软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2013,24(12):2897−2908 [doi: 10.3724/SP.J.1001.2013.04389]

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

云计算环境虚拟机匿名身份证明方案*

张 严[1,2], 冯登国[1], 于爱民[1]

[1](中国科学院 软件研究所,北京 100190)

[2](中国科学院大学,北京 100049)

通讯作者: 张严, E-mail: janian@tca.iscas.ac.cn

摘 要: 作为云环境的重要构成部分,虚拟机的身份管理与认证是云计算安全中的重要问题.由于云计算环境具有大规模、分布式等特点,通常在云内存在多个身份权威.而现有的虚拟机身份证明方案中,身份权威的信息是公开的,因此在应用于云计算环境时,将造成组织结构、虚拟机位置等相关性信息的泄露,与云环境的结构透明、位置无关等特性相违背.提出的虚拟机身份证明,在保障原有认证性和信任关系的情况下,实现了身份证明过程中对身份权威信息的隐藏,避免了上述组织结构、位置等信息的暴露,可支持云环境结构透明、位置无关的特点.此外,该方案实现了对平台属性的安全证明,且证明过程无需身份权威的参与,避免了校验者和身份权威的合谋攻击,进一步提高了方案的安全性和实用性.

关键词: 虚拟机;身份证明;隐私保护;云计算

中图法分类号: TP309 **文献标识码**: A

中文引用格式: 张严,冯登国,于爱民.云计算环境虚拟机匿名身份证明方案.软件学报,2013,24(12):2897−2908. http://www.jos.org.cn/1000-9825/4389.htm

英文引用格式: Zhang Y, Feng DG, Yu AM. Virtual machine anonymous attestation in cloud computing. Ruan Jian Xue Bao/Journal of Software, 2013,24(12):2897−2908 (in Chinese). http://www.jos.org.cn/ 1000-9825/4389.htm

Virtual Machine Anonymous Attestation in Cloud Computing

ZHANG Yan[1,2], FENG Deng-Guo[1], YU Ai-Min[1]

[1](Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

[2](University of Chinese Academy of Sciences, Beijing 100049, China)

Corresponding author: ZHANG Yan, E-mail: janian@tca.iscas.ac.cn

Abstract: Being a vital constituent of cloud environment, the identity management and authentication of the system virtual machine is of great importance to cloud computing security. Multiple identity authorities exist in the large-scale, wide-distributed cloud environment and information regarding the authorities is publicly exposed in the current identity management and authentication scheme. Such deficiency of the scheme in the application of cloud environment poses the danger of revealing the organization and location of the users' platforms, violating the nature of cloud environment, i.e. organization transparency and location i.e. This paper presents the issuer-anonymous attestation scheme which, without altering the level of authentication and creditability, protects the anonymity of the platforms and the privacy of the issuers in the process of identity certification, effectively preventing information revelation in accordance with the transparency and independence nature of cloud environment. Furthermore, the proposed scheme realizes the attestation of the attributes of the platforms independently, requiring no participation of the identity authorities, and therefore, excludes the possibility of conspiracy attack between the inspector and the identity authorities and enhances the practicability and security of the scheme.

Key words: virtual machine; identity attestation; privacy protection; cloud computing

* 基金项目: 国家自然科学基金(91118006); 国家重点基础研究发展计划(973)(2013CB338003); 国家高技术研究发展计划(863)(2012AA01A403, 2011AA01A203)

收稿时间: 2011-04-11; 修改时间: 2011-11-17; 定稿时间: 2013-02-05

1 引 言

随着网络技术的发展,云计算已经成为当今信息技术发展的主要趋势之一.云计算具有的高伸缩性、位置无关性、低成本等特点使得用户可以关注自身业务逻辑的部署,而不用关心具体物理设备的位置.然而,云计算在为用户带来便利的同时,其自身结构的复杂性也为安全功能的实施带来了新的挑战.在云计算环境中,用户通过虚拟机使用云中的服务.因此,如何为云中的每个虚拟机进行标识,从而保证用户可对自身所属的虚拟机进行有效管理,并确保虚拟机运行环境的安全,是云计算安全中需要解决的重要问题.

目前,基于可信平台模块(TPM/TCM)[1]为计算平台建立身份的方法已得到了工业界和学术界的普遍重视和深入研究.通过为每个计算平台硬件绑定一个可信计算芯片 TPM/TCM,可以实现对平台私钥的硬件级保护.为了将基于 TPM 的平台身份管理应用于虚拟机,IBM 的研究者对虚拟机环境下 TPM 模块的虚拟进行了研究.设计并实现了一个虚拟 TPM(vTPM)方案,使得可以通过一个 TPM 芯片虚拟多个 vTPM 平台,从而实现对虚拟机数据和计算的保护.

通过使用 vTPM 及相应的身份证明协议,用户可以对云环境下自身所属的虚拟机身份进行管理,并对其可靠性进行认证.然而,由于云环境通常覆盖一个较大的领域,因此势必要在每个分域内构建单独的身份权威为虚拟机颁发平台身份证书.在实际应用中,基于管理方面的需求,分域通常按照地域、组织等分布,而在现有 vTPM 方案中的身份证明方案中,上述身份权威的信息是公开的,这使得敌手可以通过平台身份证书身份权威的信息得知虚拟机所属的分域,从而获取平台位置和组织结构等关联性信息.破坏云计算具有的结构透明、位置无关性等特点,使整个云计算平台的安全性受到威胁.基于上述原因,需要提出一种新的身份证明方案,在保证原有平台身份证明的情况下,实现身份权威信息的隐藏,避免上述组织结构、位置相关性信息的暴露,以支持云环境结构透明、位置无关性的特点.

1.1 本文主要贡献

在本文中,我们针对云环境下虚拟机平台身份管理问题中安全与隐私性的需求,给出了一个基于 vTPM 的匿名平台身份证明方案,与现有方案相比,该方案可实现出示过程中证书签发者的匿名性,在保障原有认证性和平台匿名性的同时,实现了对身份权威信息的隐藏,以支持云计算环境结构透明与位置无关的特性.同时该方案还使用 vTPM 对平台证书私钥进行了硬件保护,可有效防止用户凭证出借,进一步提高了方案的安全性.

为了实现具有身份权威信息保护特性的身份证明方案,本文还提出了被称为“签发者匿名凭证”的新型凭证方案,在签发者匿名凭证方案中,存在多个可信的凭证签发者,用户首先从某个签发者处获取包含其属性信息的凭证,在出示阶段,用户可根据策略自主选择若干凭证签发者构成一个签发者匿名集合,再在无需签发者参与的情况下向校验者出示其凭证.校验者可通过该凭据确信用户拥有签发者匿名集合中某个可信的签发者签发的合法凭证,但无法确定具体的签发者信息.此外,上述出示过程还满足用户匿名性及不可关联性,即校验者无法得知用户的具体身份,并且对于多次出示过程,校验者也无法判断其是否是由同一用户执行.在本文中,我们对签发者匿名凭证方案及其应满足的安全性进行了定义,基于双线性映射给出了满足上述特性的一个方案构造并在随机预言机(random Oracle)模型下基于 k-BCAA1 困难性假设[2]对方案的安全性进行了证明.

1.2 相关研究工作

对于 TPM 平台身份证书出示时的隐私保护问题,Brickell 等人提出了 BCL 直接匿名证明方案(direct anonymous attestation,简称 DAA)[3],随后相关研究者在该方案思想的指导下,基于不同的签名机制给出了多种直接匿名证明协议.该方案的主要思想是通过零知识证明机制,使得终端设备向校验者证明身份时,无需直接出示由身份权威签发的平台身份证书,保证了验证方无法与身份权威合谋将同一平台执行的多次出示过程进行关联或唯一确定当前通信终端,从而侵犯终端的隐私性.

自从 BCL-DAA 方案被提出以来,得到了工业界和学术界的广泛关注,研究者相继提出了许多 DAA 方案,目前,DAA 方案的研究方向主要集中于以下几个方面:

(1) 设计更为高效的 DAA 方案.原始的 BCL-DAA 方案基于强 RSA 假设,Chen,Morrissey 和 Smart 使用非

对称双线性映射对 BCL-DAA 方案进行了改进[4],还有许多研究者基于双线性映射提出了新的 DAA 方案[5,6],与原始 DAA 方案相比,双线性映射的引入有效提高了 DAA 方案的效率.

(2) 将 DAA 方案应用于系统认证等方面.Camensich 提出了一种方案,将 DAA 方案应用于匿名证书的保护[7].Dietrich 则使用 DAA 方案构造了 RFID 卡的隐私保护认证方案[8].

(3) 在不同的计算环境下实现 DAA 方案.由于现有的 DAA 方案过于复杂,因此,研究人员针对移动平台提出了轻量级的 DAA 协议,减小了 DAA 协议中用户端的计算代价,以使其更适合嵌入式设备等资源受限设备,这方面的工作见文献[9]等.

然而,现有的 DAA 方案都只能实现平台身份的隐私保护,而无法隐藏平台证书签发者的身份,因此当这些方案应用于云环境时,将会破坏云环境的结构透明和位置无关特性,造成系统的安全威胁.

2001 年,Rivest,Shamir 和 Tauman 提出了环签名[10]的概念.在环签名中,任意实体可以使用其私钥和由他所选择的特定集合中其他实体的公钥生成一个签名,该签名可通过校验证明其是由集合中某一实体生成,但无法确认签名生成者的具体身份.但是,由于环签名只能由持有环中某实体私钥的实体生成,因此当使用环签名保护签发者的身份时,其凭证出示过程需要凭证签发者,即身份权威的参与,无法实现平台证书签发与出示过程的独立性.此外,在 Boyen 提出的 mesh 签名[11]和一些基于属性的签名(ABS)[12,13]方案中,对多公钥环境下的隐私保护进行了讨论.但是,上述方案的应用场景与云环境下平台证书签发者匿名的需求差别较大,因此也无法应用于云环境下的签发者匿名环境.

2 预备知识

2.1 双线性映射

首先,我们对本文中使用到的双线性映射的概念进行定义,假设 G_1,G_2 与 G_T 为 3 个素数阶循环群,其阶为 p, p_1,p_2 分别为 G_1,G_2 的生成元.ψ为 G_2 到 G_1 的同构映射,$\psi(P_2)=P_1$.

若存在映射 $e:G_1\times G_2\to G_T$ 满足以下属性,则称 e 是一个双线性映射[14]:

双线性:对所有 $P\in G_1,Q\in G_2,a,b\in Z_p,e(aP,bQ)=e(P,Q)^{ab}$.

非退化性:存在 $g_1\in G_1,g_2\in G_2$ 使得 $e(g_1,g_2)\neq 1$.

可计算性:对所有 $g_1\in G_1,g_2\in G_2$,存在可有效计算 $e(g_1,g_2)$ 的算法.

2.2 安全假设

接下来介绍方案中使用到的安全假设:

定义 1(*k*-BCAA1 假设[2]). 双线性 CAA1(*k*-BCAA1)困难性假设是指,对于整数 $k,x\in Z^*_p$, $P_2\in G^*_2$, $P_1=\psi(P_2)$, $e:G_1\times G_2\to G_T$,给定 P_1, $P_2,Q=xP_2$, h_0, $\left(h_1,\frac{1}{h_1+x}P_2\right)$,..., $\left(h_k,\frac{1}{h_k+x}P_2\right)$(其中,$h_i\in Z^*_p$ 且对于 $0\leqslant i\leqslant k$, h_i 各不相同),计算 $e(P_1,P_2)^{1/(x+h_0)}$ 是困难的.

定义 2(*k*-BDHI 假设[15]). 双线性 Diffie-Hellman 逆运算(*k*-DBHI)困难性假设是指,对于整数 $k,x\in Z^*_p$, $P_2\in G^*_2,P_1=\psi(P_2)$ 和双线性映射 $e:G_1\times G_2\to G_T$,给定 $(P_1,P_2,xP_2,x^2P_2,\ldots,x^kP_2)$,计算 $e(P_1,P_2)^{1/x}$ 是困难的.

在本文中,将基于 Chen 等人提出的 *k*-BCAA1 困难性假设对我们提出的方案进行安全性证明,根据 Chen 与 Cheng 对双线性映射下相关困难问题的研究[2]可知,*k*-BCAA1 困难性假设与 *k*-BDHI 困难性假设在多项式时间内等价,而后者曾在 Boneh 等人提出的基于身份签名协议[15]的安全性证明中被使用.

2.3 关于知识的零知识证明方案

此外,本文所提出的方案还使用到了在 DAA 等方案中使用到的关于知识的零知识证明(ZKPK)技术来实现平台身份凭证的隐私性质.通过使用 ZKPK 协议,证明方可以使校验者确信其拥有某个秘密信息(知识),却又无法获取和该秘密有关的任何信息,ZKPK 协议的形式化定义可见文献[16],在本方案中,我们使用由 Camenisch

提出的离散对数环境下对指数知识的零知识证明方案[17].举例来说,如下形式的零知识证明 $\Pi = POK\{\alpha : g^{\alpha} = h\}$ 表示证明者可使校验者相信对公开值 g,h,证明者拥有满足等式 $g^{\alpha} = h$ 的 α 值,但校验者无法通过证明获取有关 α 的任何信息.同时,对于上述知识证明方案,存在与之对应的知识抽取器,可以从任何能够完成上述证明过程的证明者处抽取出该证明对应的知识.

3 云环境下虚拟机身份平台证明方案

3.1 基本思想

为了实现云环境下虚拟机身份的安全证明与隐私保护,本文提出了满足隐私保护性质的虚拟机身份证明方案,与现有 DAA 方案相比,本方案可同时实现平台身份与平台所属域信息的匿名,并且满足身份证明过程中证书签发与出示过程的独立性以及对平台属性证明的需要.本节我们将对该方案的主要思想进行描述.

在云环境下基于 vTPM 的虚拟机身份证明系统中,存在 3 类参与方(如图 1 所示):身份权威、使用 vTPM 的虚拟机平台和校验者.在整个云环境内,存在若干分域,每个分域有其对应的身份权威 I_k,这些身份权威为虚拟机平台 U_i 签发身份凭证.每个校验者 V_j 根据其策略,信任云环境其中的某些身份权威,这些身份权威构成集合 $Trusted_j$.虚拟机 U_i 由两部分组成:具有硬件保护机制的 vTPM 安全模块 S_i 与虚拟机外部操作系统 H_i.U_i 拥有由其所属分域的身份权威 I_{ui} 颁发的平台身份凭证,当平台需要向某个校验者 $V_j(I_{ui} \in Trusted_j)$ 进行平台身份证明时,U_i 可以从 $Trusted_j$ 中自主选择一个匿名签发者集合 $I_{anou}(I_{ui} \in I_{anou})$ 并通过凭证出示过程向 V_j 证明其拥有 I_{anou} 中某个可信身份权威颁发的合法凭证,同时,该出示过程不暴露平台所属的具体分域权威 I_{ui} 的信息.

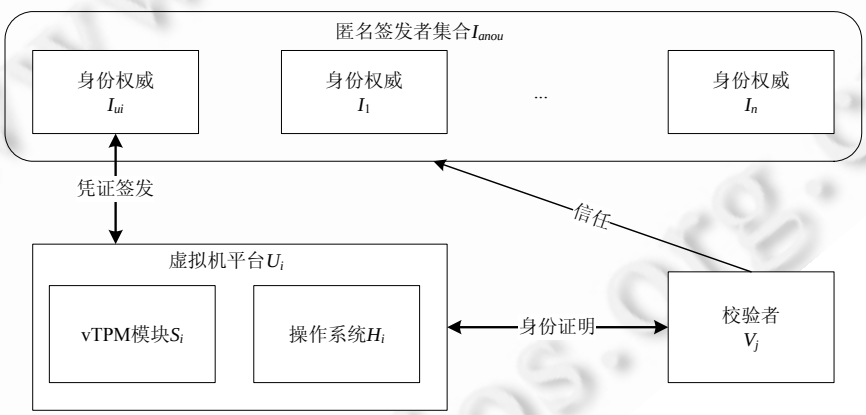

Fig.1 The framework of the VM identity attestation

图 1 虚拟机身份证明系统结构

身份证明方案包含 3 个主要阶段:系统建立、虚拟平台身份凭证颁发以及凭证出示,其具体操作如下:

(1) 系统建立.首先,生成系统公开参数,随后为每个分域的身份权威生成密钥对并使用 PKI 系统为其颁发公钥证书,以保证身份权威公钥的有效性和权威性可以得到验证.

(2) 虚拟平台身份凭证颁发.在使用 vTPM 方法建立虚拟机时,会为每台虚拟机中包含的 vTPM 生成唯一的签名密钥 EK,并由 TPM 芯片对其进行硬件级的保护.当虚拟机 U_i 需要获取平台身份凭证时,虚拟机的 vTPM 模块使用其 EK 与其所属分域的身份权威 I_{ui} 建立安全通信信道,然后 vTPM 为虚拟机生成一对身份验证密钥 AIK,其私钥为 sk_u ,公钥为 Pk_u.

接下来,虚拟机平台将其 AIK 公钥发送给身份权威 I_{ui},身份权威为用户生成凭证 $cre_u(\omega)$,凭证中包含平台 AIK 的信息与平台所拥有的属性 ω.身份权威使用 vTPM 平台 EK 的公钥对平台身份凭证 $cre_u(\omega)$ 进行加密并发送给虚拟机平台,虚拟机平台使用其 vTPM 的 EK 对其进行解密,从而确保只有拥有相应 EK 的平台才能解密获

取合法的平台身份凭证.当获得平台身份凭证后,虚拟机将该凭证储存在虚拟机操作系统 H_i 中.

(3) 凭证出示.当虚拟机平台 U_i 需要向校验者 V_j 证明其拥有的合法平台身份时,虚拟平台从 V_j 信任的签发者集合 $Trusted_j(I_{ui}\in Trusted_j)$中选择若干身份权威与其自身所属分域的身份权威 I_{ui} 一起构成匿名签发者集合 I_{anou},然后使用 $cre_u(\omega)$ 和 sk_u 生成匿名化的凭证证明.其中,与平台 AIK 私钥 sk_u 相关的操作在 vTPM 模块内部完成,其余操作在虚拟机操作系统 H_i 中完成,以降低 vTPM 的计算负担,提高凭证出示过程的效率.

收到 U_i 发送的证明后,V_j 可以使用匿名签发者集合内的所有权威的公钥对凭证及其包含的属性进行验证,确信平台拥有可信身份权威签发的凭证并具有属性 ω,同时拥有与该凭证对应的 AIK 私钥 sk_u,从而实现了在不暴露身份权威信息的同时对平台身份和属性的证明.

3.2 签发者匿名凭证方案

对于上述虚拟机身份证明方案中使用的凭证签发与出示方案,其所必须满足的安全需求总结如下:

(1) 凭证不可伪造性.不可伪造性要求只有拥有一个合法平台凭证 $cre_u(\omega)$ 的虚拟机平台才能生成正确的匿名化凭证,完成凭证出示操作,且多个虚拟机平台无法通过对凭证进行组合生成新的属性或改变其身份权威.

(2) 凭证签发者匿名性.校验者无法分辨用户所出示的凭证是由匿名集合中的哪个凭证签发者所签发的,这一特性确保了云环境下的位置无关特性得以实施.

(3) 平台身份不可关联性.对于具有相同属性 ω,且匿名签发者集合交集不为空的两次凭证出示过程,签发者无法确定其是否为同一平台所执行,且校验者不能通过凭证出示获取用户 AIK 和 EK 的信息.

(4) 出示过程独立性.虚拟机平台无需凭证签发者的参与即可独立完成凭证出示过程.

基于上述安全性需求,我们定义如下的签发者匿名凭证方案:

签发者匿名凭证方案由 4 种算法 Setup,IssuerKeyGen,Issue,Show 组成:

Setup:对于输入 1^λ,λ为安全参数,输出公共参数 $params$.

IssuerKeyGen:生成签发者密钥对,输入为公共参数 $params$ 和签发者身份 I,输出为签发者密钥对 sk_I, P_{pubI}.

Issue:凭证签发算法,对于给定的用户身份 u 和消息 ω,使用签发者密钥 sk_I 为用户生成一个凭证 cre.

Show:凭证出示与校验协议,该协议是用户与校验者间执行的交互式证明协议.其中用户输入为凭证 cre、消息 ω、匿名签发者集合 L ($I\in L$)和与其对应的用户身份 u;校验者输入为签发者集合 L 和消息 ω,如果校验者相信用户持有匿名签发者集合 L 中某个签发者为其颁发的合法凭证,且该凭证中对应的消息为 ω,则输出 1,否则输出 0.

3.3 防出借的签发者匿名凭证方案构造

令 G_1,G_2 与 G_T 为素数阶循环群,阶为 p,p_1,p_2 分别为 G_1,G_2 的生成元.ψ为 G_2 到 G_1 的同构映射,$\psi(P_2)=P_1$. $e:G_1\times G_2\to G_T$ 为双线性映射(定义见第 2.1 节),则签发者匿名凭证方案构造如下:

Setup.首先,选取杂凑函数 $h:\{0,1\}^*\to Z^*_p$, $H:\{0,1\}^*\to G_2$, $P_0\in G_2$.则系统的公共参数定义为 $params=\{G_1,G_2,G_T,p,e,\psi,P_1,P_2,P_0,h,H\}$.

IssuerKeyGen. 对于给定的签发者 I,随机选择 $x_I\in Z^*_p$,计算 I 的公钥 $P_{pubI}=x_IP_2$,对应的签发者私钥为 x_I .

Issue.对于输入的用户身份 u 和消息 ω,签发者 I 可通过如下方式为用户签发凭证:

首先 I 计算 $Q_\omega=H(\omega)$,然后随机选择 $r,r_u\in Z^*_p$,计算 $cre=(c_1,c_2,d_1,d_2)=\left(\frac{P_2+uP_0+rQ_\omega}{h(\omega\|I)+x_I},rP_2,\frac{r_uQ_\omega}{h(\omega\|I)+x_I},r_uP_2\right)$ 并发送给用户.

当用户收到凭证后,可以通过等式 $e(h(\omega\|I)P_1+\psi(P_{pubI}),c_1)=e(P_1,P_2)e(P_1,P_0)^u e(\psi(c_2),H(\omega))$ 与 $e(h(\omega\|I)P_1+\psi(P_{pubI}),d_1)=e(\psi(d_2),H(\omega))$ 来验证凭证的有效性.

Show. 当用户需要向校验者出示凭证时,他首先选择匿名签发者集合 L,L 中某个签发者 I 为用户凭证 cre 的真实签发者.接下来,用户随机选择 $r_d,s,t\in Z^*_p$ 并计算匿名化的凭证 $f_1=s^{-1}t^{-1}(c_1+r_dd_1),f_2=c_2+r_dd_2$.

然后,对于 L 中除 I 外的所有签发者 i,用户随机选择 $a_i\in Z^*_p$,并使用 I 的公钥 $P_{pubI}=x_IP_2$ 计算

$S_i = sa_i(h(\omega\|I)P_1 + \psi(P_{pubI}))$.对于 I,计算 $S_I = sP_1 - s\cdot\sum_{i\in L, i\neq I} a_i(h(\omega\|i)P_1 + \psi(P_{pubi}))$. 最后,用户计算 $T = s(h(\omega\|I)P_1 + \psi(P_{pubI}))$.

将所有 $S_i(i\in L)$ 组成的集合记为 S,则用户将 $a=(S,T,f_1,f_2)$ 及相应的签发者集合 L 发送给校验者.

然后,用户使用 u 和 t 生成如下的 ZKPK 证明:

$$\Pi = POK\{u,t: e(P_1,P_2)\cdot e(\psi(f_2),H(\omega)) = e(T,f_1)^t\cdot e(P_1,P_0)^{-u}\}.$$

当校验者接收到用户发来的消息 α,Π和签发者集合 L 时,他首先获取所有对应的签发者公钥,再验证等式 $\prod_{i\in L} e(S_i,h(\omega\|i)P_2 + P_{pubi}) = e(T,P_2)$ 是否成立,并校验知识证明Π的正确性.如果上述验证式均成立,则出示协议执行成功,校验者输出 1,否则输出 0.

3.4 安全性分析

由于在凭证出示时,仅需使用用户所拥有的凭证和签发者集合中的公钥,因此本文方案显然满足凭证出示过程的独立性.此外,由于在出示时需要使用用户身份信息 u 生成对应的知识证明,因此即使敌手获取到了出示过程的消息记录,也无法使用该记录生成新的证明.对于方案的正确性、隐私性和不可伪造性,安全分析如下:

(1) 正确性.本方案的正确性验证见附录 A.

(2) 隐私性.对于签发者匿名性,我们要求凭证的真实签发者在匿名签发者集合中完全匿名,也就是说,对于大小为 n 的匿名签发者集合,校验者在凭证出示过程中所获得的信息对凭证出示过程所对应的真实签发者进行猜测,其猜测正确的概率与 $1/n$ 的差是可忽略的.

对于用户不可关联性,我们要求对于具有相同属性凭证且签发者集合交集不为空的两次出示过程,签发者无法确定其是否为同一用户所执行.

在凭证出示阶段,校验者可获得四元组 (S,T,f_1,f_2) 和与其对应的知识证明Π,根据零知识证明的零知识性质,校验者无法从Π中获取任何有关凭证签发者和用户身份的信息.又根据定义 $f_1 = s^{-1}t^{-1}(c_1 + rad_1)$, $f_2 = c_2 + rad_2$ 以及 $T = s(h(\omega\|I)P_1 + \psi(P_{pubI}))$ 可知,对于 Z^*_p 中随机选择的 s,t 和 rd,f_1,f_2 与 T 独立随机分布于 G_1 及 G_2 之上.接下来,假设 $S=\{S_1,...,S_n\}$ 由其中的第 k 个签发者签发的凭证生成,由于 a_i 随机分布于 Z_p 上,则除 S_k 以外,因此集合中所有其他的 S_i 为 G_1 中随机元素.而 S_k 又是由 $a_i,h(\omega\|i),T$ 和公钥计算得到,因此对于给定的 $\omega, S=\{S_1,...,S_n\}$ 的分布与下列分布: $\{a_1P,\ldots,a_nP : \sum a_iP = C\}$ 相同,其中 C 仅由 T 与ω的值决定.

因此,对于任何算法 A,大小为 n 的签发者匿名集合 L,以及 $I\in L$,A 猜测成功的概率与 $1/n$ 的差是可忽略的.通过上述分析,可得知本文提出的签发者匿名凭证方案满足无条件签发者匿名性与用户不可关联性,且校验者在与签发者合谋的情况下,也无法获取用户的签发者信息与身份信息.

(3) 不可伪造性.对于不可伪造性,本文在随机预言机模型下定义选择信息下的存在性伪造攻击,在该攻击下,敌手可以访问以下预言机:

凭证签发预言机.对于给定的用户身份 u,消息ω和签发者 I,输出与之对应的凭证 cre.

随机预言机.对于消息 m,输出随机值 r.

由此,我们定义挑战者 C 与敌手 F 间的如下 Game:

(1) 初始化阶段.F 给出其要挑战的属性信息 ω^* 与签发者集合 L^*.

(2) 系统建立阶段.C 选择足够大的安全参数执行 Setup 算法,将公共参数 $params$ 发送给 F.

(3) 签发者生成阶段.对于签发者集合 L^* 中的每个签发者 I,C 执行 IssuerKeyGen 算法生成相应的密钥对,C 保留私钥 sk_I 并将公钥集合 Pub_L^* 发送给 F.

(4) 查询阶段.F 可对随机预言机和凭证签发预言机进行有限次数的访问,对于凭证签发预言机的所有输入,C 记录其中的属性信息ω.

(5) 伪造阶段.C 扮演诚实的校验者,与 F 执行凭证出示过程,F 对消息 ω^* 和签发者集合 L^* 进行证明.

如果 F 能够通过证明使得 C 相信其拥有签发者集合 L^* 中某个签发者为其签发的一个合法凭证,其中包含

的消息为 ω^*,且对于签发者集合 L^* 中的每个签发者 i,敌手 F 未使用(ω^*,i)对凭证签发预言机进行过查询,则称 F 获得此游戏的胜利.定义 F 获得胜利的概率为敌手 F 的优势 $Adv_F(1^\lambda)$.

定义 3(不可伪造性). 如果一个敌手 F 在运行时间不超过 t,且最多进行 q_I 次凭证签发查询和 q_H 次杂凑函数查询的情况下,其优势 $Adv_F(1^\lambda)$ 不低于 ε,则称该敌手 (t,q_I,q_H,ε)-破坏一个凭证方案.如果对于一个凭证方案,不存在任何敌手可以 (t,q_I,q_H,ε)-破坏该方案,则称该方案是 (t,q_I,q_H,ε)-不可伪造的.

对于第 3.3 节中的签发者匿名凭证方案的不可伪造性,有如下定理:

定理 1. 如果存在 (t,q_I,q_H,ε) 敌手 F 可以有效地伪造证据 α,其中签发者集合大小为 n,则可构造一个 (t',ε') 算法 A 解决 q_I-BCAA1 问题,其中,

$$t' \leqslant t + (2q_I + 3n - 1)t_{Gsm} + (5q_I + q_H + 4n + 4)t_{Gadd} + (6q_I + q_H + 1)t_{mu} + (2q_I + q_H + 1)t_{add} + 3q_I t_{inv} + 2t_p,$$

$$\varepsilon' \geqslant \left(\frac{q_I}{q_H}\right)^{q_I} \cdot \varepsilon.$$

上式中,t_{Gsm},t_{Gadd} 分别为群 G_1,G_2 和 G_T 中乘法运算、加法运算所需时间,t_{add},t_{inv},t_{mu} 分别为 Z_p 中加法、求逆运算和乘法运算所需时间,t_p 为一次双线性映射运算所需时间.证明参见附录 B.

3.5 云计算环境下虚拟机身份证明方案

通过使用第 3.3 节中提出的签发者匿名凭证方案,可以实现满足安全需求与隐私保护需求的虚拟机身份证明方案,该方案的具体实施方法如下:

(1) 系统建立.首先,执行第 3.3 节中签发者匿名凭证方案的 Setup 算法生成系统公开参数,随后加入系统的身份权威可通过 IssuerKeyGen 算法生成其密钥对并公布,为了保护签发者公钥的有效性和权威性,使用 PKI 系统来为身份权威颁发公钥证书.

(2) 虚拟平台身份凭证颁发.虚拟机平台 U_i 首先使用 EK 向身份权威 I_{ui} 认证其平台身份并建立安全通信信道.平台生成 AIK 密钥对,其中私钥为 $sk_u \in Z_p$,公钥 $Pk_u = sk_u P_0$.接下来,虚拟机平台将其 AIK 公钥发送给身份权威,身份权威将用户 AIK 信息作为凭证中包含的消息,为 U_i 生成如下格式的凭证:

$$cre_u(\omega) = (c_1, c_2, d_1, d_2) = \frac{P_2 + Pk_u + rQ_\omega}{h(\omega \| I) + x_I}, rP_2, \frac{r_u Q_\omega}{h(\omega \| I) + x_I}, r_u P_2.$$

(3) 凭证出示.U_i 从校验者 V_j 信任的签发者集合 $Trusted_j(I_{ui} \in Trusted_j)$中选择匿名签发者集合 I_{anou},使用其 AIK 私钥和上一阶段获取的凭证按照与签发者匿名凭证中 Show 算法相同的步骤计算 f_1, f_2, S, T,然后 vTPM 使用 AIK 私钥生成 ZKPK 证明:

$$\Pi = POK\{sk_u, t := e(P_1, P_2) \cdot e(\psi(f_2), H(\omega)) = e(T, f_1)^t \cdot e(P_1, P_0)^{-sk_u}\}.$$

随后,U_i 将其生成的所有消息发送给校验者 V_j,V_j 可按照第 3.3 节中的方法进行校验.通过上述过程,V_j 可验证虚拟机拥有 I_{anou} 中某个可信身份权威签发的合法平台身份凭证,并且用户平台对应的 vTPM 拥有与凭证对应的 AIK 私钥,此外还可验证虚拟机平台具有的属性.

容易看出,上述方案中用户凭证的格式与第 3.3 节中签发者匿名凭证方案中的凭证相同,只是使用了 vTPM 的 AIK 私钥 sk_u 作为凭证中所包含的消息 u,因此该凭证满足不可伪造性、签发者匿名性和用户身份的不可关联性.同时由于证明时需要使用 sk_u 进行计算,而 sk_u 储存于 vTPM 内部,受到 vTPM 的硬件级保护,因此可以防止平台身份凭证的出借.

综上所述,本节中描述的平台身份证明方案可以实现凭证不可伪造性、签发者匿名性和用户身份匿名性,此外该方案还保证了现有 DAA 方案中凭证签发与出示过程的独立性以及对平台属性的证明,因此可满足云环境对虚拟机平台身份证明中的需求.

4 效率分析与实现

对于本文第 3.5 节中给出的云环境下虚拟机身份证明方案,其效率分析如下:用户凭证的长度为 4 个群元

素,凭证出示时的通信量与匿名签发者集合中的签发者个数 n 线性相关,共包含 n+5 个群 G_1,G_2,G_T 中元素和 3 个群 Z_p 中元素.

对于计算开销,我们主要对凭证出示时的计算量进行分析,由于与模乘运算和双线性映射运算相比,其他运算的时间所需时间很短,可以忽略不计,因此我们使用模乘运算和双线性映射运算的次数作为衡量方案效率的主要指标,具体的分析结果见表 1.

Table 1 Efficiency analysis

表 1 效率分析

		模乘运算次数(群 G_1,G_2)	模乘运算次数(群 G_T)	双线性映射运算次数
用户计算量	操作系统	$3n$+2	1	1
	vTPM 模块	0	1	0
校验方计算量		n	3	n+3

接下来,我们对本文中提出的虚拟机身份证明方案进行了原型实现,由于目前真实的 TPM/TCM 芯片尚不支持本文协议中采用的密码算法,因此采用 jPBC 库(java Paring-based Cryptography Library)进行了模拟实现,并使用一台配置为 Intel Q6600 CPU,2GB 内存的计算机进行了性能测试,表 2 给出了原型系统的性能测试结果.

Table 2 Experimental data of prototype system

表 2 原型系统实验数据

分域数目	5	10	15	20
凭证签发(ms)	69	70	70	70
凭证出示(ms)	512	859	1 202	1 589

由表 2 可见,系统签发凭证所需的时间与分域数目无关,凭证出示所需时间与分域数目基本呈线性关系,符合本节中对系统计算效率的分析.当系统中存在 20 个分域时(可满足大多数云计算系统的分布式管理需求),我们所提出的方案可使得用户在 1.6s 内完成对虚拟机身份的证明.在真实系统中,由于 TPM/TCM 芯片仅需执行 1 次模指数运算,因此即使考虑到 TPM/TCM 芯片的运算速度对整个方案性能的影响,本文所提出方案的效率也是可以接受的.

5 结论与进一步工作

本文针对云环境中虚拟机身份证明的需求,提出了一个保护隐私的虚拟机身份证明方案,与现有方案相比,该方案可实现出示过程中身份权威的匿名性、平台证书签发与出示过程的独立性以及平台身份的匿名性,在实现对虚拟机安全管理的同时支持云环境结构透明、位置无关性的特点.

为实现上述身份证明方案中的签发者匿名性,我们提出了一种签发者匿名凭证的新型匿名凭证方案,该方案可使得拥有由可信签发者 I 签发凭证的用户自主选择签发者集合 $L(I\in L)$并在不暴露 I 具体信息的情况下,向校验者证明凭证的有效性以及凭证的签发者属于匿名集合 L.上述证明过程可由用户独立完成,不需 I 的参与,且满足签发者与校验者合谋情况下的无条件匿名性.

在下一步工作中,我们将对该协议进行改进,以提高其计算效率,减少凭证的长度并考虑在标准模型下实现满足签发者匿名性的凭证协议.

致谢 在此,我们向对本文的工作给予支持和建议的同行,尤其是中国科学院软件研究所张振峰研究员、张立武博士以及由他们领导的讨论班上的各位老师和同学表示感谢.

References:

[1] Trusted Computing Group. TCG TPM Specifiction, Version 1.2, Revision 103. 2007. http://www.trustedcomputinggroup.org/

[2] Chen LQ, Cheng ZH. Security proof of Sakai-Kasahara's identity-based encryption scheme. In: Smart NP, ed. Proc. of the Cryptography and Coding. LNCS 3796, Berlin: Springer-Verlag, 2005. 442−459. [doi: 10.1007/11586821_29]

[3] Brickell E, Camenisch J, Chen LQ. Direct anonymous attestation. In: Atluri V, ed. Proc. of the 11th ACM Conf. on Computer and Communications Security. New York: ACM, 2004. 132−145. [doi: 10.1145/1030083.1030084]

[4] Chen LQ, Morrissey P, Smart NP. Pairings in trusted computing. In: Galbraith SD, Paterson KG, eds. Proc. of the Pairing-Based Cryptography—Pairing 2008. LNCS 5209, Berlin: Springer-Verlag, 2008. 1−17. [doi: 10.1007/978-3-540-85538-5_1]

[5] Chen LQ. A DAA scheme requiring less TPM resources. In: Bao F, Yung M, Lin DD, Jing JW, eds. Proc. of the Information Security and Cryptology. LNCS 6151, Berlin: Springer-Verlag, 2009. 350−365. [doi: 10.1007/978-3-642-16342-5_26]

[6] Brickell E, Li JT. A pairing-based DAA scheme further reducing TPM resources. In: Acquisti A, Smith SW, Sadeghi A-R, eds. Proc. of the Trust and Trustworthy Computing. LNCS 6101, Berlin: Springer-Verlag, 2010. 181−195. [doi: 10.1007/978-3-642-13869-0_12]

[7] Camenisch J. Protecting (Anonymous) credentials with the trusted computing Group's TPM V1.2. In: Fischer-Hübner S, Rannenberg K, Yngström L, Lindskog S, eds. Proc. of the Security and Privacy in Dynamic Environments. Berlin: Springer-Verlag, 2006. 135−147. [doi: 10.1007/0-387-33406-8_12]

[8] Dietrich K. Anonymous RFID authentication using trusted computing technologies. In: Yalcin SBO, ed. Proc. of the Radio Frequency Identification: Security and Privacy Issues. LNCS 6370, Berlin: Springer-Verlag, 2010. 91−102. [doi: 10.1007/978-3-642-16822-2_9]

[9] Wachsmann C, Chen L, Dietrich K, Löhr H, Sadeghi A, Winter J. Lightweight anonymous authentication with TLS and DAA for embedded mobile devices. In: Burmester M, Tsudik G, Magliveras S, IlićI, eds. Proc. of the Information Security. LNCS 6531, Berlin: Springer-Verlag, 2010. 84−98. [doi: 10.1007/978-3-642-18178-8_8]

[10] Rivest RL, Shamir A, Tauman Y. How to leak a secret. In: Boyd C, ed. Advances in Cryptology—ASIACRYPT 2001. LNCS 2248, Berlin: Springer-Verlag, 2001. 552−565. [doi: 10.1007/3-540-45682-1_32]

[11] Boyen X. Mesh signatures. In: Naor M, ed. Advances in Cryptology—EUROCRYPT 2007. LNCS 4515, Berlin: Springer-Verlag, 2007. 210−227. [doi: 10.1007/978-3-540-72540-4_12]

[12] Li J, Au MH, Susilo W, Xie DQ, Ren K. Attribute-Based signature and its applications. In: Feng DG, ed. Proc. of the 5th ACM Symp. on Information, Computer and Communications Security. New York: ACM, 2010. 60−69. [doi: 10.1145/1755688.1755697]

[13] Maji HK, Prabhakaran M, Rosulek M. Attribute-Based signatures. In: Kiayias A, ed. Topics in Cryptology—CT-RSA 2011. Berlin: Springer-Verlag, 2011. 376−392. [doi: 10.1007/978-3-642-19074-2_24]

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

[15] Boneh D, Boyen X. Efficient selective-ID secure identity-based encryption without random oracles. In: Cachin C, Camenisch JL, eds. Advances in Cryptology—EUROCRYPT 2004. LNCS 3027, Berlin: Springer-Verlag, 2004. 223−238. [doi: 10.1007/978-3-540-24676-3_14]

[16] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof-systems. In: Sedgewick R, ed. Proc. of the 17th Annual ACM Symp. on Theory of Computing. New York: ACM, 1985. 291−304. [doi: 10.1145/22145.22178]

[17] Camenisch J. Group signature schemes and payment systems based on the discrete logarithm problem [Ph.D. Thesis]. Zurich: ETH Zurich, 1998.

附录 A:方案正确性验证

证明:本方案的正确性可通过以下等式得到验证,其中 I 为用户凭证的真实签发权威:

$$\prod_{i\in L} e(S_i,(h(\omega\|i)P_2+P_{pubi})$$
$$=e(S_I,(h(\omega\|I)P_2+P_{pubI})\cdot\prod_{i\in L,i\neq I} e(S_i,(h(\omega\|i)P_2+P_{pubi})$$
$$=e(sP_1-s\sum_{i\in L,i\neq I} a_i(h(\omega\|i)P_1+\psi(P_{pubi})),h(\omega\|I)P_2+P_{pubI})\cdot\prod_{i\in L,i\neq I} e(s\cdot a_i(h(\omega\|I)P_1+\psi(P_{pubi})),h(\omega\|i)P_2+P_{pubi})$$
$$=e(sP_1-s\sum_{i\in L,i\neq I} a_i(h(\omega\|i)+x_i)P_1,(h(\omega\|I)+x_I)P_2)\cdot\prod_{i\in L,i\neq I} e(s\cdot a_i(h(\omega\|I)+x_I)P_1,(h(\omega\|i)+x_i)P_2)$$
$$=e(sP_1-s\sum_{i\in L,i\neq I} a_i(h(\omega\|i)+x_i)P_1,(h(\omega\|I)+x_I)P_2)\prod_{i\in L,i\neq I} e(sa_i(h(\omega\|I)+x_I)P_1,(h(\omega\|i)+x_i)P_2)$$
$$=e(sP_1-s\sum_{i\in L,i\neq I} a_i(h(\omega\|i)+x_i)P_1,(h(\omega\|I)+x_I)P_2)\prod_{i\in L,i\neq I} e(sa_i(h(\omega\|i)+x_i)P_1,(h(\omega\|I)+x_I)P_2)$$
$$=e(sP_1-s\sum_{i\in L,i\neq I} a_i(h(\omega\|i)+x_i)P_1,(h(\omega\|I)+x_I)P_2)\cdot e(s\sum_{i\in L,i\neq I} a_i(h(\omega\|i)+x_i)P_1,(h(\omega\|I)+x_I)P_2)$$
$$=e(sP_1,(h(\omega\|I)+x_I)P_2)$$
$$=e(s(h(\omega\|I)+x_I)P_1,P_2)$$
$$=e(T,P_2),$$

以及

$$e(T,f_1)^t=e(s(h(\omega\|I)P_1+\psi(P_{pubI})),s^{-1}t^{-1}(c_1+r_d d_1))^t=e((h(\omega\|I)+x_I)P_1,c_1+r_d d_1)$$
$$=e((h(\omega\|I)+x_I)P_1,\frac{P_2+uP_0+(r+r_d r_u)Q_\omega}{h(\omega\|I)+x_I})=e(P_1,P_2+uP_0+(r+r_d r_u)Q_\omega)$$
$$=e(P_1,P_2)\cdot e(P_1,P_0)^u\cdot e((r+r_d r_u)P_1,Q_\omega)=e(P_1,P_2)\cdot e(P_1,P_0)^u\cdot e(\psi((c_2+r_d d_2)P_2),Q_\omega)$$
$$=e(P_1,P_2)\cdot e(P_1,P_0)^u\cdot e(\psi(f_2),H(\omega)).$$

即

$$e(P_1,P_2)\cdot e(\psi(f_2),H(\omega))=e(T,f_1)^t\cdot e(P_1,P_0)^{-u}.$$ □

附录 B:定理 1 的证明

证明:假设存在敌手 F 可以 (t,q_I,q_H,ε)-破坏本文中所描述的凭证方案,则我们可以使用 F 构造算法 A 解决 q_I-BCAA1 问题.

对于 $x\in Z^*_p$, $P_2\in G^*_2, P_1=\psi(P_2)$, $e:G_1\times G_2\to G_T$ 和给定的 $\left(P_1,P_2,Q=xP_2,h_0,\left(h_1,\frac{P_2}{h_1+x}\right),\ldots,\left(h_{qI},\frac{P_2}{h_{qI}+x}\right)\right)$ ($h_0\sim h_{qI}$ 为 Z^*_p 中 q_I+1 个互不相同的元素),算法 A 的目的是计算与 h_0 对应的值 $e(P_1,P_2)^{1/(h_0+x)}$,其中 $h_0\notin\{h_1,\ldots,h_{qI}\}$.

系统建立:A 选择足够长度的安全参数 1^λ,然后从 Z^*_p 中随机选择 a_0 并设置 $P_0=a_0P_2$,接下来 A 执行方案中的 Setup 步骤获取其他公共参数,保留公共参数 *params* 并将其发送给 F.此外,A 还需要预先随机选择 q_H 个杂凑函数查询结果 $\{v_1,\ldots,v_{qH}\}$, $\{h_1,\ldots,h_{qI}\}$ 随机分布在这些结果中.

签发者生成:A 从 Z_p 中随机选择 $a_1,\ldots,a_n,b_1,\ldots,b_n$,$n$ 为作为挑战的签发者集合 L^*中元素个数,A 令签发者公钥 $P_{pubIj}=a_jQ+b_jP_2(j=1,\ldots,n)$,并将 $\{P_{pubI1},\ldots,P_{pubIn}\}$ 发送给 F.

杂凑函数查询:对于第 m 次杂凑函数查询,若其输入值已经询问过,则 A 返回已记录的杂凑函数值,否则假设其输入为 $\omega\|i$,若 $\omega\neq\omega^*$,则 A 从 G_2 中随机选择 Q_ω 并返回 $h(\omega\|i)=a_iv_m-b_i, H(\omega)=Q_\omega$.若 $\omega=\omega^*$,则 A 返回结果 $h(\omega^*\|i)=a_ih_0-b_i$ 以及 $H(\omega^*)=h^*(h_0P_2+Q)$,其中 h^* 为 Z_p 中随机元素.然后 A 记录返回的杂凑函数值.

在上述查询过程中,由于 $a_1,\ldots,a_n,b_1,\ldots,b_n$, $\{v_1,\ldots,v_{qH}\}$, h_ω 和 h^* 为随机选择的元素,因此 F 无法分辨该结果是由 A 生成的还是由随机预言机产生的.

凭证签发查询:对于输入 ω,u 及对应的签发者 I,A 查找 $h(\omega\|I)$ 及对应的 v_m,若对于某个值 $j, v_m=h_j$,则 A 随机选择 $\tilde{r},\tilde{r}_u\in Z^*_p$ 并令 $r=(h_j+x)\tilde{r}, r_u=(h_j+x)\tilde{r}_u$,则 A 可以模拟计算:

$$c_1=\frac{P_2+uP_0+rH(\omega)}{h(\omega\|I)+x_I}=\frac{1+ua_0}{a_I}\cdot\frac{P_2}{h_j+x}+\frac{\tilde{r}Q_\omega}{a_I},d_1=\frac{r_uH(\omega)}{h(\omega\|I)+x_I}=\frac{\tilde{r}_uQ_\omega}{a_I},$$

$$c_2=\tilde{r}h_jP_2+\tilde{r}Q,d_2=\tilde{r}_uh_jP_2+\tilde{r}_uQ,$$

并输出 $cre=(c_1,c_2,d_1,d_2)$.否则,A 输出错误并中止.

输出.最终,F 输出一个伪造的证明 $a^*=(S^*,T^*,f_1^*{}_1,f_2^*)=(\{S_1^*,...,S_n^*\},T^*,f_1^*,f_2^*)$, 其相应的签发者公钥为 $\{P_{pubI1},...,P_{pubIn}\}$.

根据凭证方案的校验算法可知:

$$\prod_{i=1}^{n}e(S_i^*,h(\omega^*\|i)P_2+P_{pubIi})=e(T^*,P_2).$$

因此,

$$e(T^*,P_2)=\prod_{i=1}^{n}e(S_i^*,h(\omega^*\|i)P_2+P_{pubi})=\prod_{i=1}^{n}e(S_i^*,a_ih_0P_2+a_ixP_2)=\prod_{i=1}^{n}e(a_i(h_0+x)S_i^*,P_2)=e((h_0+x)\sum_{i=1}^{n}a_iS_i^*,P_2),$$

$$T^*=(h_0+x)\sum_{i=1}^{n}a_iS_i^*.$$

此外,对于知识证明 Π ,A 可以使用与之对应的知识抽取器从中恢复知识 (t^*,u^*) .因为知识证明方案的正确性, (t^*,u^*) 满足 $e(T^*,f_1^*{}_1)^{t^*}=e(P_1,P_2)\cdot e(P_1,P_0)^{u^*}\cdot e(\psi(f_2^*),H(\omega^*))$, 所以 A 可以计算:

$$\begin{aligned}\Phi&=\frac{e\left(\sum_{i=1}^{n}a_iS_i^*,f_1^*{}_1\right)^{t^*}}{e(\psi(f^*{}_2),h^*P_2)}\\&=\frac{e(T^*,f_1^*{}_1)^{t^*/(h_0+x)}}{e(\psi(f^*{}_2),h^*P_2)}\\&=\frac{e(P_1,P_2)^{1/(h_0+x)}e(P_1,u^*P_0)^{1/(h_0+x)}e(\psi(f^*{}_2),H(\omega^*))^{1/(h_0+x)}}{e(\psi(f^*{}_2),h^*P_2)}\\&=\frac{e(P_1,P_2+u^*P_0)^{1/(h_0+x)}e(\psi(f^*{}_2),h^*(h_0P_2+Q))^{1/(h_0+x)}}{e(\psi(f^*{}_2),h^*P_2)}\\&=\frac{e(P_1,P_2+u^*P_0)^{1/(h_0+x)}e(\psi(f^*{}_2),h^*(h_0+x)P_2)^{1/(h_0+x)}}{e(\psi(f^*{}_2),h^*P_2)}\\&=\frac{e(P_1,P_2+u^*P_0)^{1/(h_0+x)}e(\psi(f^*{}_2),h^*P_2)}{e(\psi(f^*{}_2),h^*P_2)}\\&=e(P_1,P_2+u^*P_0)^{1/(h_0+x)}\\&=e(P_1,P_2+u^*a_0P_2)^{1/(h_0+x)}\\&=e(P_1,P_2)^{(1+u^*a_0)/(h_0+x)}.\end{aligned}$$

进一步计算 $\Phi^{1/(1+u\times a_0)}=e(P_1,P_2)^{1/(h_0+x)}$.至此,A 得到了 q_I-BCAA1 问题的一个解.在系统建立阶段,A 共需进行 1 次群 G 上的模乘运算;在签发权威生成阶段,需进行群 G 上的 $2n$ 次模乘运算和 n 次加法运算;在凭证签发阶段,需进行 Z_p 上的 $6q_I$ 次乘法运算、$2q_I$ 次加法运算和 $3q_I$ 次求逆运算,以及群 G 上的 $5q_I$ 次模乘运算、$2q_I$ 次加法运算.此外,在杂凑函数查询阶段,还需进行 Z_p 上的 q_H 次乘法运算和 q_H 次加法运算(对 h 的查询)以及群 G 上的 q_H+n 次模乘运算和 n 次加法运算(对 H 的查询);在输出阶段,最多需要进行 Z_p 上的 1 次乘法运算和 1 次加法运算,群 G 上的 n+2 次模乘运算和 n–1 次加法运算,以及群 G_T 上 1 次模乘运算,此外还需进行 2 次双线性映射.若将 G 与 G_T 中的模乘、加法运算所需时间记为 t_{Gsm},t_{Gadd},将 Z_p 中的乘法、加法和求逆运算所需时间记为 t_{mu},t_{add} 和 t_{inv},双线性映射所需时间记为 t_p, 则算法 A 所需时间 t' 至多为算法 F 所需运行时间加上 $(2q_I+3n-1)t_{Gsm}+(5q_I+q_H+4n+4)t_{Gadd}+(6q_I+q_H+1)t_{mu}+(2q_I+q_H+1)t_{add}+3q_It_{inv}+2t_p$, 即

$$t'\leqslant t+(2q_I+3n-1)t_{Gsm}+(5q_I+q_H+4n+4)t_{Gadd}+(6q_I+q_H+1)t_{mu}+(2q_I+q_H+1)t_{add}+3q_It_{inv}+2t_p.$$

至此,定理 1 成立. □

张严(1987－),男,北京人,博士生,主要研究领域为网络与系统安全.
E-mail: janian@tca.iscas.ac.cn

冯登国(1965－),男,博士,研究员,博士生导师,主要研究领域为信息安全,密码学.
E-mail: aqlsm@163.com

于爱民(1980－),男,博士,主要研究领域为可信计算,系统安全.
E-mail: yuaimin@tca.iscas.ac.cn