# 一种基于BB+签名的PBA方案

岳笑含 周福才 孙 玮
(东北大学信息科学与工程学院 沈阳 110819)

**摘 要** 在可信计算环境中,为了弥补原有可信计算组织(TCG)提出的二进制证明方案的缺陷,提出了一种新型的基于属性的证明(Property-Based Attestation,PBA)方案。首先介绍了基于属性的证明思想及其安全模型;然后基于改进的BB+签名技术给出了一个具体的基于属性的证明构造方案,并与其他方案在性能上进行了比较;最后在随机预言模型下证明了该方案具有配置隐私及不可伪造等安全性。

**关键词** 可信计算,基于属性的证明,BB+签名
**中图法分类号** TP309.7 **文献标识码** A

## Property-based Attestation Scheme Based on the BB+ Signature

YUE Xiao-han ZHOU Fu-cai SUN Wei
(College of Information Science and Engineering, Northeastern University, Shenyang 110819, China)

**Abstract** In trusted omputing environment, to solve the problem of binary attestation scheme proposed by the trusted computing group(TCG), this paper proposed a new property-based attestation scheme. Firstly, this paper introduced the ideas of PBA and the security model of PBA-BB+, secondly, based on improved BB+ signature technology, presented a concrete construction of PBA-BB+ scheme, and compared the scheme with other PBA schemes, finally, in oracle random model, proved the PBA-BB+ scheme meets configuration privacy and unforgeability.

**Keywords** Trusted computing, Property-based attestation, BB+ signature

随着计算机科学和网络技术飞速发展,人们对数据和平台的安全需求越来越高,而传统的安全措施所提供的保障能力是有限的。在这种情况下,计算机行业提出了可信计算(TC)技术,从而为软件及硬件都是新构架的新一代可信计算平台提供了安全基础,其中平台证明方案是可信计算技术的一项重要功能,该方案称作二进制证明方案[2]。在TCG[1]的平台二进制证明方案中,示证者P通过度量平台所有可执行代码,将其结果的哈希值(称作平台配置信息 Configuration Specification,CS)存储在TPM内部的PCR寄存器中,当需要向验证者V证明平台配置信息安全性时,用TPM的AIK私钥对PCR中配置信息的哈希值进行签名,然后发送给验证者V进行校验。但是这种方案本身有一定的缺陷:首先是校验过程中验证者负担过重并且可执行性差,因为验证者V要验证证明者P的平台配置信息是否可信,这需要在本地维护一个包含所有"可信"配置信息哈希值的数据库,然后将P的配置信息进行比较,除非在数据库里就说明信息可信,否则不可信。但是由于网络中各个平台的配置信息多种多样并且时时更新导致哈希值发生变化,会让验证者端维护这样一个数据库变得非常困难。其次,该方法会破坏平台的隐私性,示证者报告了自身系统中所拥有软、硬件的标识,敌手通过该标识得出该平台拥有的特性,并针对特征进行相应的攻击。

为了弥补二进制证明方案的缺陷,Sadeghi和Stueble在2004年提出了基于属性证明(Property- Based Attestation,PBA)的方案[3,13]。在这个方案中,验证者并不关心示证者平台的具体配置信息,而关心的是示证者平台的配置信息是否满足某种规定的属性(Property Specification,PS)。在基于属性的证明方案研究方面,比较有代表性的是:2006年,陈立群使用CL签名实现了基于属性证明方案[4],但是其使用CL签名是基于强RSA假设的,所以计算代价较大;2009年,秦等人利用PBA的思想提出了基于组件属性的远程证明[15];2010年,冯等人提出基于LRSW假设实现的属性认证方案[5],由于其中使用了大量的配对运算,因此方案中计算代价也相当大。针对计算代价较大的问题,本文提出了一种利用BB+签名[6-8]和零知识证明[12,14]实现的PBA-BB+方案,方案中对原有BB+签名进行了改进,而且总体方案在安全性与前面提出的PBA方案相同的情况下,其计算代价相对较小。本文的最后在随机预言模型下证明了方案的安全性并将其与其他PBA方案的性能进行了比较。

## 1 预备知识

### 1.1 双线性配对

双线性配对[11,13]是指两个循环群之间对应的线性映射关系,其构造过程如下:$G_1$ 和 $G_2$ 是两个阶为素数 $p$ 的循环乘法群,$g_1$ 和 $g_2$ 分别是 $G_1$ 和 $G_2$ 的生成元,$G_T$ 是群。$e$ 是一个

到稿日期:2011-09-22 返修日期:2012-02-17 本文受国家高技术研究发展计划(2009AA01Z122),辽宁省自然科学基金(20062023)资助。
岳笑含(1982-),男,博士生,主要研究方向为可信计算,E-mail:yxh21@yeah.net;周福才(1964-),男,教授,主要研究方向为网络与信息安全保障,E-mail:fczhou@mail.neu.edu.cn(通信作者);孙 玮(1987-),男,硕士生,主要研究方向为可信计算。

可计算的映射 $e:G_1\times G_2\to G_T$，该双线性映射具有下列属性：

(1)双线性：对于所有 $u\in G_1$，$v\in G_2$，$a,b\in Z$，有 $e(u^a,v^b)=e(u,v)^{ab}$ 成立；

(2)非退化性：$e(g_1,g_2)\neq 1$；

(3)可计算性：存在有效算法计算 $e(g_1,g_2)\neq 1$。

### 1.2 承诺

承诺[9]是隐藏签名者私有信息而使用的一种方法。用承诺对象与随机数混合计算得到承诺值，之后签名者用该承诺值代替承诺对象与其他人进行交互，并且此承诺值与承诺对象是一一映射关系，此后仲裁者可以打开承诺值，取得承诺对象即签名者私有信息。

本文使用的是 Pedersen 承诺方案。该方案中公钥 $g,h\in G$，其中 $G$ 的阶为素数 $q$，承诺密钥是随机数 $r\leftarrow Z_q$，对消息 $m\in Z_q$ 的承诺值为 $com=h^m g^r$，其中 $g$ 是循环群的生成元，$h$ 是循环群 $\langle g\rangle$ 中随机生成的。承诺方不知道 $\log_g h$，所以承诺在离散对数假设下完美地隐藏了消息并将消息与承诺 $com$ 进行了绑定。

### 1.3 BB+签名

BB+签名是由 Giuseppe Ateniese 等人[7]在原有 BB 签名[6]基础上做的改进，签名方案具体过程如下：

(1)初始化算法：输入安全参数 $1^k$，输出公共参数 $p,G_1,G_2,G_T,e,g_1,g_2$，其中 $g_1$ 和 $g_2$ 分别是 $G_1$ 和 $G_2$ 的生成元；输出公钥 $g_2^{sk}$，其中 $sk\in Z_p^*$ 为签名私钥；

(2)签名算法：输入私钥 $sk$ 及消息 $m$，并选择一个随机数 $r\in Z_p$，输出签名为 $\sigma=(g_2^r,g_1^{1/(sk+r)},g_1^{1/(r+m)})$；

(3)校验算法：输入签名 $\sigma$ 及公钥 $g_2^{sk}$ 并校验以下等式是否成立：

$$e(g_1^{1/(sk+r)},g_2^r\cdot g_2^{sk})=e(g_1,g_2)\wedge e(g_1^{1/(r+m)},g_2^r\cdot g_2^m)$$

以上 BB+签名方案在选择明文攻击下是存在性不可伪造的。

### 1.4 难题假设

**假设 1** $q$-Strong Diffie-Hellman Assumption($q$-SDH)。在群 $G$ 中的 $q$-SDH 假设定义如下：给定 $(q+1)$ 个元素的组 $(g,g^x,g^{(x^2)},\cdots,g^{(x^q)})$，没有概率多项式时间算法 A 以不可忽略的优势 $\varepsilon$ 生成一对 $(c,g^{1/(x+c)})$，即

$$\mathrm{Adv}_A^{q\text{-}SDH}=\Pr[(c,g^{1/(x+c)})\leftarrow A(g,g^x,g^{(x^2)},\cdots,g^{(x^q)})]<\varepsilon$$

**假设 2** Decision Linear Assumption(DLA)。给定任意生成元 $u,v,h\in G_1$ 及 $u,v,h,u^a,v^b,h^c\in G_1$ 作为输入，没有概率多项式时间算法 A 以不可忽略的优势 $\varepsilon$ 判定 $a+b$ 是否等于 $c$，即

$$\mathrm{Adv}_A^{q\text{-}SDH}=(\Pr[(c=a+b)\leftarrow A(u,v,h,u^a,v^b,h^c)]-\Pr[(c\neq a+b)\leftarrow A(u,v,h,u^a,v^b,h^c)])<\varepsilon$$

### 1.5 PBA-BB+方案的模型

PBA-BB+方案的参与者共 3 方：发行者 I 由一个可信第三方担任；示证者 P 是一个可信平台，包含 TPM(记作 M)和主机 H；以及验证者 V。方案主要分为 Setup、Issue、Sign、Verify、Check 5 个过程：

(1)Setup：输入安全参数 $1^k$，I 使用随机算法产生密钥对 $(isk,ipk,itk)$，其中 $isk$ 是发布者的密钥，$ipk$ 是包含全局公共参数的公钥，$itk$ 是追踪密钥，用于在 Check 阶段检查 P 是否拥有有效的属性证书。

(2)Issue：P 向 I 申请获得属性证书。TPM 芯片 M 安全地收集平台的配置信息 $cs$，并采用传统的传输方式；I 验证 $cs$ 满足属性 $ps$ 要求后，对 $(cs,ps)$ 进行签名产生签名密钥 $(B,C)$ 并颁发属性证书 $cred_{PBA}$；I 利用可信计算中密封的方式将 $cred_{PBA}$ 在 $cs$ 下的密封值发送给示证者 P；最后 P 验证证书的有效性。

(3)Sign：P 计算属性签名。为了保证方案的配置隐私性，TPM 芯片 M 对秘密值 $cs$ 计算承诺 $com$，并产生包含证明者随机数 $N_v$ 的 TPM 签名 $\sigma_M$；为了保证方案的匿名性，主机 H 将 $cred_{PBA}$ 中签名密钥加密，在通过构造零知识证明的方式，产生属性签名 $\sigma_{PBA}$，发送给验证者验证。

(4)Verify：V 验证属性签名正确性。主要验证以下几点：消息的新鲜性；消息是否由真实 TPM 产生；属性证书是否有效；当前示证者平台配置信息是否与属性证书中签名的 $cs$ 一致。

(5)Check：验证者通过在线可信第三方(即发行者 I)验证示证者 P 属性证书的有效性，即 P 的签名密钥 $(B,C)$ 的有效性。

### 1.6 PBA-BB+方案的安全模型

在安全性方面，PBA-BB+方案满足以下安全属性：正确性、不可伪造性、配置隐私性。

正确性：如果在示证者 P 和验证者 V 都是诚实的情况下，即 P 的配置属性对 $(cs_i,ps)\in CS$，P 的证书是有效的 $cred_{PBA}\notin CRL$，由 P 产生的属性签名 $\sigma_{PBA}$ 能够被验证者以压倒性概率成功接受，那么 PBA 方案是正确的，即

$$\Pr[(ipk,isk)\leftarrow Setup(1^k),(B_i,C_i,cred_{PBAi})\leftarrow Issue,(\sigma_{PBA})\leftarrow Sign(cs,B_i,C_i,ipk,N_v)\Rightarrow 1\leftarrow Verify(N_v,\sigma_{PBA},cred_{AIK},CRL)]=1$$

不可伪造性：设 $Game_A^{att\text{-}fg}(1^k)$ 是在示证者 P、验证者 V、发行者 I 以及敌手 A 之间交互运行的伪造攻击游戏。如果在示证者产生正确的属性签名之前，A 输出的 PBA 签名 $\sigma_{PBA}$ 能够成功被 V 接受，那么 A 赢得了游戏。A 赢得游戏的优势概率记作 $\mathrm{Adv}_A^{att\text{-}fg}(1^k)=\Pr[Game_A^{att\text{-}fg}(1^k)=win]$。假如不存在敌手在概率多项式时间内以不可忽略的概率 $\mathrm{Adv}_A^{att\text{-}fg}(1^k)$ 伪造属性签名，就说方案是不可伪造的。

配置隐私性：设 $Game_A^{cf\text{-}prv}(1^k)$ 是能够在示证者 P、验证者 V、发行者 I 以及敌手 A 之间交互运行的攻击游戏。定义 A 能够破坏属性 $ps$ 的 $n$ 对可能配置信息对 $(cs_i,ps)$ 的配置隐私性的优势概率为：$\mathrm{Adv}[A_{PBA}^{cf\text{-}prv}(1^k)]=|\Pr[b=j]-1/n|$。如果对于任何概率多项式时间敌手 A 在安全参数 $k$ 下 $\mathrm{Adv}[A_{PBA}^{cf\text{-}prv}(1^k)]$ 都是可忽略的概率，那么说方案具有配置隐私性。

## 2 PBA-BB+方案

### 2.1 初始化(Setup)算法

在 Setup 系统初始化中，$G_1,G_2$ 和 $G_T$ 是双线性循环群，$g_1,g_2,g_T$ 分别是其生成元，$e:G_1\times G_2\to G_T$；SDH 假设在 $(G_1,G_2)$ 中成立；$H:\{0,1\}^*\to Z_p$ 为哈希函数；随机选择 $u,v\in G_2$，$x,y\in Z_p$，使 $u^x=v^y=h$，其中 $(x,y)$ 为发行者 I 查询撤销密钥。$isk\leftarrow Z_p$ 为发行者 I 私钥，$w_1=g_1^{isk}\in G_1$，$\Omega=e(g_1,g_2)$，发行者 I 公钥为 $ipk=(g_1,g_2,g_T,u,v,h,w_1,\Omega)$。

### 2.2 发行(Issue)算法

(1)首先示证者 P 获得发行者 I 的 RSA 公钥 $pk_I$，将 $pk_I$

传给 TPM；TPM 用 $pk_I$ 对平台配置信息 $cs$ 和要申请的属性 $ps$ 进行加密得：$T=E(pk_I, cs \| ps)$，$cs\in Z_p$，$ps\in Z_p$；将 $T$ 和 TPM 的 AIK 证书 $cred_{AIK}$ 一起发给发行者 I 进行验证。

(2)发行者 I 收到来自示证者的请求信息后，首先用自己的 RSA 私钥解密 $T$ 得到示证者 P 平台配置信息 $cs$ 及 P 想要申请的属性 $ps$：$cs=D(sk_T, T)$；然后检查 $cs$ 值是否满足属性 $ps$ 的要求；如果满足则 I 利用 PBA 私钥 $isk$ 计算签名：选择一次性密钥 $r\in_R Z_p$，计算验证值 $w_2=g_1^{isk+r}$，$A=g_1^{ips+r}$，计算签名值 $B=g_2^{1/(isk+ips+r)}$，$C=g_2^{1/(\alpha+ps+r)}$。所以对 $(cs, ps)$ 的签名为 $\sigma=(B,C)$，属性证书为

$cred_{PBA}=(A, w_2, \sigma, ipk)$

(3)最后 I 在 $cred_{AIK}$ 中公钥 $pk_{AIK}$ 和 $cs$ 下密封证书 $S=seal(cs, pk_{AIK}, cred_{PBA})$，将密封值发送给示证者 P。

(4)示证者 P 收到来自 I 的密封值 S 直接发送给 TPM 验证；TPM 收到密封值 S 后首先解密封：$cred_{PBA}=unseal(cs, sk_{AIK}, S)$ 得到证书信息，然后利用属性证书 $cred_{PBA}$ 传给主机 H 验证其有效性。

(5)主机 H 利用 $cred_{PBA}$ 中的公钥信息 $ipk$ 验证证书中签名值是否正确，看下列等式是否成立：$e(w_1A, B)=\Omega$，$e(Ag_1^{cs}, C)=\Omega$。如果成立，说明证书有效，否则是无效证书，重新申请证书或者终止协议。

### 2.3 签名(Sign)算法

(1)当验证者 V 需要示证者 P 证明其平台安全性时，会产生一个随机数 $N_v\in Z_p^*$ 作为挑战发给示证者 P。P 收到随机数 $N_v$ 后传给 TPM；

(2)TPM 也为属性证明产生一个随机数 $N_t\in Z_p^*$；TPM 对配置信息 $cs$ 进行承诺：产生随机数 $r, r_0\in_R Z_p$，计算 $h_2=g_2^r\in G_2$，计算承诺 $com=g_2^{cs}h_2^{r_0}$；TPM 用 AIK 私钥产生一个 TPM 签名：$\sigma_M=Sign(sk_{AIK}, h_2 \| com \| N_v \| N_t)$；TPM 为主机加密选择参数并计算帮助值：选择随机数 $\alpha, \beta\in_R Z_p$；计算两个帮助值 $\delta_1=cs\cdot\alpha$，$\delta_2=cs\cdot\beta$；最后 TPM 将签名 $\sigma_M$、承诺 $com$、$h_2$、TPM 随机数 $N_t$、参数 $\alpha$、$\beta$，以及帮助值 $\delta_1$、$\delta_2$ 全部发送给主机 H。

(3)主机 H 对证书中签名值进行加密：计算加密值 $T_1=u^{\alpha}$，$T_2=v^{\beta}$，$T_3=B\cdot h^{\alpha+\beta}$，$T_4=C\cdot h^{\alpha+\beta}$。

(4)主机 H 按照下列步骤构造知识证明协议，满足下列等式：

$SPK\{(\alpha,\beta,cs,ps,\delta_1,\delta_2,com): T_1=u^{\alpha}\wedge T_2=v^{\beta}\wedge T_1^{cs}\cdot u^{-\delta_1}=1\wedge e(T_3,g_1)^{ps}e(h,w_2)^{-\alpha-\beta}\cdot e(h,g_1^{ps})^{-\alpha-\beta}=\Omega\cdot e(T_3,w_2)\wedge e(T_4,g_1)^{cs}e(h,A)^{-\alpha-\beta}\cdot e(h,g_1)^{-\delta_1-\delta_2}=\Omega\cdot e(T_4,A)\}(N_v \| N_t)$

主机随机选择随机数 $r_{\alpha}, r_{\beta}, r_{cs}, r_{ps}, r_{\delta_1}, r_{\delta_2}, r_{r_0}\in_R Z_p$，计算 $R_1=u^{r_{\alpha}}$，$R_2=v^{r_{\beta}}$，$R_3=e(T_3,g_1)^{r_{ps}}e(h,w_2)^{-r_{\alpha}-r_{\beta}}e(h,g_1)^{-r_{\alpha}-r_{\beta}}R_4=e(T_4,g_1)^{r_{cs}}\cdot e(h,A)^{-r_{\alpha}-r_{\beta}}\cdot e(h,g_1)^{-r_{\delta_1}-r_{\delta_2}}$，$R_5=T_1^{r_{cs}}\cdot u^{r_{\delta_1}}$，$R_6=T_2^{r_{cs}}\cdot v^{r_{\delta_2}}$，以及 $\tilde{C}_{com}=g_2^{r_{cs}}h_2^{r_{r_0}}$。

(5)主机 H 利用哈希函数的摘要值来盲化随机数：摘要值 $c$ 中包含属性信息 $ps$，承诺值 $com$，随机化后的承诺 $\tilde{C}_{com}$，验证者随机数 $N_v$，TPM 随机数 $N_t$，知识证明参数 $R_1, R_2, R_3, R_4, R_5, R_6$，所以 $c=H(ps \| com \| \tilde{C}_{com} \| R_1 \| R_2 \| R_3 \| R_4 \| R_5 \| R_6 \| N_v \| N_t)$，计算 $s_{\alpha}=r_{\alpha}+c\cdot\alpha$，$s_{\beta}=r_{\beta}+c\cdot\beta$，$s_{\delta_1}=r_{\delta_1}+c\cdot\delta_1$，$s_{cs}=r_{cs}+c\cdot cs$，$s_{r_0}=r_{r_0}+c\cdot r_0$。其中由于主机不知道平台配置信息 $cs$ 及承诺密钥 $r_0$，所以 $s_{cs}$，$s_{r_0}$ 是在 TPM 中计算的。

(6)最后主机 H 将属性签名 $\sigma_{PBA}$ 和 TPM 的 AIK 证书 $cred_{AIK}$ 一起发送给验证者 V，其中

$\sigma_{PBA}=(\sigma_M, T_1, T_2, T_3, T_4, c, s_{\alpha}, s_{\beta}, s_{cs}, s_{ps}, s_{\delta_1}, s_{\delta_2}, s_{r_0})$

### 2.4 验证(Verify)算法

(1)验证者 V 收到示证者的证明信息后，首先验证信息是否由真正的 TPM 产生并验证消息的新鲜性：验证者使用 $cred_{AIK}$ 中的 AIK 公钥验证 TPM 签名 $\sigma_M$，如果能得到正确的消息 $ipk, com, N_v, N_t$ 信息，则表示证明信息是由真实 TPM 产生的；然后验证得到的随机数 $N_v$ 是否是刚刚发送的挑战值，判断证明信息是否是新鲜的。

(2)承诺的正确性：$V$ 计算 $\hat{C}_{com}=(com)^{-c}g_2^{s_{cs}}h_2^{s_{r_0}}$。

(3)属性证书中 BB+签名的正确性：V 计算，

$\hat{R}_1=u^{s_{\alpha}}/T_1^c$，$\hat{R}_2=u^{s_{\beta}}/T_2^c$

$\hat{R}_3=e(T_3,g_1)^{s_{ps}}e(h,w_2)^{-s_{\alpha}-s_{\beta}}e(h,g_1^{ps})^{-s_{\alpha}-s_{\beta}}[e(T_3,w_2)/\Omega]^c$

$\hat{R}_4=e(T_4,g_1)^{s_{cs}}e(h,A)^{-s_{\alpha}-s_{\beta}}e(h,g_1)^{-s_{\delta_1}-s_{\delta_1}}[e(T_4,A)/\Omega]^c$

$\hat{R}_5=T_1^{s_{cs}}\cdot u^{s_{\delta_1}}$，$\hat{R}_6=T_2^{s_{cs}}\cdot v^{s_{\delta_2}}$

(4)验证等式是否成立：$c=H(ps \| com \| \hat{C}_{com} \| \hat{R}_1 \| \hat{R}_2 \| \hat{R}_3 \| \hat{R}_4 \| \hat{R}_5 \| \hat{R}_6 \| N_v \| N_t)$

### 2.5 撤销检查(Check)算法

(1)验证者将 $(T_1, T_2, T_3, T_4)$ 发送给发行者 I 检验其是否是已撤销的证书。

(2)I 首先计算 $B=T_3/(T_1^x\cdot T_2^y)$，$C=T_4/(T_1^x\cdot T_2^y)$，然后查询 $(B,C)$ 是否在撤销列表 CRL 中。如果不在 CRL 中，说明是有效的证书，并将结果发送给验证者 V。

## 3 安全性证明及安全性分析

### 3.1 安全性证明

本节在随机预言模型下证明方案的安全性，PBA-BW 方案必须满足以下的安全性质：正确性、不可伪造性及配置隐私性。根据本文第 2 节给出的基于属性证明的安全模型及相关假设定义，给出如下定理。

**Theorem 1**(正确性) PBA-BB+方案是正确的

证明：首先证明 PBA-BB+方案的正确性，一个有效的并且证书没有被撤销的示证者产生的签名能够被验证者成功接受即 $\hat{R}_1, \hat{R}_2, \hat{R}_3, \hat{R}_4, \hat{R}_5, \hat{R}_6$ 与 $R_1, R_2, R_3, R_4, R_5, R_6$ 相等：

$\hat{R}_1=u^{s_{\alpha}}/T_1^c=u^{r_{\alpha}+c\cdot\alpha}/u^{\alpha\cdot c}=u^{r_{\alpha}}=R_1$

$\hat{R}_2=v^{s_{\beta}}/T_2^c=v^{r_{\beta}+c\cdot\beta}/v^{\beta\cdot c}=v^{r_{\beta}}=R_2$

$\hat{R}_3=e(T_3,g_1)^{s_{ps}}\cdot e(h,w_2)^{-s_{\alpha}-s_{\beta}}\cdot e(h,g_1^{ps})^{-s_{\alpha}-s_{\beta}}\cdot[e(T_3,w_2)/\Omega]^c$

$=e(T_3,g_1)^{r_{ps}}\cdot e(T_3,g_1)^{c\cdot ps}\cdot e(h,w_2)^{-r_{\alpha}-r_{\beta}}\cdot e(h,w_2)^{c(-\alpha-\beta)}\cdot e(h,g_1^{ps})^{-r_{\alpha}-r_{\beta}}\cdot e(h,g_1^{ps})^{c(-\alpha-\beta)}\cdot[e(T_3,w_2)/\Omega]^c$

$=e(T_3,g_1)^{r_{ps}}\cdot e(h,w_2)^{-r_{\alpha}-r_{\beta}}\cdot e(h,g_1^{ps})^{-r_{\alpha}-r_{\beta}}\cdot[\Omega/$

$$e(T_3,w_2)]^c\cdot[e(T_3,w_2)/\Omega]^c$$
$$=e(T_3,g_1)^{r_{ps}}\cdot e(h,w_2)^{-r_\alpha-r_\beta}\cdot e(h,g_1^{ps})^{-r_\alpha-r_\beta}=R_3$$
$$\hat{R}_4=e(T_4,g_1)^{s_{cs}}e(h,A)^{-s_\alpha-s_\beta}e(h,g_1)^{-s_{\delta_1}-s_{\delta_1}}[e(T_4,A)/\Omega]^c$$
$$=e(T_4,g_1)^{r_{cs}}\cdot e(T_4,g_1)^{c\cdot cs}\cdot e(h,A)^{-r_\alpha-r_\beta}\cdot e(h,A)^{c(-\alpha-\beta)}\cdot e(h,g_1)^{-r_{\delta_1}-r_{\delta_2}}\cdot e(h,g_1)^{c(-\delta_1-\delta_2)}\cdot[e(T_4,A)/\Omega]^c$$
$$=e(T_4,g_1)^{r_{cs}}\cdot e(h,A)^{-r_\alpha-r_\beta}\cdot e(h,g_1)^{-r_{\delta_1}-r_{\delta_2}}\cdot[\Omega/e(T_4,A)]^c\cdot[e(T_4,A)/\Omega]^c$$
$$=e(T_4,g_1)^{r_{cs}}\cdot e(h,A)^{-r_\alpha-r_\beta}\cdot e(h,g_1)^{-r_{\delta_1}-r_{\delta_2}}=R_4$$
$$\hat{R}_5=T_1^{cs}/u^{s_{\delta_1}}=T_1^{cs}/u^{r_{\delta_1}}=R_5$$
$$\hat{R}_6=T_2^{cs}/v^{s_{\delta_2}}=T_2^{cs}/v^{r_{\delta_2}}=R_6$$

因此有$\hat{R}_1=R_1,\hat{R}_2=R_2,\hat{R}_3=R_3,\hat{R}_4=R_4,\hat{R}_5=R_5,\hat{R}_6=R_6$成立。

**Theorem 2**(不可伪造性) PBA-BB+方案提供不可伪造性。具体地说,签名机制的安全性是建立在SDH假设、TPM物理安全以及离散对数难题的基础上的。敌手应得游戏的优势概率为:

$$\mathrm{Adv}_A^{att\text{-}fg}(1^k)=\Pr[winG_0]\leqslant q^2/2^{l_\phi}+\varepsilon_{d\log}+\varepsilon_{TPM}+\varepsilon_{SDH}$$

式中,$q$是质询次数,$\varepsilon_{SDH}$是解决SDH难题的概率,$\varepsilon_{d\log}$是解决离散对数难题的概率。

证明:证明过程通过构造*Game*序列来完成,概率多项式时间(PPT)敌手A与模拟器S进行交互。在证明的过程中定义一序列游戏$Game_0,Game_1,\cdots,Game_n$(通过$G_i,i=0,\cdots,n$的形式来定义),其中$G_0$是$Game_A^{att\text{-}fg}$游戏。在每一个序列的游戏中,一个新的事件$S_i$会被引进到$G_i$中来。每当事件发生的时候,S中止。用$\Pr[winG_i]$来定义PPT敌手赢得游戏的概率。

$G_0$:$Game_A^{att\text{-}fg}$是最初的游戏,S通过模拟方案规范中诚实的一方来与A完成这个游戏。A选择一对配置属性对$(cs',ps')\notin CS$,其中$CS$是发行者I能够接受的满足属性$ps$要求的配置信息列表。S扮演诚实的TPM芯片M。A运行$Game_A^{att\text{-}fg}$游戏并输出属性签名$\sigma_{PBA}=(\sigma_M,T_1,T_2,T_3,s_1,s_2,s_{cs})$,希望S(扮演诚实的验证者)能够通过接受$\sigma_{PBA}$的证明来相信$(cs',ps')\in CS$,尽管实际上$(cs',ps')\notin CS$。因为$Game_A^{att\text{-}fg}$是$G_0$,所以定义A赢得这个游戏的概率$\Pr[winG_0]=\mathrm{Adv}_A^{att\text{-}fg}(1^k)$。

$G_1$:S扮演一个验证者来选择一个nonce $N_v$。定义事件$S_1$是在前面的方案中已经发送过挑战$N_v$。如果事件发生,S终止模拟。在这次通信中S记录所有的nonce。$N_v$作为S随机选择的挑战,概率$\varepsilon_1\leqslant q^2/2^{l_\phi}$,对于安全参数$l_\phi$来说这个概率可以忽略。因此$\Pr[G_0]\leqslant\Pr[G_1]+\varepsilon_1$。

$G_2$:S扮演可信芯片M,像之前一样模拟方案的执行部分,不同的是TPM签名$\sigma_M$从相应的签名语言机里获得。$G_2$中定义的事件$S_2$是S接收到来自A输出的$\sigma_{PBA}$,其中$\sigma_M$不是由S之前产生的,S终止模拟过程。这种情况下,A需要提供给S伪造的对配置信息的承诺$com$,以及伪造的TPM对签名$\sigma_M$。首先来看伪造承诺:$g_1^{cs}\cdot h_T^{r_0}=g_1^{cs'}\cdot h_T^{r_0'}$,因为$cs\neq cs'$,$r_0\neq r_0'$,所以敌手要计算离散对数$\log_{h_T}g_T=(cs'-cs)/(r_0-r_0')$;之后S模仿M伪造TPM签名,用到的AIK私钥$sk_{AIK}$是存在在TPM里的秘密值。假设解决离散对数难题的概率是$\varepsilon_{d\log}$,能破坏TPM芯片的概率是$\varepsilon_{TPM}$,则A赢得游戏的概率为

$$\Pr[winG_1]\leqslant\Pr[winG_2]+\varepsilon_1+\varepsilon_{d\log}+\varepsilon_{TPM}$$

$G_3$:S扮演主机H来模拟方案规定中的证明阶段,所有的属性签名都是从签名语言机中获得。定义事件$S_3$为S收到来自A的属性签名$\sigma_{PBA}$,但并不是S之前产生的,这时S终止模拟过程。A想要在$G_3$中赢得游戏需要伪造属性证书$cred_{PBA}$以及对$cred_{PBA}$中签名密钥的线性加密(LE)。$cred_{PBA}$中由I颁发给示证者P的签名密钥$(B,C)$是由基于$q$-SDH假设的改进BB+签名产生的。所以假设$\varepsilon_{SDH}$是解决SDH假设的概率,那么A赢得游戏$G_3$的概率为$\Pr[winG_3]=\varepsilon_{SDH}$。

所以敌手总的优势概率为$\mathrm{Adv}_A^{att\text{-}fg}(1^k)=\Pr[winG_0]\leqslant q^2/2^{l_\phi}+\varepsilon_{d\log}+\varepsilon_{TPM}+\varepsilon_{SDH}$。因此在TPM物理上是安全的、基于SDH假设的BB签名是安全的以及离散对数难题成立的情况下,A成功伪造的概率可以忽略不计。

**Theorem 3**(配置隐私性) PBA-BB+方案提供配置隐私性的安全属性。具体地说,如果敌手A能以不可忽略的概率区分来自同一属性的不同配置信息,那么一定存在一个多项式时间模拟器S能够以不可忽略的概率破坏承诺隐藏信息的机制。

证明:构造一个模拟器S扮演方案中任何诚实的一方来与敌手A进行$Game_A^{cf\text{-}prv}(1^k)$游戏。用下面的过程来证明敌手赢得游戏的最优概率$\mathrm{Adv}_A^{cf\text{-}prv}(1^k)$是可忽略的,尽管敌手拥有不受限制的计算能力。

将承诺值$com=g_1^{cs}\cdot h_T^{r_0}$给模拟器S,其中$cs\in CS$,S与A进行$Game_A^{cf\text{-}prv}$游戏。S通过send询问从A得到nonce$N_v$,自己产生一个nonce $N_t$,然后使用$C$作为TPM的承诺执行PBA方案(不知道$cs$和$r_0$),创建一个TPM签名$\sigma_M=Sign(sk_{AIK},h_T\|com\|N_v\|N_t)$。因为S的计算能力是无限的,所以它可以计算$\varepsilon$值,使$g_T=h^\varepsilon \bmod P$,并计算$k$值,使$com=h_T^k=h_T^{cs+r_0\cdot\varepsilon}$,尽管S既不知道$cs$也不知道$r_0$,但是可以在属性证书列表中找到同一个目标属性对应的证书$cred_{PBAi}$,建立$n$个等式:$k=cs_j+\varepsilon\cdot r_{0j}$,其中$j=1,\cdots,n$,然后对每个属性证书$cred_{PBAi}$计算出$n$个配置及承诺密钥对$(cs_j,r_{1j},r_{2j})$,计算属性签名$\sigma_{PBA}^{(i)}=(\sigma_M^{(i)},T_1^{(i)},T_2^{(i)},T_3^{(i)},s_1^{(i)},s_2^{(i)},s_{cs}^{(i)})$,发送给A。

在游戏的最后,A输出$j$,如果$cs_j=cs$,则S可以用$(cs_j,r_{1j},r_{2j})$打开承诺$C_1,C_2$。A能够判断$cs_j=cs$的概率取决于S破坏承诺的概率,所以如果S能够以不可忽略的概率打开承诺,那么A赢得游戏$Game_A^{cf\text{-}prv}(1^k)$的概率$\mathrm{Adv}_A^{cf\text{-}prv}(1^k)$也是不可忽略的。

### 3.2 性能分析

在本节中首先通过PBA-BB方案的计算代价和签名长度两方面来分析方案的性能。

首先比较PBA-BB+方案与其他方案的计算代价,本文基于双线性配对的幂运算(exponentiation)和配对运算(pairing)来计算方案代价,幂运算一般分为单次幂运算和多次幂运算。为了能够衡量证明过程中的计算量,在分析的过程中将方案的单次幂运算用符号$S$来表示,多次幂运算用符号$M$来表示,配对运算用符号$P$来表示。另外对于PBA-CL方

案，由于其基于的是一般群中的指数运算，因此同上规定方法，令 $S^*$ 和 $M^*$ 分别表示在一般群中的单次幂运算及多次幂运算，在一般群中的幂运算代价要远大于在双线性群中的运算代价[5]，与一次配对运算代价相当。PBA-BB+方案及其它属性证明方案的计算代价如表1所列。

表1 PBA-BB+与其他方案的性能比较

| 方案 / 算法 | PBA-CL[4] | PBA-BM[5] | PBA-BB |
|---|---|---|---|
| Issue | 2M* | 3S+1M+4P | 4S+2P |
| Sign | 2S* +3M* | 9S+3M+4P | 7S+4M+2P |
| Verify | 2M* | 4M+7P | 7M+2P |
| Revoke | (k+3)S* + (3k+4)M* | M | 2S |
| 总体代价 | (k+5)S* + (3k+11)M* | 12S+9M+15P | 13S+11M+6P |

其次比较各方案的签名长度。定义各属性证明方案的签名长度。对于基于双线性配对的方案，系统一般选择的是椭圆曲线 $E(Fq)(|q|=170)$，所以在群 $G$ 和群 $G_T$ 中的元素大小分别为171bits和1020bits，因此其安全参数为：$l_p(170)$，$l_H(160)$，$l_\phi(80)$。对于本方案，PBA签名中包含一个TPM签名 $\sigma_M$、4个 $G_2$ 中元素、一个哈希值、7个 $Z_p^*$ 中元素。TPM签名长度一般为512bit，所以签名总长度为2717bit；同理对于PBA-BM方案，其签名长度为3397bit；对于PBA-CL方案，其签名长度[4]为9210bit。

综上可以看出，PBA-BB+在运算代价及签名长度方面均小于以上的其他方案。

**结束语** 本文提出了一个全新的属性证明方案，给出了具体的构造，并在随机预言模型下证明了其安全性。通过与其他属性证明方案的比较可以明显地看到，本文提出的PBA-BB方案计算代价明显小于其他的属性证明方案。在未来的工作中，将进一步提高方案的性能，使其更符合实际应用的需求。

## 参考文献


[1] Trusted Computing Group. TPM Main Part 1, Design Principles Specification, Version 1.2 Revision 62[EB/OL]. https://www.trustedcomputinggroup.org/home

[2] Jaeger T, Sailer R, Shankar U. PRIMA: policy-reduced integrity measurement architecture[C]// Proc. of the 11th ACM Symposium on Access Control Models and Technologies. New York, 2006: 19-28

[3] Sadeghi A, Stuble C. Property-based attestation for computing platforms: caring about properties, not mechanisms [C]// Proc. of the 2004 Workshop on New Security Paradigms. Nova Scotia: ACM, 2004: 67-77

[4] Chen Li-qun, Landfermann R, Lohr H, et al. A protocol for property-based attestation[C]// Proc. of the first ACM workshop on Scalable trusted computing. New York: ACM, 2006: 7-16

[5] Feng Deng-guo, Qin Yu. A property-based attestation protocol for TCM [J]. Science China (Information Sciences), 2010, 53(3): 454-464

[6] Boneh D, Boyen X. Short signatures without random oracles[C]// Cachin C, Camenisch J L, eds. EUROCRYPT 2004. LNCS, vol. 3027, Heidelberg, Springer Press, 2004: 56-78

[7] Ateniese G, Camenisch J, Hohenberger S, et al. Practical Group Signatures without Random Oracles [EB/OL]. Cryptology ePrint Archive, Report 2005/385, 2005, http://eprint.iacr.org/

[8] Boneh D, Boyen X, Shacham H. Short Group Signatures[C]// Franklin M, ed. Proc. of CRYPTO 2004. LNCS, vol 3152, Heidelberg, Springer Press, 2004: 41-55

[9] Pedersen T P. Non-interactive and information-theoretic secure verifiable secret sharing[C]// Feigenbaum J, ed. Proc. of CRYPTO'91. LNCS, vol 576, Berlin: Springer-Verlag, 1992: 129-140

[10] Jens G. Simulation-sound NIZK proofs for a practical language and constant size group signatures[C]// Proc. of ASIACRYPT' 2006. Shanghai, 2006: 444-459

[11] Neal K, Alfred M. Pairing-based cryptography at high security levels[C]// Proc. of the 10th IMA International Conference on Cryptography and Coding. LNCS, vol 3796, Berlin: Springer, 2005: 13-36

[12] Mao Wen-bo. Modern Cryptography: Theory and Practice [M]. New Jersey: Prentice Hall Press, 2003

[13] Poritz J, Herreweghen V, et al. Property Attestation- Scalable and Privacy-friendly Security Assessment of Peer Computers [R]. RZ 3548. IBM Press, 2004

[14] Fiat A, Shamir A. How To Prove Yourself: Practical Solutions to Identification and Signatrue Problems[C]// Proc. of CRYPTO'86. LNCS, vol 263, Berlin: Springer-Verlag, 1986: 186-194

[15] 秦宇，冯登国. 基于组件属性的远程证明[J]. 软件学报，2009，20(6)：1625-1641


(上接第7页)


[29] Cohn D, Chang H. Learning to probabilistically identify authoritative documents [C]// Citeseer. 2000: 167-174

[30] Erosheva E, Fienberg S, Lafferty J. Mixed-membership models of scientific publications [J]. Proceedings of the National Academy of Sciences of the United States of America, 2004, 101: 5220-5233

[31] Nallapati R M, Ahmed A, Xing E P, et al. Joint latent topic models for text and citations [C]// ACM. 2008: 542-550

[32] Yang T, Chi Y, Zhu S, et al. Directed network community detection: A popularity and productivity link model [C]// SDM. 2010: 742-753

[33] Yang T, Jin R, Chi Y, et al. Combining link and content for community detection: a discriminative approach [C]// KDD. 2009: 927-936

[34] Yang T, Jin R, Chi Y, et al. A Bayesian framework for community detection integrating content and link [C]// BUAI. 2009: 615-622

[35] Hofmann T. Probabilistic latent semantic indexing [C]// ACM. 1999: 50-57

[36] Rissanen J. Modeling by shortest data description [J]. Automatica, 1978, 14(5): 465-471