_A 和 PK_B 分别是会话发起方 A 和会话响应方 B 的公钥。

[0074] 步骤 115 : 会话响应方 B 依次计算 $K_{B_1} = e(R_A + Q_A, bP_{pub} + Cert_B)$, $K_{B_2} = SK_B PK_A + H_2(ID_A, ID_B, Cert_B, SK_B)W_A$, $K_{B_3} = bPK_A + SK_B R_A$ 和 $K_{B_4} = bR_A$, 其中, $Q_A = H_1(ID_A, PK_A)$; 然后计算并获得会话密钥 $K_{BA} = H_3(ID_A, ID_B, PK_A, PK_B, R_A, R_B, W_A, W_B, K_{B_1}, K_{B_2}, K_{B_3}, K_{B_4})$ 。

[0075] 如附图 3 所示, 本发明还提供了一种基于证书的两方认证密钥协商系统, 所述系统包括: 系统参数生成模块、用户密钥生成模块、证书生成模块、密钥协商模块;

[0076] 系统参数生成模块, 用于根据输入的安全参数生成证书中心 CA 的主密钥以及密码系统的公开参数集;

[0077] 用户密钥生成模块, 用于根据系统参数生成模块生成的公开参数集, 以及用户的身份信息, 生成用户的公钥和私钥, 所述用户包括会话发起方和会话响应方;

[0078] 证书生成模块, 用于根据系统参数生成模块生成的公开参数集和证书中心 CA 的主密钥、用户的身份信息和公钥, 生成用户的证书;

[0079] 密钥协商模块, 用于根据系统参数生成模块生成的公开参数集、会话发起方和响应方的身份信息、用户密钥生成模块生成的会话发起方和响应方的公钥和私钥以及证书生成模块生成的会话发起方和响应方的证书, 生成会话两方共享的会话密钥。

[0080] 所述密钥协商模块包括会话发起方单元和会话响应方单元; 其中, 所述会话发起方单元用于会话发起方计算会话密钥; 所述会话响应方单元用于会话响应方计算会话密钥。

[0081] 以上只是对本发明的优选实施方式进行了描述。对该技术领域的普通技术人员来说, 根据以上实施方式可以很容易地联想到其它的优点和变形。因此, 本发明并不局限于上述实施方式, 其仅仅作为例子对本发明的一种形态进行详细、示范性的说明。在不背离本发明宗旨的范围内, 本领域普通技术人员在本发明技术的方案范围内进行的通常变化和替换, 都应包含在本发明的保护范围之内。

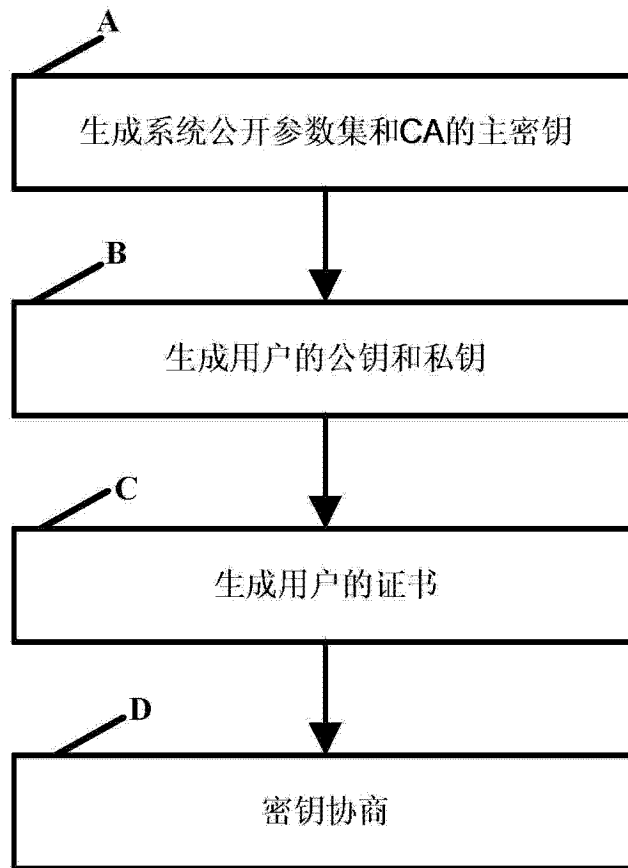


图 1

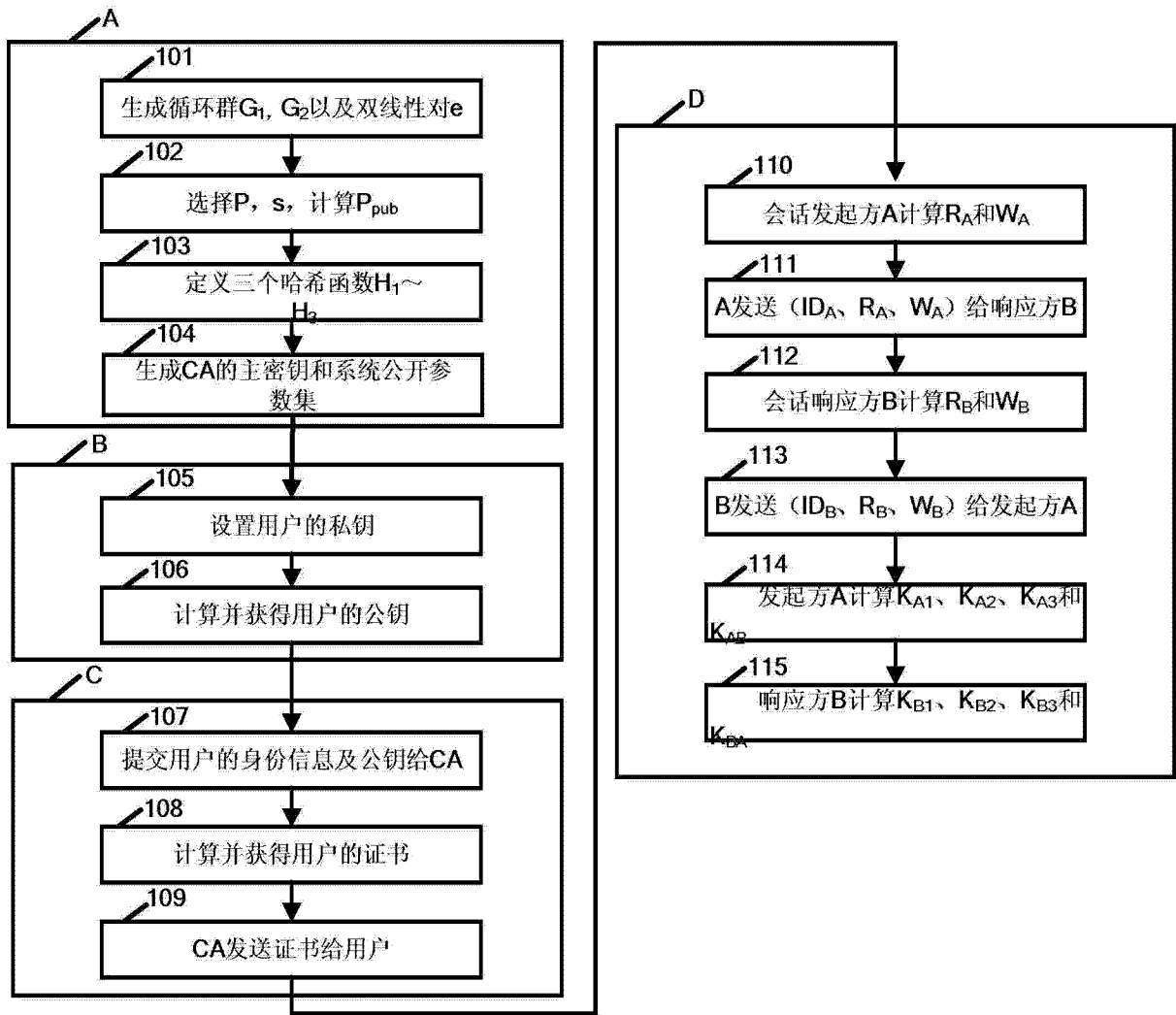


图 2

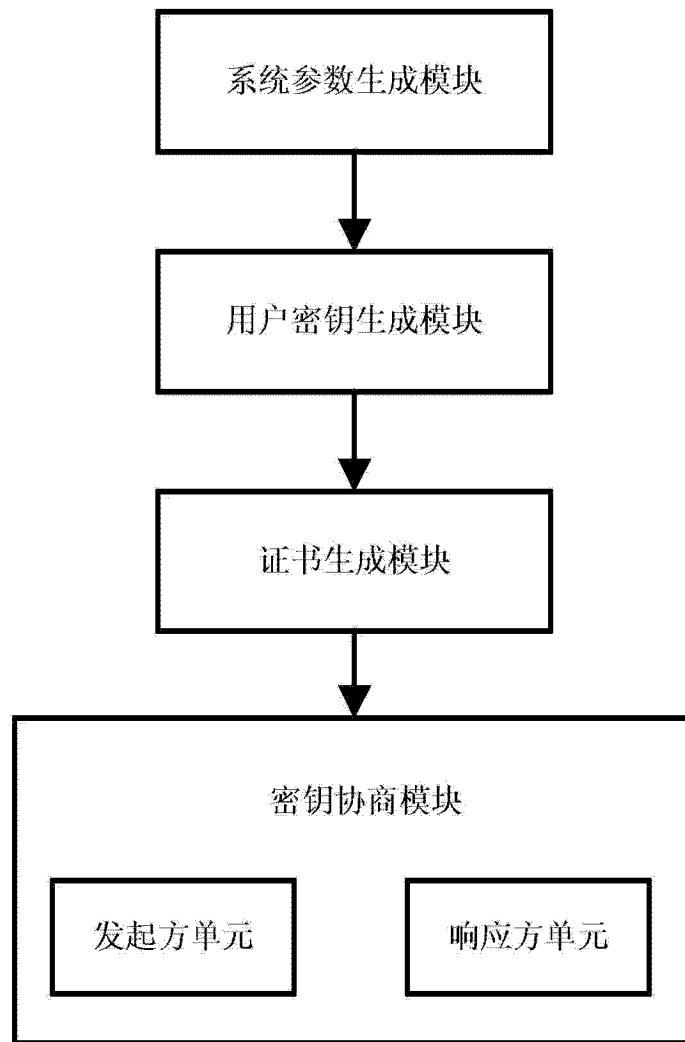


图 3