# 基于可信芯片的终端平台匿名身份建立方法研究

于爱民 初晓博 冯登国

(中国科学院软件研究所信息安全国家重点实验室 北京 100190)
(中国科学院信息安全共性技术国家工程研究中心 北京 100190)

**摘 要** 文章针对当前基于隐私 CA(Privacy CA)的平台身份建立方案和 DAA(直接匿名证明)方案应用于网络终端平台身份管理时存在的两个问题:EK(Endorsement Key)证书管理复杂以及与传统基于管理员身份的终端管理方案未有效结合,无法支持基于管理员的平台身份撤销,提出了改进的基于可信芯片的网络终端平台身份管理方案.该方案包括平台 EK 产生、平台匿名身份建立、身份撤销、身份认证时的安全协议定义,利用了零知识证明以及基于 ID 的加密机制,有效解决了上述问题.同时在随机预言机模型下,作者还给出了该方案的正确性、匿名性以及不可伪造性的安全性证明.

**关键词** TPM/TCM;平台匿名身份;可信网络连接
**中图法分类号** TP309 **DOI 号**: 10.3724/SP.J.1016.2010.01703

# Research of Platform Anonymous Identity Management Based on Trusted Chip

YU Ai-Min CHU Xiao-Bo FENG Deng-Guo

(*State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing* 100190)
(*National Engineering Research Center of Information Security, Chinese Academy of Sciences, Beijing* 100190)

**Abstract** TPM/TCM-Based platform identity management is the base to construct TNC (trusted network connect). However there are two problems when managing platform identity of the network terminals using privacy-CA and DAA (direct anonymous attestation) approaches. The first one is that it is hard to manage EK certificate of TPM/TCM, especially in large scale networks. Secondly traditional administrator-based terminal management can not be combined with the approaches based on TPM/TCM. The paper proposes an improved approach to manage terminal platform identity based on TPM/TCM. It defines the protocols to issue EK, establish platform anonymous identity, revoke platform identity, and authenticate platform identity. Moreover the security of this approach is proven under RO (random oracle) model.

**Keywords** TPM/TCM; platform anonymous identity; trusted network connect

## 1 引 言

随着网络技术的不断发展和网络规模的持续扩大,实现随时随地的网络接入逐渐成为现实.然而,随之而来的一个安全威胁是现代网络环境下用户可能使用各类终端设备(手机、笔记本等)实施网络访问,如果终端设备不安全,则很有可能导致用户或者服务提供者的秘密信息遭到窃取或篡改.例如,公司开发人员通过公共网吧或者个人电脑访问公司的代

收稿日期:2010-04-14;最终修改稿收到日期:2010-08-09.本课题得到国家科技支撑计划(2008BAH22B06)、国家"八六三"高技术研究发展计划项目基金(2007AA01Z412)和中国科学院知识创新工程领域前沿项目(ISCAS2009-DR14,ISCAS2009-GR)资助.**于爱民**,男,1980 年生,博士研究生,主要研究方向为可信计算与系统安全.E-mail: yuaimin@is.iscas.ac.cn. **初晓博**,男,1984 年生,博士研究生,主要研究方向为可信计算与系统安全. **冯登国**,男,1965 年生,博士,研究员,博士生导师,主要研究领域为网络和信息安全.

码服务器就有可能造成公司软件代码的泄露.针对这种威胁,对终端设备进行有效的管理,为接入网络的终端设备建立平台身份,在网络活动中对终端平台进行身份认证就成为网络安全的研究热点之一.

目前,基于 TPM/TCM[1-2] 等可信芯片为终端设备建立身份已得到了工业界和学术界的普遍重视和深入研究,部分研究结果也以规范标准的形式被相关国际及国内研究机构和组织制定和发布.该类方法的基本思路是生产商为每个终端设备硬件绑定一个可信计算芯片 TPM/TCM,每个芯片内嵌一个唯一的公私钥对 EK(Endorsement Key),由芯片对私钥部分实施硬件级保护,公钥部分由生产商通过公钥证书的形式发布.当需要为终端建立身份时,首先利用 EK 与负责颁发平台身份证书的身份权威(又称隐私 CA,Privacy-CA)建立认证信道,通过该信道隐私 CA 确认当前终端设备是由可信的终端厂商生产,并且与一个硬件安全的可信计算芯片 TPM/TCM 相绑定.然后 TPM/TCM 将产生一对称为 AIK(PIK)的公私钥对,将公钥通过认证信道发送给隐私 CA.由隐私 CA 为其生成 AIK(PIK)的公钥证书,则该 AIK(PIK)证书即成为该平台的身份证书.在网络活动中,验证者可以通过 AIK(PIK)证书确认终端设备已具有身份权威颁发的合法身份.在上述身份建立过程中,对应一个 EK,隐私 CA 可通过颁发多个 AIK(PIK)证书给该平台,使得在网络活动中验证者无法唯一确定终端平台身份,一定程度上保证了终端的隐私性.然而该方案的最大缺点在于无法防止当隐私 CA 被攻破或者与验证者合谋时,验证者可以将同一终端发生的多次网络交易进行关联或者唯一性确定当前通信终端,从而侵犯终端的隐私性.

针对这一问题,Brickell 等人提出了直接匿名证明方案(Direct Anonymous Attestation,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各种直接匿名证明协议[4-7].DAA 方案的主要思想是通过零知识证明机制,使得终端设备向验证者证明身份时,无需出示由身份权威签发的平台身份证书,从而保证了验证方无法与身份权威合谋从而侵犯终端平台的隐私性.然而,利用现有 DAA 方案实施终端平台身份管理在实际应用时仍然存在以下不足:

(1)EK 证书管理复杂.在上述隐私 CA 方案或者 DAA 方案中,为了建立平台身份,终端设备都需要利用 TPM/TCM 中的 EK 私钥与负责颁发平台身份证书的身份权威建立认证信道.然而在一个大型网络中(例如某跨国公司的私有网络),由于网络中的终端设备(个人 PC/便携电脑等)众多,如何对众多设备的 EK 证书实施有效管理变得十分复杂.

(2)无法与传统的基于管理员身份的终端管理方法有效结合.考虑现有方案应用于银联网络对于移动 POS 机终端的管理.基于金融安全考虑,银联要求只有可信厂商生产的 POS 机才能获得身份凭证;同时为了保证其自身利益,银联需要对发给各个商户的移动 POS 机数量进行管理.对于商户,为了防止竞争对手获取其经营信息,其需要保证每笔交易的隐私性,即任何一方无法将某一 POS 发生的交易进行关联分析.对于上述银联需求,现有方案中基于 EK 建立认证信道可以保证移动 POS 机由可信厂商生产,通过利用用户认证技术验证当前为移动 POS 机申请平台身份的用户为被授权管理员可以实现对 POS 机数量的管理.对于商户需求,现有 DAA 方案可以满足隐私性需求.然而,当某些商户通过贿赂管理员或者由于管理员恶意行为导致为超出数量限制的 POS 机建立平台身份时,由于现有 DAA 方案平台身份的匿名性,即使银联事后发现某一管理员的该类行为,银联也无法对该管理员已颁发的 POS 机身份实施撤销.

针对上述问题,本文提出了新的 EK 证书颁发协议以及支持基于管理员身份增强的平台身份建立、撤销、认证协议,解决了 EK 证书过多带来的管理问题,实现了与传统基于管理员的终端管理方法的良好结合.此外,基于随机预言机(RO)模型[12],本文还对方案的安全性给出了详细的形式化证明.

本文第 2 节主要对本文中用到的一些基本概念给出了介绍;第 3 节给出整个方案的系统描述;第 4 节给出方案中的具体协议和机制描述;第 5 节对方案的安全性进行证明和分析;第 6 节将本文方案与现有主要方案进行功能与效率上的比较;第 7 节给出本文方案在可信网络接入系统中的应用;最后给出全文的总结以及下一步工作展望.

## 2 预备知识

本文主要用到以下基本概念.

**双线性映射**. 设 $G_1$,$G_2$ 为素数 $p$ 阶循环群,$g_1$ 和 $g_2$ 分别为群 $G_1$,$G_2$ 的生成元.如果映射 $e:G_1\times G_2\rightarrow G_T$ 满足如下条件,则称该映射为双线性映射,群 $(G_1,G_2)$ 被称为双线性群对.

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

(2) 非退化性. $e(g_1,g_2)\neq 1_{G_T}$ 并且 $e(g_1,g_2)$ 是 $G_T$ 的生成元.

(3) 可计算性. 对于任意 $u\in G_1, v\in G_2$, 存在有效算法计算 $e(u,v)$.

**$q$-SDH 问题及其困难性假设.**

$q$-SDH 问题. 对于素数 $p$ 阶循环群 $G_1, G_2, g_1$ 和 $g_2$ 分别为这两个群的生成元. 对于一个给定的 $(q+3)$ 元组 $(g_1, g_1^r, \cdots, g_1^{r^q}, g_2, g_2^r)$, 求二元组 $(g_1^{1/(r+x)}, x)$, 其中 $x\in Z_p^*$.

$q$-SDH 假设. 不存在多项式时间算法能以不可忽略的概率解决 $G_1, G_2$ 中的 $q$-SDH 问题.

**DDH 问题及其困难性假设.**

DDH 问题. 对于素数 $p$ 阶循环群 $G, g$ 为生成元. 对于元组 $(g,g^a,g^b,g^c)$ 作为输入, 当等式 $c=ab$ 成立时, 输出 1, 否则输出 0.

对于算法 $A$, 当下述条件满足时我们称其解决 DDH 问题具有优势 $\varepsilon$.

$$|\Pr[g,a,b: A(g,g^a,g^b,g^{ab})=1]-\Pr[g,a,b: A(g,g^a,g^b,g^c)=1]|\geq\varepsilon.$$

DDH 假设. 不存在多项式时间算法能以不可忽略的优势解决 DDH 问题.

**BBS$^+$ 签名方案**[8].

BBS$^+$ 签名方案是基于双线性映射设计的一个高效的签名算法, 该方案主要包括以下算法.

密钥创建. 选择 $p$ 阶双线性群对 $(G_1,G_2)$, 构造双线性映射 $e: G_1\times G_2\rightarrow G_T$. 选择 $g_0,\cdots,g_{L+1}$ 为群 $G_1$ 的生成元, $h_0$ 为 $G_2$ 的生成元. 随机选择 $r\in Z_p^*$, 计算 $w=h_0^r$, 则私钥 $SK=r$, 公钥 $PK=\{g_0,\cdots,g_{L+1},h_0,w\}$.

签名. 对于消息 $(m_1,\cdots,m_L)\in Z_p^L$, 选择 $e$ 和随机数 $s$, 计算 $A=(g_0g_1^sg_2^{m_1}\cdots g_{L+1}^{m_L})^{1/(e+r)}$, 则 $(A,e,s)$ 即为消息 $(m_1,\cdots,m_L)$ 的签名.

验证. 对于消息 $(m_1,\cdots,m_L)\in Z_p^L$ 的签名 $(A,e,s)$, 当等式 $e(A,wh_0^e)=e(g_0g_1^sg_2^{m_1}\cdots g_{L+1}^{m_L},h_0)$ 成立时则签名正确.

**基于离散对数的知识证明.**

本文采用 Camenisch 和 Stadler 给出的标记法[9]来描述基于离散对数的零知识证明协议, 例如 $PK\{\alpha,\beta,\lambda: y=g^\alpha h^\beta\wedge\tilde{y}=\tilde{g}^\alpha\tilde{h}^\lambda\wedge(u\leq\alpha\leq v)\}$ 表示"关于整数 $\alpha,\beta,\lambda$ 的零知识证明, 使得 $y=g^\alpha h^\beta, \tilde{y}=\tilde{g}^\alpha\tilde{h}^\lambda$ 成立, 并且 $u\leq\alpha\leq v$. 其中的 $y,g,h,\tilde{y},\tilde{g},\tilde{h}$ 是群 $G=\langle g\rangle=\langle h\rangle$ 和群 $\tilde{G}=\langle\tilde{g}\rangle=\langle\tilde{h}\rangle$ 中的元素. 根据 Fiat-Shamir 启发式[10]可以将零知识证明转化为对消息 $m$ 的知识签名, 对于每一个知识证明, 均采用固定的标记法来表示对应的知识签名. 例如, 对于上面的例子, 其对应的知识签名可以记作 $SPK\{\alpha,\beta,\lambda: y=g^\alpha h^\beta\wedge\tilde{y}=\tilde{g}^\alpha\tilde{h}^\lambda\wedge(u\leq\alpha\leq v)\}(m)$.

## 3　系统架构

基于可信芯片的终端平台身份构建系统架构如图 1 所示. 其中每个终端设备均包括主机及可信芯片 TPM/TCM, 两者由终端厂商通过硬件方式进行绑定. 身份权威负责对网络域中的终端实施平台身份管理, 例如银行网络域的身份权威负责对属于该网络的 ATM 机、POS 机等设备进行身份管理.

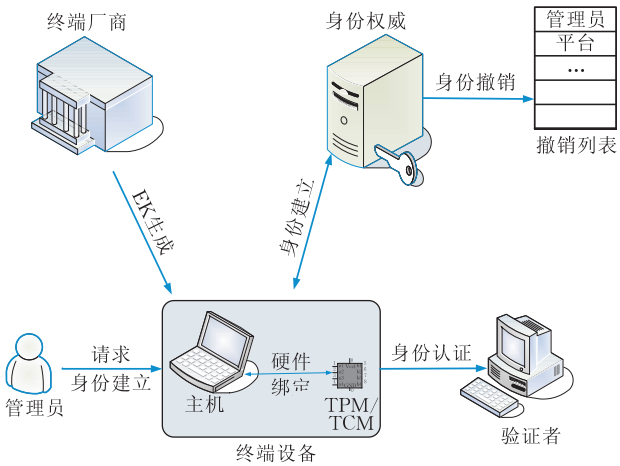



图 1　系统架构

本系统主要包括如下几项流程/功能:

(1) EK 生成. 利用该功能, 终端厂商完成终端设备生产时的 EK 公私钥产生, 并将该公私钥对注入 TPM/TCM 芯片, 由可信芯片为私钥部分提供硬件保护.

(2) 身份建立. 该过程完成终端设备在具体网络域中身份的建立. 当一个终端设备申请加入某网络域时, 网络管理员负责发起平台身份建立请求, 身份权威将认证该管理员是否具有相应权限, 该终端是否是由可信终端厂商生产. 在上述两步验证通过后, 身份权威为终端设备颁发平台身份凭证.

(3) 身份撤销. 当身份权威发现某终端的 TPM/TCM 芯片被破解或者某管理员不可信时, 将该终端的平台身份或者该管理员身份加入撤销列表.

(4) 身份认证. 网络通信中, 终端设备通过身份

认证向验证者证明其拥有身份权威颁发的合法平台身份,并且该平台身份以及负责为该终端申请平台身份的管理员身份未被撤销.

本文方案需要满足目前已有基于可信芯片的终端身份建立方法的安全性,同时解决第 1 节提到的新的管理和安全问题.具体来讲,本文方案在管理需求上要求 EK 证书管理简单,身份权威无需维护大量的 EK 证书.在安全需求上,需要满足如下安全定义:

身份建立的正确性.在身份建立阶段,如果终端设备由可信终端厂商生产,且为其申请身份的管理员具有相应权限,则该终端将获得身份权威颁发的平台身份.

身份认证的正确性.在身份认证过程中,如果终端已成功建立了平台身份,并且该平台身份或者申请身份的管理员身份未被撤销,则身份认证将成功.

身份建立的不可伪造性.在身份建立阶段,非可信终端厂商生产的设备或者不具有权限的管理员无法为终端设备获得平台身份凭证.

身份认证的不可伪造性.在身份认证过程中,未建立身份或身份已被撤销的终端设备无法通过身份认证.

终端匿名性.该安全要求包含匿名性与不可链接性两个方面.匿名性要求身份认证过程中验证者与身份权威合谋也无法唯一确定当前认证的终端设备,不可链接性要求验证者无法分辨多次身份认证过程是否来自于同一终端设备.

# 4 方案设计

本节给出本文方案所包含的具体安全协议和算法描述.

## 4.1 系统初始化

为了构建网络终端匿名身份管理系统,终端厂商和身份权威首先需要进行各自的初始化.

基于文献[11]中给出的加密方案,终端厂商 C 的系统初始化过程定义如下.

1. 选择双线性映射 $e_C:G_{C1}\times G_{C1}\rightarrow G_{C2}$.其中 $G_{C1}$ 为素数 $q$ 阶循环群.

2. 选择 Hash 函数 $H_1:\{0,1\}^*\rightarrow G_{C1}^*$, $H_2:G_{C2}\rightarrow\{0,1\}^n$, $H_3:\{0,1\}^n\times\{0,1\}^n\rightarrow Z_q^*$, $H_4:\{0,1\}^n\rightarrow\{0,1\}^n$.

3. 选定 $G_{C1}$ 的生成元 $g_{C1}$,生成随机数 $s\in Z_q^*$,计算 $P_{pub}=sg_{C1}$.

4. 生成公钥 $PK_C=\{q,G_{C1},G_{C2},e_C,n,g_{C1},P_{pub},H_1,H_2,H_3,H_4\}$并发布,存储并保护对应私钥 $SK_C=s$.

对于身份权威 I,其初始化过程定义如下:

1. 选择 $G_1,G_2,G_3$ 为素数 $p$ 阶循环群.$g_1,g_2,g_3$ 分别为群 $G_1,G_2,G_3$ 的生成元,构造双线性映射 $e:G_1\times G_2\rightarrow G_T$.

2. 选择 Hash 函数 $H:\{0,1\}^*\rightarrow Z_p$.

3. 从群 $G_1$ 选择 $h_1,h_2,h_3$,选择随机数 $\gamma\in Z_p^*$,计算 $\omega=g_2^{\gamma}$.

4. 选择可信厂商 C,存储公钥 $PK_C=\{q,G_{C1},G_{C2},e_C,n,g_{C1},P_{pub},H_1,H_2,H_3,H_4\}$.

5. 生成身份权威公钥 $PK_I=\{p,G_1,G_2,G_3,g_1,g_2,g_3,h_1,h_2,h_3,H,\omega\}$并发布,存储并保护身份权威私钥 $SK_I=\gamma$.

## 4.2 EK 生成

对于终端设备(U,M),其中 U 表示该设备包含的主机平台,M 表示该设备绑定的可信芯片,厂商 C 初始化生成公钥 $PK_C=\{q,G_{C1},G_{C2},e_C,n,g_{C1},P_{pub},H_1,H_2,H_3,H_4\}$,私钥为 $SK_C$.C 通过执行如下过程为设备生成 EK 公私钥:

1. 为设备分配唯一性 $ID_M\in\{0,1\}^*$,该 $ID_M$ 即成为该设备的 EK 公钥.$ID_M$ 通常包含厂商标识符、设备序列号等信息.

2. 生成 EK 私钥 $EK_{priv}=SK_C\cdot Q_{ID}$,其中 $Q_{ID}=H_1(ID_M)\in G_{C1}^*$.

3. 将 $EK_{priv}$ 和 $ID_M$ 注入可信芯片 M.

为了下文描述方便,此处分别定义 $enc(m,ID_M)$ 和 $dec(m_s,EK_{priv})$ 用来表示对于消息 $m\in(0,1)^n$,利用 $ID_M$ 对其进行加密和利用 $EK_{priv}$ 对密文进行解密的方法.具体算法定义如下[11]:

$enc(m,ID_M)=\langle rg_{C1},\sigma\oplus H_2(g_{ID}^r),m\oplus H_4(\sigma)\rangle$,其中 $\sigma\in\{0,1\}^n$ 为随机数,$r=H_3(\sigma,m)$,$g_{ID}=e_C(Q_{ID},P_{pub})$,$Q_{ID}=H_1(ID_M)$.

$dec(m_s,EK_{priv})=W\oplus H_4(V\oplus H_2(e_C(EK_{priv},Q)))$,其中 $m_s=\langle Q,V,W\rangle$,是 $m$ 被加密后形成的密文.

## 4.3 身份建立与撤销

设身份权威 I 公钥为 $PK_I=\{p,G_1,G_2,G_3,g_1,g_2,g_3,h_1,h_2,h_3,H,\omega\}$.当管理员 A 试图为终端设备$(U,M)$申请身份时,身份建立协议定义如下:

1. A 向 U 输入其在该网络域的管理员身份标识 $ID_A$①.

2. U 计算 $u=H(ID_A)$,发送 $u$ 给 M.

3. M 选择随机数 $f,y'\in Z_p$,计算 $T=h_1^f\cdot h_2^{y'}$,发送 $(T,ID_M)$给主机平台 U.

① 管理员与设备的交互方式与传统基于管理员的设备管理方法相同,例如可通过 U-Key 等方式进行.本文不对该类方式进行赘述.

4. U 将 $(T, ID_M)$ 发送给 A，由 A 利用自身私钥对 $(T, ID_M)$ 进行签名，并将签名结果发送给身份权威 I.

5. 身份权威 I 判断签名为合法管理员 A 的签名，如果不是，协议执行失败.

6. 身份权威 I 从终端设备(U，M)获取知识签名：$SPK\{(f, y'): h_1^f h_2^{y'} = T\}(n_1)$.

6.1. I 选择随机数 $n_I$ 发送给 U.

6.2. M 选择随机数 $r_f, r_{y'} \in Z_p$，计算 $\widetilde{T} = h_1^{r_f} \cdot h_2^{r_{y'}}$，发送 $\widetilde{T}$ 给 U.

6.3. U 计算 $c = H(p \| h_1 \| h_2 \| T \| \widetilde{T} \| n_I)$，发送 $c$ 给 M.

6.4. M 计算 $s_f = r_f + c \cdot f$，$s_{y'} = r_{y'} + c \cdot y'$，发送 $s_f, s_{y'}$ 给 U.

6.5. U 发送 $(s_f, s_{y'}, c, \widetilde{T})$ 给 I.

6.6. I 验证如下等式，如果成立，则成功完成知识证明：

$\widetilde{T} = T^{-c} h_1^{s_f} h_2^{s_{y'}}$，$c = H(p \| h_1 \| h_2 \| T \| \widetilde{T} \| n_I)$.

7. 身份权威 I 选择随机数 $x, y'' \in Z_p$，计算 $u = H(ID_A)$，计算 $A = (g_1 \cdot T \cdot h_2^{y''} \cdot h_3^u)^{1/(x+\gamma)}$，根据 $ID_M$ 选择本地存储的可信厂商公钥，计算 $enc((A, x, y''), ID_M)$ 并将加密结果发送给 U.

8. U 转发 $enc((A, x, y''), ID_M)$ 给 M，M 利用 4.2 节定义的解密算法进行解密得到 $(A, x, y'')$，计算 $y = y' + y'' (\mathrm{mod} p)$，验证 $e(A, \omega g_2^x) = e(g_1 h_1^f h_2^y h_3^u, g_2)$ 成立，保存 $(A, x, y, f, u)$.

对于身份撤销功能，身份权威通过维护两个撤销列表实现对两种类型身份撤销功能的支持. 对于被破解的可信芯片，通过将身份建立协议步 8 中保存的信息 $f$ 加入终端撤销列表 $RL$ 实现对该芯片绑定终端的平台身份撤销. 对于不可信管理员 $ID_A$，通过将 $H(ID_A)$ 加入管理员撤销列表 $AL$ 实现对该管理员所申请平台身份的撤销.

### 4.4　身份认证

终端设备(U，M)利用身份认证协议向验证者 V 证明自己拥有身份权威 I 颁发的且未被撤销的平台身份凭证，设 I 的公钥为 $PK_I = \{p, G_1, G_2, G_3, g_1, g_2, g_3, h_1, h_2, h_3, H, \omega\}$. 身份认证协议定义如下：

1. V 向终端平台 U 发送挑战消息 $m$.

2. U 选择 $B_1, B_2 \in G_3$，转发 $(m, B_1, B_2)$ 给 M.

3. M 计算 $K_1 = B_1^f, K_2 = B_2^u$，选择随机数 $a \in Z_p$，计算 $b = y + ax$，$T = A \cdot h_2^a$，发送 $(K_1, K_2, T)$ 给 U.

4. 终端设备为验证者生成如下知识签名：

$$SPK\{(x, f, u, a, b): K_1 = B_1^f \wedge K_2 = B_2^u \wedge e(T, g_2)^x \cdot e(T, \omega) = e(g_1, g_2) \cdot e(h_1, g_2)^f \cdot e(h_2, g_2)^b \cdot e(h_3, g_2)^u \cdot e(h_2, \omega)^a\}(m).$$

4.1. M 选择随机数 $r_x, r_f, r_u, r_a, r_b \in Z_p$，计算 $R_1 = B_1^{r_f}, R_2 = B_2^{r_u}, R_3 = e(T, g_2)^{-r_x} \cdot e(h_1, g_2)^{r_f} \cdot e(h_2, g_2)^{r_b} \cdot e(h_3, g_2)^{r_u} \cdot e(h_2, \omega)^{r_a}$，发送 $(R_1, R_2, R_3)$ 给 U.

4.2. U 计算 $c = H(PK_1, B_1, K_1, B_2, K_2, T, R_1, R_2, R_3, m)$，发送 $c$ 给 M.

4.3. M 计算 $s_x = r_x + cx$，$s_f = r_f + cf$，$s_u = r_u + cu$，$s_a = r_a + ca$，$s_b = r_b + cb$，输出 $(s_x, s_f, s_u, s_a, s_b)$ 给 U.

4.4. U 发送 $\sigma$ 给验证者 V，其中 $\sigma = (B_1, K_1, B_2, K_2, T, c, s_x, s_f, s_u, s_a, s_b)$.

5. 验证者 V 验证 $B_1, B_2 \in G_3, T \in G_1, s_x, s_f, s_u, s_a, s_b \in Z_p$，如果不成立，则认证失败.

6. V 计算 $\widehat{R}_1 = B_1^{s_f} \cdot K_1^{-c}$，$\widehat{R}_2 = B_2^{s_u} \cdot K_2^{-c}$，$\widehat{R}_3 = e(T, g_2)^{-s_x} \cdot e(h_1, g_2)^{s_f} \cdot e(h_2, g_2)^{s_b} \cdot e(h_3, g_2)^{s_u} \cdot e(h_2, \omega)^{s_a} \cdot (e(g_1, g_2)/e(T, \omega))^c$，验证等式 $c = H(PK, B_1, K_1, B_2, K_2, T, \widehat{R}_1, \widehat{R}_2, \widehat{R}_3, m)$ 是否成立. 如果不成立，则认证失败.

7. 对于撤销列表 $RL = \{f_1, f_2, \cdots, f_m\}$，对于所有 $1 \leq i \leq m$，验证者检查 $K_1 = B_1^{f_i}$ 是否成立，如果成立，则认证失败.

8. 对于撤销列表 $AL = \{u_1, u_2, \cdots, u_m\}$，对于所有 $1 \leq i \leq m$，验证者检查 $K_2 = B_2^{u_i}$ 是否成立，如果成立，则认证失败.

## 5　安全性证明及分析

本节对方案的安全性进行分析，为了确定上述方案满足安全要求，我们首先给出如下定理.

**定理 1**[8]. BBS$^+$ 签名方案在 $q$-SDH 假设下是安全的.

证明. 该定理在文献[8]中已给出详细证明，此处略.

下面证明身份认证协议中步 4 生成的知识签名以及步 5、6 进行的验证实际上完成了终端设备拥有身份权威颁发的合法身份凭证 $(A, x, y, f, u)$ 的零知识签名：

$$SPK\{(A, x, y, f, u): K_1 = B_1^f \wedge K_2 = B_2^u \wedge e(A, \omega g_2^x) = e(g_1 h_1^f h_2^y h_3^u, g_2)\}(m).$$

具体分为如下两个定理的证明.

**定理 2.** 身份认证协议知识签名 $\sigma$ 中的 $(T, c, s_x, s_f, s_u, s_a, s_b)$ 可以被模拟.

证明. 根据协议描述，$T = A \cdot h_2^a$，由于 $a$ 为随机数，因此可知 $T$ 在群 $G_1$ 的分布满足随机性. 因此模拟器可以随机选择 $G_1$ 中元素来模拟 $T$. 假定 Hash 函数 $H$ 为随机预言机，由于 $c$ 为 Hash 函数 $H$ 的计算结果，因此可知 $c$ 在 $Z_p$ 中也随机分布. 类似的，由于 $r_x, r_f, r_u, r_a, r_b$ 的随机性，$s_x, s_f, s_u, s_a, s_b$ 在 $Z_p$ 中也服从随机分布. 因此模拟器可以从 $Z_p$ 中随机选择元素进行 $c, r_x, r_f, r_u, r_a, r_b$ 的模拟. 由此，模拟器成功模拟 $(T, c, s_x, s_f, s_u, s_a, s_b)$，定理得证.

证毕.

**定理 3.** 对于成功执行身份认证协议步 4 的

终端设备,存在知识提取器(knowledge extractor)可以从该终端设备中提取$(A,x,y,f,u)$,使得$e(A,\omega g_2^x)=e(g_1h_1^fh_2^yh_3^u,g_2)$,$K_1=B_1^f$,$K_2=B_2^u$同时成立.

证明. 假定知识提取器可以回卷(rewind)终端设备计算过程,并且控制了 Hash 函数 $H$ 的输出.则其可以通过下述过程获得$(A,x,y,f,u)$:

1. 终端计算 $T$.

2. 根据身份认证协议步 4.1,终端选择 $r_x,r_f,r_u,r_a,r_b$,计算 $R_1=B_1^{r_f}$,$R_2=B_2^{r_u}$,$R_3=e(T,g_2)^{-r_x}\cdot e(h_1,g_2)^{r_f}\cdot e(h_2,g_2)^{r_b}\cdot e(h_3,g_2)^{r_u}\cdot e(h_2,\omega)^{r_a}$.

3. 根据身份认证协议步 4.2,终端请求计算$H(PK_I,B_1,K_1,B_2,K_2,T,R_1,R_2,R_3,m)$,知识提取器输出 Hash 值 $c$.

4. 根据身份认证协议步 4.3,终端计算并输出 $s_x,s_f,s_u,s_a,s_b$.

5. 知识提取器回卷步 3、4,对于步 3 请求的 Hash 计算,返回 Hash 值 $c'$,$c'\neq c$,终端根据 $c'$在步 4 计算并输出$s_x',s_f',s_u',s_a',s_b'$.

6. 知识提取器计算 $\bar{c}=c-c'$,$\bar{s}_x=s_x-s_x'$,$\bar{s}_f=s_f-s_f'$,$\bar{s}_u=s_u-s_u'$,$\bar{s}_a=s_a-s_a'$,$\bar{s}_b=s_b-s_b'$,$\Delta x=\bar{s}_x/\bar{c}=x$,$\Delta f=\bar{s}_f/\bar{c}=f$,$\Delta u=\bar{s}_u/\bar{c}=u$,$\Delta a=\bar{s}_a/\bar{c}=a$,$\Delta b=\bar{s}_b/\bar{c}=b$.则可知 $K_1=B_1^{\Delta f}$,$K_2=B_2^{\Delta u}$,$e(T,g_2)^{\Delta x}\cdot e(T,\omega)=e(g_1,g_2)\cdot e(h_1,g_2)^{\Delta f}\cdot e(h_2,g_2)^{\Delta b}\cdot e(h_3,g_2)^{\Delta u}\cdot e(h_2,\omega)^{\Delta a}$等式满足.

计算 $\Delta y=\Delta b-\Delta a\cdot\Delta x$,$\Delta A=T\cdot h_2^{-\Delta a}$,则

$$e(\Delta A,\omega g_2^{\Delta x})=e(T\cdot h_2^{-\Delta a},\omega g_2^{\Delta x})=e(T,\omega)\cdot e(h_2^{-\Delta a},g_2^{\Delta x}).$$

根据 $e(T,g_2)^{\Delta x}\cdot e(T,\omega)=e(g_1,g_2)\cdot e(h_1,g_2)^{\Delta f}\cdot e(h_2,g_2)^{\Delta b}\cdot e(h_3,g_2)^{\Delta u}\cdot e(h_2,\omega)^{\Delta a}$可得

$$\begin{aligned}e(\Delta A,\omega g_2^{\Delta x})&=e(h_2^{-\Delta a},g_2^{\Delta x})\cdot e(T,g_2)^{-\Delta x}\cdot e(g_1,g_2)\cdot\\&\quad e(h_1,g_2)^{\Delta f}\cdot e(h_2,g_2)^{\Delta b}\cdot\\&\quad e(h_3,g_2)^{\Delta u}\cdot e(h_2,\omega)^{\Delta a}\\&=e(g_1h_1^{\Delta f}h_2^{\Delta y}h_3^{\Delta u},g_2).\end{aligned}$$

因此,$(\Delta A,\Delta x,\Delta y,\Delta f,\Delta u)$即为所求秘密信息.定理得证. 证毕.

基于上述定理,我们对本文方案的安全性进行分析.

**定理 4.** 本方案满足身份建立的正确性要求.

证明. 根据身份建立协议,在步 5 中将对管理员签名进行验证,从而认证管理员身份.如果管理员具有相关权限,则步 5 将成功.如果设备由可信终端厂商生产,在步 7 中身份权威将身份凭证信息$(A,x,y'')$根据厂商公钥和芯片 $ID_M$ 加密,根据文献[11]中对于基于 $ID$ 的加解密方案安全性证明,可知在步 8 中终端平台可正确解密,获得身份凭证信息$(A,x,y,f,u)$.由此可知,本方案满足身份建立时的正确性保证要求. 证毕.

**定理 5.** 本方案满足身份认证的正确性要求.

证明. 当终端设备正确的执行身份认证协议步 1～4 后,易知身份认证协议的步 5、步 6 将验证成功.假设 $RL=\{f_1,f_2,\cdots,f_m\}$,$AL=\{u_1,u_2,\cdots,u_m\}$.如果该平台未被破解,即 $f\notin RL$,则步 7 将成功.如果负责为该平台申请身份的管理员未被破解,即 $u\notin AL$,则步 8 将成功.因此可知,本方案满足身份认证时的正确性要求. 证毕.

**定理 6.** 本方案满足身份建立时的不可伪造性.

证明. 根据身份建立协议可知,如果当前管理员不具有权限,则身份建立协议的步 5 将验证失败.如果终端不是可信终端厂商生产,根据文献[11]中对于基于 ID 的加解密方案安全性证明,可知步 8 加密的身份凭证信息在步 9 无法被终端设备正确解密,终端也就无法获得合法的身份凭证.因此,本方案满足身份建立时的不可伪造性. 证毕.

**定理 7.** 本方案满足身份认证的不可伪造性.

证明. 为了证明该定理,我们首先给出身份认证不可伪造性的形式化定义.

对于攻击者,如果其无法赢得下述游戏,则称方案满足身份认证的不可伪造性.该游戏的基本思路是假设所有由攻击者掌握平台的平台身份均已被撤销,攻击者的目的是伪造一个合法签名.定义攻击者 A 与挑战者 C 间游戏如下:

1. 初始化. C 执行身份权威初始化算法,生成 $PK=\{p,G_1,G_2,G_3,g_1,g_2,g_3,h_1,h_2,h_3,\omega\}$,$\gamma\in Z_p^*$.设置 $U=I=\varnothing$,$U,I$ 分别表示当前已被撤销的平台和管理员列表.

2. 请求. A 向 C 任意发出以下请求:

2.1. Join. A 请求为平台 $P_i$ 申请身份. C 检查 $i$ 未被请求过,则 C 作为身份权威,执行以下几类操作之一;

2.1.1. 与 A 执行身份建立过程,A 获得$(A_i,x_i,y_i,f_i,u_i)$后,发送 $f_i$ 给 C,则 C 将 $f_i$ 加入 $U$;

2.1.2. 与 A 执行身份建立过程,A 获得$(A_i,x_i,y_i,f_i,u_i)$后,发送 $u_i$ 给 C,则 C 将 $u_i$ 加入 $I$;

2.1.3. 与 A 执行身份建立过程,A 获得$(A_i,x_i,y_i,f_i,u_i)$,发送 $f_i,u_i$ 给 C,则 C 将 $f_i$ 加入 $U$,$u_i$ 加入 $I$;

2.1.4. C 在本地执行身份建立过程,产生$(A_i,x_i,y_i,f_i,u_i)$;

2.2. Sign. A 请求为消息 $m$ 产生平台 $P_i$ 的知识签名. C 检查 $P_i$ 已建立身份,根据身份认证协议步 4 计算消息 $m$ 的知识签名 $\sigma$ 并发送给 A;

2.3. Corrupt. A 发出对平台 $P_i$ 的破解请求,分以下几类破解可能:

2.3.1. A 请求平台 $P_i$ 的 $f_i$,C 检查 $P_i$ 已建立身份,将 $f_i$ 发送给 A,将 $f_i$ 加入 $U$;

2.3.2. A 请求平台 $P_i$ 的 $u_i$，C 检查 $P_i$ 已建立身份，将 $u_i$ 发送给 A，将 $u_i$ 加入 $I$；

2.3.3. A 请求平台 $P_i$ 的 $f_i$，$u_i$，C 检查 $P_i$ 已建立身份，将 $f_i$，$u_i$ 发送给 A，将 $f_i$ 加入 $U$，将 $u_i$ 加入 $I$.

3. 回应. A 输出消息 $m^*$，$RL=\{f_1,f_2,\cdots,f_m\}$，$AL=\{u_1,u_2,\cdots,u_m\}$，知识签名 $\sigma^*$.

如果下述条件满足，则判定攻击者赢得该游戏.

条件 1. 该签名通过身份认证协议步 5～8 的验证.

条件 2. 对于任意的 $f_i\in U$ 和 $u_i\in I$，$f_i\in RL$，$u_i\in AL$.

条件 3. A 未通过 sign 请求获得消息 $m^*$ 的知识签名.

下面我们证明不存在多项式时间的算法 A 能以不可忽略的概率赢得上述游戏.

假设算法 A 存在，则我们可以基于 A 构造算法 B，使得其可以破坏 BBS$^+$ 签名算法的不可伪造性. 该算法 B 与算法 A 之间的交互定义如下：

初始化. 给定 $(G_1,G_2)$ 为素数 $p$ 阶的双线性群. $g_1$，$g_2$ 分别为其生成元. 给定 BBS$^+$ 签名机制中公钥的 $\{g_1,g_2,h_1,h_2,h_3,\omega\}$ 部分. B 执行如下操作

1. 选择 $p$ 阶循环群 $G_3$，$g_3$ 为生成元. 将公钥 $PK=\{p,G_1,G_2,G_3,g_1,g_2,g_3,h_1,h_2,h_3,\omega\}$ 发送给 A.

2. 建立列表 $U$，$I$ 分别用于表示当前已被撤销的终端设备和管理员，初始化 $U=I=\varnothing$.

Hash 请求. 在任意时刻，A 均可向 Hash 函数 $H$ 发起查询. 对于该查询，B 在满足一致性的前提下返回任意随机数. 一致性要求对于两次相同的查询，B 将返回相同的查询结果.

Join 请求 1. B 和 A 运行身份建立协议，当 A 执行完身份建立协议的步 6 后，由于步 7 是知识证明协议，因此 B 通过回卷 A 可获得 $(f_i,y_i')$. 接着 B 通过查询 BBS$^+$ 签名预言机(Signature Oracle)获得 $f_i$，$u_i$ 的签名 $(A_i,x_i,y_i)$. B 计算 $y_i''=y_i-y_i'$，将 $(A_i,x_i,y_i'')$ 返回给 A. B 将 $f_i$ 加入 $U$.

Join 请求 2. B 和 A 运行身份建立协议，当 A 执行完身份建立协议的步 6 后，B 通过回卷 A 获得 $(f_i,y_i')$. 接着 B 通过查询 BBS$^+$ 签名预言机获得 $f_i$，$u_i$ 的签名 $(A_i,x_i,y_i)$. B 计算 $y_i''=y_i-y_i'$，将 $(A_i,x_i,y_i'')$ 返回给 A. B 将 $f_i$ 加入 $U$，$u_i$ 加入 $I$.

Join 请求 3. B 选择随机数 $f_i\in Z_p$，设置 $(A_i,x_i,y_i)=unknown$ 用来表示 B 不知道 $f_i$ 的 BBS$^+$ 签名. B 将 $u_i$ 加入 $I$.

Join 请求 4. B 选择随机数 $f_i\in Z_p$，设置 $(A_i,x_i,y_i)=unknown$ 用来表示 B 不知道 $f_i$ 的 BBS$^+$ 签名.

Sign 请求. A 请求为消息 $m$ 产生平台 $P_i$ 的知识签名.

如果 $(A_i,x_i,y_i)\neq unknown$，B 按照身份认证协议步 4，计算签名 $\sigma$ 并发送给 A.

如果 $(A_i,x_i,y_i)=unknown$，B 按照身份认证协议生成 $(B_1,K_1)$，$(B_2,K_2)$. 然后选择 $T\in G_1$，$s_x$，$s_f$，$s_a$，$s_b$，$s_u\in Z_p$. 按照身份认证协议的步 6 计算 $R_1$，$R_2$. 然后增补 Hash 预言机使得 $c=H(PK,B_1,K_1,B_2,K_2,T,R_1,R_2,R_3,m)$. 如果该等式与该预言机已给出的计算结果冲突，则报告失败并退出. 否则 B 生成签名 $\sigma=(B,K,T,c,s_x,s_f,s_u,s_a,s_b)$.

Corrupt 请求. A 请求平台 $P_i$ 的私钥. 如果 $(A_i,x_i,y_i)=unknown$，B 查询 BBS$^+$ 签名预言机，获得签名 $(A_i,x_i,y_i)$ 并将其发送给 A，B 将 $f_i$ 加入 $U$.

Response. A 输出消息 $m^*$，$RL=\{f_1,f_2,\cdots,f_m\}$，$AL=\{u_1,u_2,\cdots,u_m\}$，签名 $\sigma^*$，满足如下条件：

条件 1. 该签名可被身份认证协议步 5～8 验证通过.

条件 2. 对于任意的 $f_i\in U$，$f_i\in RL$，对于任意的 $u_i\in I$，$u_i\in AL$.

由定理 4 可知 B 可以通过回卷 A 从签名 $\sigma^*$ 中获得 $(A,x,y,f,u)$，使得 $e(A,\omega g_2^x)=e(g_1h_1^fh_2^yh_3^u,g_2)\wedge K_1=B_1^f\wedge K_2=B_2^u$. 由于 $G_3$ 是循环素阶群，因此对于 $(B_1,K_1)$，$(B_2,K_2)$，有唯一的 $f^*$，$u^*$ 使得 $K_1=B_1^f$ 和 $K_2=B_2^u$ 成立.

下面证明 $f^*\notin U$. 如果 $f^*=f_i\in RL$，则 $K_1=B_1^f$ 成立，与认证协议的步 7 冲突，由于对于任意的 $f_x\in U$，$f_x\in RL$. 根据算法 B 与算法 A 之间的交互定义，可知 $U$ 包含了所有 B 通过查询签名预言机生成的签名，由此可知 $f^*\notin U$，则 B 即在不查询 BBS$^+$ 签名预言机的条件下获得了未知消息 $f^*$ 的 BBS$^+$ 签名. 这与定理 1 中指出的 BBS$^+$ 签名算法的安全性相矛盾. 证毕.

此外，对于方案满足终端匿名性的证明类似文献[7]中给出的匿名性证明，具体证明此处略.

## 6　分　析

相比较利用隐私 CA 的平台身份建立和 DAA(直接匿名证明)等协议实施网络终端平台身份管理，本文提出的方案降低了 EK 证书管理的复杂性、提高了匿名身份的撤销能力，同时还具有密钥与签名长度短，计算效率高的优点，具体分析如下.

在基于可信计算芯片的终端平台身份建立方案中，基于 EK 证书确保终端绑定可信芯片是保证方案可信性的基础. 因此，基于传统方案建立平台匿名身份时，身份权威需要管理每个终端的 EK 证书. 以移动网为例，为每个终端设备维护一个 EK 证书必然给身份权威带来极大的管理负担. 同时考虑到新设备的不断加入，如果每个新设备初始入网时通过网络传送自身的 EK 证书给身份权威，这必将带来较大的网络负载. 基于本文的身份建立协议，当一台新终端加入网络域时，该终端只需要将自身的身份标识 $ID_M$(通常包括厂商标识符、设备序列号等)发送给身份权威，相比较发送完整的 EK 证书，本方案

极大地降低了网络负载. 此外,在本文方案中,身份权威只需要对可信终端厂商的公钥证书进行管理,通过该证书即可保证其颁发的匿名平台身份只能被绑定可信芯片的终端平台获得. 因此,相比较传统方案,本文方案极大地降低了身份权威管理的复杂性.

由管理员负责平台终端的管理是目前通用的终端管理方法,可信芯片的推出为实现硬件保护的平台身份管理提供了基础,然而基于传统隐私 CA 或 DAA 方案无法与现有基于管理员的方案有效结果. 根据引言的问题 2 描述,现有方案在这方面的不足主要体现在无法支持基于管理员的平台身份撤销. 根据本文描述的身份撤销和身份认证协议,当负责为平台颁发身份的管理员被撤销时,可以通过将该管理员身份标识的 Hash 值放入撤销列表,在身份认证协议中,通过检查撤销列表即可判断当前平台身份是否由该不可信管理员颁发,从而很好地实现了基于管理员的平台身份撤销.

下面对本方案的效率进行分析. 以达到 RSA 1024 位安全强度要求为例,根据文献[7,13-17]所述方法进行终端厂商以及身份权威初始化过程中双线性映射构造和安全参数选择,则可信芯片需要保护的 EK 私钥长度为 513 位;平台身份建立后被保护的身份秘密信息长度为 851 位,身份认证协议过程中产生的知识签名长度为 1875 位. 在计算效率上,通过提前计算 $e(A,g_2),e(h_1,g_2),e(h_2,g_2),e(h_3,g_2),e(h_2,\omega)$ 以及 $e(g_1,g_2)$,终端计算 $e(A,g_2)^{-r_x}\cdot e(h_1,g_2)^{r_f}\cdot e(h_2,g_2)^{r_b-ar_x}\cdot e(h_3,g_2)^{r_u}\cdot e(h_2,\omega)^{r_a}$ 即可获得身份认证协议的步 4 中的 $R_3$. 对于身份认证协议的步 6 中的 $\hat{R}_3$,验证者计算 $e(T,g_2^{-s_x}\omega^{-c})\cdot e(h_1,g_2)^{s_f}\cdot e(h_2,g_2)^{s_b}\cdot e(h_3,g_2)^{s_u}\cdot e(h_2,\omega)^{s_a}\cdot e(g_1,g_2)^{c}$ 即可获得该值. 因此在一次身份认证过程中,终端设备只需要进行 4 次群 $G_3$ 上的幂次运算,1 次群 $G_1$ 上的幂次运算以及 1 次群 $G_T$ 上的乘幂运算,验证者只需要进行 1 次双线性映射运算,2 次群 $G_3$ 上的乘幂运算,1 次群 $G_2$ 上的乘幂运算以及 1 次群 $G_T$ 上的乘幂运算. 用 ME 表示一次乘幂运算,P 表示一次双线性映射运算,表 1 给出了本文方案与其它方案的效率对比.

**表 1 相关工作效率比较**

| | 身份秘密信息/Byte | 签名长度/Byte | 签名效率 | 验证效率 |
|---|---|---|---|---|
| 本文方案 | 107 | 235 | 6ME | 4ME+1P |
| 文献[6]方案 | 213 | 512 | 10ME | 2ME+5P |
| 文献[18]方案 | 86 | 148 | 8ME+1P | 1ME+5P |
| 文献[19]方案 | 86 | 320 | 10ME | 7ME+2P |

## 7 系统实现

基于上述方案,我们在可信网络接入系统中实现了对于接入网络终端设备的管理. 该系统的体系架构如图 2 所示. 其中平台身份管理服务负责对终端平台身份进行管理,当终端试图接入 Internet 时,网络接入点将作为验证者将对终端平台身份进行验证. 确认该终端拥有平台身份管理服务颁发的合法身份.

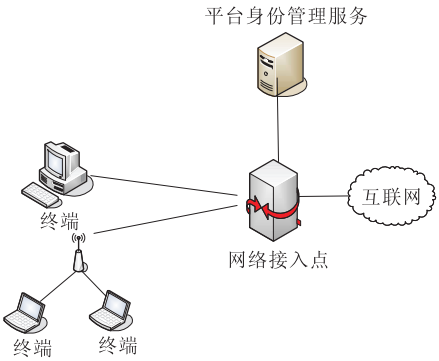



图 2 可信网络接入终端身份管理系统架构


图 3 平台身份注册界面

平台身份管理服务以 Web Service 的形式提供身份颁发和撤销列表查询功能. 当一台新的终端加入网络时,管理员在客户端(如图 3 所示)输入管理员的用户名、密码以及其它相关描述信息后,终端设备与平台身份管理服务将按照本文方案所述进行身份建立. 当客户端试图接入网络时,网络接入点从平台身份管理服务查询当前的撤销列表,通过验证当前接入平台是否由该平台身份管理服务颁发以及是否在撤销列表,从而实现网络接入控制.

在具体实现中,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,因此我们采用 PBC 库(Pairing-based Cryptography Library)①进行了模拟实现. 表 2 给出了原型系统的性能测试结果.

① http://crypto.stanford.edu/pbc/

表 2　原型系统实验数据

| | 身份建立时间/s | 身份认证时间/s |
|---|---|---|
| 1 轮 | 48 | 16 |
| 5 轮 | 235 | 85 |
| 10 轮 | 495 | 201 |
| 15 轮 | 735 | 270 |
| 20 轮 | 1020 | 360 |

## 8　总结及下一步工作

本文方案利用基于 ID 的加解密机制，提出了新的可信芯片 EK 证书产生办法. 通过该办法，身份权威只需要存储可信厂商的公钥证书，不再需要为每个终端设备维护其 EK 证书，因此极大降低了 EK 证书管理的复杂性. 此外，本文对现有 DAA 方案进行了改进，使得在保证平台身份匿名性和安全性的同时，将传统的基于管理员的终端管理方法结合进来，支持了基于管理员身份的平台身份建立和撤销，极大地提高了终端平台身份管理的灵活性和安全性.

在下一步工作中，我们将基于上述方案和原型系统，进一步展开对 TPM/TCM 可信芯片和可信网络连接的研究，设计合理的 TPM/TCM 接口规范，实现网络终端身份管理系统和网络接入时的身份认证，从而提高现有网络基础架构的可管可控性和安全性.

## 参　考　文　献


[1] Trusted Computing Group. TCG Specification Architecture Overview v1.2, 2004

[2] State Cryptography Administration. Functionality and Interface Specification of Cryptographic Support Platform for Trusted Computing. 2007(in Chinese)
(国家密码管理局. 可信计算密码支撑平台功能与接口规范. 2007)

[3] Brickell Ernie, Camenisch Jan, Chen Li-Qun. Direct anonymous attestation//Proeeedings of the ACM Conference on Computer and Communications Security. Washington DC, USA, 2004: 132-145

[4] Ge He, Tate Stephen R. A direct anonymous attestation scheme for embedded devices//Okamoto Tatsuaki, Wang Xiaoyun. Public Key Cryptography. Berlin: Springer, 2007: 16-30

[5] Brickell Ernie, Li Jiang-Tao. Enhanced privacy ID: A direct anonymous attestation scheme with enhanced revocation capabilities//Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society. Alexandria, Virginia, USA, 2007: 21-30

[6] Brickell Ernie, Chen Li-Qun, Li Jiang-Tao. A new direct anonymous attestation scheme from Bilinear Maps// Lipp Peter, Sadeghi Ahmad-Reza, Koch Klaus-Michael. Trusted Computing—Challenges and Applications. Berlin: Springer, 2008: 166-178

[7] Brickell Ernie, Li Jiang-Tao. Enhanced privacy ID from bilinear maps. Cryptology ePring Archive: 095, 2009

[8] Au Man H, Susilo Willy, Mu Yi. Constant-size dynamic k-TAA//Prisco Roberto D, Yung Moti. Security and Cryptography for Networks. Berlin: Springer, 2006: 111-125

[9] Camenisch Jan, Stadler Markus. Efficient group signature schemes for large groups//Kaliski Burton S. Advances in Cryptology. Berlin: Springer, 1997: 410-424

[10] Fiat Amos, Shamir Adi. How to prove yourself: Practical solutions to identification and signature problems//Odlyzko Andrew M. Advances in Cryptology. Berlin: Springer, 1987: 186-194

[11] Boneh Dan, Franklin Matt. Identity-based encryption from the Weil pairing//Kilian Joe. Advances in Cryptology. Berlin: Springer, 2001: 213-229

[12] Feng Deng-Guo. Research on theory and approach of provable security. Journal of Software, 2005, 16(10): 1743-1756 (in Chinese)
(冯登国. 可证明安全性理论与方法研究. 软件学报, 2005, 16(10): 1743-1756)

[13] Lynn Ben. On the implementation of pairing-based cryptosystems[Ph. D. dissertation]. Stanford University, Stanford, 2007

[14] Barreto, Paulo S L, Kim Hae Y, Lynn Ben, Scott Michael. Efficient algorithms for pairing-based cryptosystems//Yung Moti. Advances in Cryptology. Berlin: Springer, 2002: 354-369

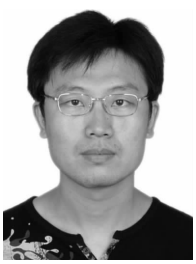
[15] Brickell Ernie, Camenisch Jan, Chen Li-Que. Trusted Computing. London: IEE, 2005

[16] Boneh Dan, Boyen Xavier, Shacham Hovav. Short group signatures//Franklin Matt. Advances in Cryptology. Berlin: Springer, 2004: 41-55

[17] Miyaji Atsuko, Nakabayashi Masaki, Takano Shunzo. New explicit conditions of elliptic curve traces for FR-reduction. IEICE Transactions on Fundamentals, 2001, 84-A(5): 1234-1243

[18] Chen Li-Qun, Morrissey Paul, Smart Nigel P. Pairings in trusted computing//Galbraith Steven D, Paterson Kenneth G. Pairing-Based Cryptography. Berlin: Springer, 2008: 1-17

[19] Tsang Patrick P, Au Man H, Kapadia Apu, Smith Sean W. Black-listable anonymous credentials: Blocking misbehaving users without TTPs//Proceedings of the ACM Conference on Computer and Communications Security. Alexandria, Virginia, USA, 2007: 72-81


**YU Ai-Min**, born in 1980, Ph. D. candidate. His research interests include system security and trusted computing.

**CHU Xiao-Bo**, born in 1984, Ph. D. candidate. His research interests include system security and trusted computing.

**FENG Deng-Guo**, born in 1965, Ph. D., professor, Ph. D. supervisor. His research interests include network and information security.

**Background**

In this paper how to manage the terminal's anonymous platform identity based on a trusted chip (i. e. TPM or TCM) is studied, as the base to construct a trusted network. The basic idea of existing solutions is that the trusted vendor binds each terminal with a trusted chip. And an unique key pair which is called endorsement key(EK) is embed in the chip. When a platform identity is needed, the terminal generates a key pair called an Attestation Identity Key (AIK), sends the public part of AIK to the identity authority (i. e. Privacy CA), and authenticates this public key w. r. t. the EK. The identity authority will check whether it finds the EK in its list and, if so, issues a certificate on the TPM's AIK. Then the certificate is the identity of the terminal. This solution has the obvious drawback that if the identity authority and the verifier collude, the verifier will be able to uniquely identify a terminal in a transaction. Thus the privacy of the terminal may be violated. To solve the above problem, Brickell, Camenisch, and Chen introduced a cryptographic scheme called Direct Anonymous Attestation(DAA). It utilized zero-knowledge proof, so the terminal can attest its identity without presenting the platform certificate.

However there are still two problems when managing platform identity of the terminal using these approaches mentioned above. The first one is that it is hard to manage EK certificate of TPM/TCM, especially in large scale networks. Secondly traditional user-based terminal management can not be combined with the approaches based on TPM/TCM.

Aiming at these problems, in this paper an improved approach is proposed to manage terminal platform identity based on TPM/TCM. It made use of zero-knowledge proof and ID-based cryptography and defined the protocols to issue EK, establish platform anonymous identity, revoke platform identity, and authenticate platform identity. Moreover the security of this approach is proved under RO (random oracle) model.

The work described in this paper was supported by the National High Technology Research and Development Program (863 Program) of China under grant No. 2007AA01Z412, the National Science & Technology Pillar Program of China under grant No. 2008BAH22B06, CAS Innovation Program under grant No. ISCAS2009-DR14, ISCAS2009-GR. One major objective of these projects is to investigate the key mechanisms which are important to construct a trusted network environment.

Currently the team has proposed multiple platform anonymous identity protocol and developed a trusted network prototype. Some of them were published in papers and technical reports. The work of this paper is one of the latest progresses and it resolves the terminal identity management problems incurred when developing the trusted work prototype.