doi:10.3969/j.issn.1000-436x.2013.06.008

改进的移动计算平台直接匿名证明方案

杨力，张俊伟，马建峰，刘志宏
（西安电子科技大学 计算机学院，陕西 西安 710071）

摘 要：分析了 Ge 等人提出的直接匿名证明方案的安全缺陷，指出该方案的认证协议在用于远程证明时不能抵抗重放攻击和平台伪装攻击。提出一种改进的直接匿名证明的认证协议，引入会话密钥协商机制，增强互认证功能。分析表明，改进方案在正确进行直接匿名证明的前提下，满足不可伪造性和匿名性，能够抵抗重放攻击和平台伪装攻击，协议性能满足移动计算平台的可信验证需求。
关键词：可信计算；远程证明；直接匿名证明；密钥协商
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1000-436X(2013)06-0069-07

Improved direct anonymous attestation scheme for mobile computing platforms

YANG Li, ZHANG Jun-wei, MA Jian-feng, LIU Zhi-hong
(School of Computer Science & Technology, Xidian University, Xi'an 710071, China)

Abstract: The security flaws of a direct anonymous attestation scheme proposed by Ge, *et al*. Were analyzed, and the result shows that the authentication protocol of the scheme is vulnerable to reply attacks and platform masquerade attacks when being used for remote attestation. An improved direct anonymous attestation authentication scheme with the involvement of key agreement was proposed to provide the property of mutual authentication. The analysis shows that the proposal can realize direct anonymous attestation with the properties of forgery-resistance and anonymity, and resist reply attacks and platform masquerade attacks; the scheme is effective and suitable for the mobile trusted computing platforms.
Key words: trusted computing; remote attestation; direct anonymity attestation; key agreement

1 引言

可信计算组织（TCG, trusted computing group）提出的可信计算技术的核心是在计算平台中嵌入可信平台模块（TPM, trusted platform module），为可信机制和安全功能提供硬件保障，为度量和验证平台的可信属性提供基础[1]。TPM 具有远程证明的能力，能够响应远程验证方的验证请求，对平台身份和平台完整性等可信属性进行证明。在远程证明过程中，按照 TCG 要求，要能够对平台身份信息的隐私性进行保护[2]，向验证方进行远程证明时不能暴露 TPM 的身份信息，也不能由验证方将多次的证明信息进行关联以推断平台身份信息。

TCG 先后采用引入可信的第三方隐私 CA（privacy-CA）[3]的方法和直接匿名证明（DAA, direct anonymous attestation）[4]的方法等，来解决远程证明时平台隐私信息的保护问题。其中 TPM 规范 v1.1b 中所采用的 Privacy-CA 方法是在证明系统中引入可信第三方 Privacy-CA，作为权威的证书颁发机构可以向 TPM 颁发身份证书，进行远程认证

收稿日期：2012-06-26；**修回日期**：2012-12-20
基金项目：长江学者和创新团队发展计划基金资助项目(IRT1078)；国家自然科学基金资助项目(U1135002, 61202390, 61202389, 61173135, 61100230, 61100233)；陕西省自然科学基础研究计划基金资助项目(2012JM8025, 2011JQ8003, 2011JM8004, 2012JQ8043, 2012JM8030)
Foundation Items: The Program for Changjiang Scholars and Innovative Research Team in University(IRT1078); The National Natural Science Foundation of China (U1135002,61202390,61202389,61173135,61100230,61100233); The Natural Science Basic Research Plan in Shaanxi Province of China (2012JM8025,2011JQ8003,2011JM8004,2012JQ8043,2012JM8030)

时 TPM 向远程验证方出示身份证书，验证方将收到的证书发回给 Privacy-CA，且一同验证其合法性。但是，Privacy-CA 方法存在一定的缺陷，由于每次进行证明时都需要 Privacy-CA 的参与，因此，它会成为整个系统的安全瓶颈与性能瓶颈。

由 Brickell 等[4]提出的直接匿名证明方法(以下简称 BCC 方案)被 TPM 规范 v1.2 所采纳，用以克服上述缺陷。直接匿名证明方法及应用广受研究关注[5,6]，但大都采用 BCC 方案的证明框架和思路。基本的 BCC 方案是基于 CL 群签名技术[7]和知识证明方法[8]构建的，在此方案中可信平台及 TPM 进行远程证明时不泄露身份等隐私信息。在 BCC 方案中，TPM 选择私有的秘密值，通过一个安全的两方协议获得 DAA 证书即 DAA 颁发者（DAA Issuer）在其上的 CL 签名，当 TPM 向远程验证方证明身份时，利用 DAA 证书和秘密值对消息进行 DAA 签名，验证者确认此 DAA 签名并相信 TPM 通过知识证明获得了匿名签名。

但是，在 BCC 方案中，TPM 及所在平台与验证者交互复杂且运算量大，不能应用于计算资源有限的嵌入式设备，上述方案均不能适用于移动网络环境。因此，Ge 等提出能够满足计算能力受限系统的直接匿名证明方案[9]，可简称为 DAA-ED 方案。DAA-ED 基于 CM 群签名技术[10]，缩减了交互证明的复杂度，简化了协议运算量，适用于移动计算平台等资源受限系统。

本文分析发现，DAA-ED 方案在进行直接匿名证明时，其认证协议中 TPM 的签名信息仅由验证者进行单向认证，当实际应用于远程证明时，不能有效地抵抗重放攻击和平台伪装攻击，攻击者可以通过对旧消息的重放，或者借助一个合法的可信计算平台完成对认证消息的签名以欺骗验证者。针对上述安全缺陷，对 DAA-ED 方案的认证协议进行改进，引入基于会话密钥协商的双向认证机制，TPM 与验证者交互过程中协商安全会话密钥。改进方案能够正确地进行直接匿名证明，满足不可伪造性和匿名性，能够有效地抵抗针对可信计算平台的重放攻击和平台伪装攻击，运算量比 BCC 方案大为缩减且与 DAA-ED 方案相似，满足移动计算平台需要。

2 DAA-ED 方案及认证协议的安全缺陷

2.1 背景知识

定义 1 强 RSA 假设（strong RSA assumption）

Flexible RSA 问题如下，设 n 是 RSA 模数，$z \in Z_n^*$ 是随机元素，指找到 $e>1$ 和 $u \in Z_n^*$，使其满足 $u^e \equiv z \bmod n$。强 RSA 假设是指不存在多项式时间算法能够以不可忽略的概率解决 Flexible RSA 问题。

定义 2 DDH 假设（decisional Diffie-Hellman assumption）

设 k 为安全参数，p,q 为素数，其中 q 的长度为 k 比特，且 $q \mid p-1$，g 是阶为 q 的群 Z_p^* 中元素，对于任何的多项式时间算法，若 x,y,z 是从 Z_p 中均匀选择的，则 $Q_0=\{<p,g,g^x,g^y,g^{xy}>: x,y \leftarrow^R Z_p\}$ 与 $Q_1=\{<p,g,g^x,g^y,g^z>: x,y \leftarrow^R Z_p\}$ 的概率分布是计算不可区分的。

定义 3 CDH 假设（computational Diffie- Hellman assumption）

设 k 为安全参数，p,q 为素数，其中 q 的长度为 k 比特，且 $q \mid p-1$，g 是阶为 q 的群 Z_p^* 中元素，对于任何的多项式时间算法 A，若 x,y 是从 Z_p 中均匀选择的，则 $\Pr[A(p,q,g,g^x,g^y)=g^{xy}]$ 可忽略。

2.2 DAA-ED 方案介绍

DAA-ED 方案包括 3 类参与方：包括证书颁发者 I（issuer）、可信计算平台 P（包括 host 与 TPM）和验证者 V（verifier）。该方案的实施过程：首先，由证书颁发者产生系统公共参数和群主密钥以用于生成群成员的证书；通过与颁发者的交互，TPM 获得其群成员证书，同时，公共证书和 TPM 的身份信息由颁发者存储在相应的数据库中；接着，TPM 利用私钥等对认证消息进行匿名签名并发送给验证者，验证者验证签名消息以确定其自合法的 TPM，但未获知具体身份信息；需及时检测失效 TPM，并排除出颁发者群。具体而言，该过程包括以下阶段：系统参数设定、加入协议、认证协议和失效 TPM 的检测等。

1) 系统参数设定

由证书颁发者 I 选择并产生系统的公共参数 $n,g,\alpha,l_c,l_s,l_b,X,Y,H$。其中，$n$ 是 RSA 模数，且 $n=pq$，p 和 q 至少是 σ bit 的长度，且 $p=2p'+1$，$q=2q'+1$，p',q' 均为素数；g 是循环群 QR_n 的随机生成元。n,g 被公开，p,q 由群管理员秘密保存；α,l_c,l_s,l_b 是安全参数，其值均大于 1；X,Y 为常量整数，且满足 $Y>2^{\alpha(l_c+l_b)+1}$，$X>2Y+2^{\alpha(l_s+l_c)+2}$。其

中，H 为散列函数定义为 $H:\{0,1\}^{*}\to\{0,1\}^{l_c}$，并具有强抗碰撞性。

2) 加入协议

TPM 加入证书颁发者群，从而获得其群成员身份证书即密钥对 (E,s)，其中，s 是素数，且满足 $s\in(X,X+2^{l_s})$，$E^s\equiv g \bmod n$，s 由 TPM 秘密保存并被 TPM 作为私钥使用。

3) 直接匿名认证协议

对于消息 m，可信计算平台 P 与验证者 V 执行以下全匿名认证协议完成验证者 V 对可信计算平台 P 的验证。

①平台 P 产生随机数 $b\in_R[Y-2^{l_b},\ Y+2^{l_b}]$，$t_1\in_R\pm\{0,1\}^{\alpha(l_s+l_c)}$，$t_2\in_R\pm\{0,1\}^{\alpha(l_b+l_c)}$，计算 $T_1=E^b \bmod n$，$T_2=g^b \bmod n$；$d_1=T_1^{t_1} \bmod n$，$d_2=g^{t_2} \bmod n$。

②平台 P 计算 $c=H(g\|T_1\|T_2\|d_1\|d_2\|m)$；并计算 $w_1=t_1-c(s-X)$，$w_2=t_2-c\ (b-Y)$。

③平台 P 发送消息 (c,w_1,w_2,T_1,T_2) 给验证者 V。

④验证者 V 计算 $c'=H(g\|T_1\|T_2\|T_1^{w_1-cX}T_2^{c}\|g^{w_2-cY}T_2^{c}\|m)$，检查 $c=?c'$，$w_1\in?\pm\{0,1\}^{\alpha(l_s+l_c)+1}$ 和 $w_2\in?\pm\{0,1\}^{\alpha(l_b+l_c)+1}$，如果都正确，则完成对 TPM 的认证。

4) 失效 TPM 的检测

被攻击者攻陷的或已失效的 TPM 的秘密值 (EK,E,s) 被公布在公开撤销列表之中。根据撤销列表中公布的 (E,s)，验证者 V 检查 $T_1^s=?T_2 \bmod n$ 是否成立来判断访问请求是否自己失效的 TPM。

2.3 DAA-ED 方案认证协议的安全缺陷

分析发现，由于 DAA-ED 方案中验证者对可信计算平台签名消息正确性的单向验证，其认证协议存在安全缺陷。当该认证协议应用于具体的远程证明时，会遭受针对可信计算平台的 2 类安全攻击：重放攻击和平台伪装攻击。

1) 重放攻击

假设可信计算平台 P 与验证者 V 的某次会话消息 (c,w_1,w_2,T_1,T_2) 被攻击者 A 所截获，且要发送的消息 m 由平台 P 选择。攻击者 A 将此消息重放给验证者 V，验证者 V 通过验证算法计算 c，接着检查 w_1,w_2 的正确性。消息 (c,w_1,w_2,T_1,T_2) 由合法的 TPM 产生，满足 $c=H(g\|T_1\|T_2\|T_1^{w_1-cX}T_2^{c}\|g^{w_2-cY}T_2^{c}\|m)$，$w_1=t_1-c(s-X)$，$w_2=t_2-c(b-Y)$，可以被正确的验证，重放攻击成功。

2) 平台伪装攻击

结合实例，给出攻击者 A 针对认证协议的平台伪装攻击。假设攻击者 A 控制了 2 个计算平台，分别是：可信计算平台 P 和非可信计算平台 P’，攻击者尝试过将 P’伪装成 P 来欺骗验证者 V，该平台伪装攻击的简要过程如图 1 所示。

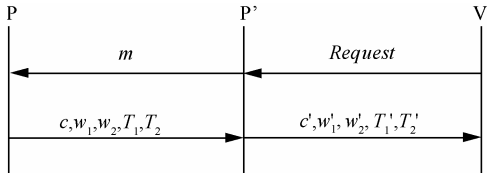

图 1　平台伪装攻击实例

①攻击者 A 通过非可信计算平台 P’，将需要签名的消息 m 转发给可信计算平台 P。

②收到 m 后可信计算平台 P 对消息进行签名，即分别计算 $T_1=E^b \bmod n$，$T_2=g^b \bmod n$；$d_1=T_1^{t_1} \bmod n$，$d_2=g^{t_2} \bmod n$，$c=H(g\|T_1\|T_2\|d_1\|d_2\|m)$；$w_1=t_1-c(s-X)$，$w_2=t_2-c(b-Y)$，$b,t_1,t_2$ 是 P 按要求所产生的正确随机数。随后，P 将消息 (c,w_1,w_2,T_1,T_2) 发送给 P’。

③P’按照验证要求，重新计算发给验证者 V 的消息：$c'=c$，$w_1'=w_1$，$w_2'=w_2$，$T_1'=T_1$，$T_2'=T_2$，并发送消息 (c',w_1',w_2',T_1',T_2') 给验证者 V。

④验证者 V 检查消息 (c',w_1',w_2',T_1',T_2') 的正确性，因为该消息来自合法的 TPM，满足 $c'=H(g\|T_1'\|T_2'\|(T_1')^{w_1'-c'X}(T_2)^{c'}\|g^{w_2'-c'Y}(T_2')^{c'}\|m)$，$w_1'\in\pm\{0,1\}^{\alpha(l_s+l_c)+1}$ 和 $w_2'\in\pm\{0,1\}^{\alpha(l_b+l_c)+1}$，能够通过验证者的验证。因此，验证者 V 认为 P’是合法的可信计算平台。

利用该攻击，攻击者 A 将非可信计算平台伪装成可信计算平台，成功欺骗验证者为其提供服务。

3　改进的直接匿名证明认证协议

DAA-ED 方案所提供的认证协议存在单向性，不能有效地抵抗重放攻击和平台伪装攻击。针对此安全缺陷，提出新的直接匿名认证协议，在原协议的基础上增加双向认证功能，在认证的同时进行可信计算平台与验证者之间的会话密钥协商，对认证协议进行优化，提高协议执行效率，在满足安全性的前提下，可信计算平台中的 Host 和 TPM 分别计算各自的数据量，Host 完成对 T_1,T_2,d_2,w_2 的计算，TPM 完成对 d_1,w_1 的计算。改进的直接匿名认证协

议是可信计算平台 P（包括 Host 和 TPM）与验证者 V 之间的具有会话密钥协商功能的双向认证协议，实施步骤如图 2 所示。

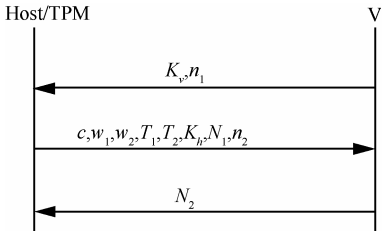

图 2 改进的直接匿名认证协议

1) 验证者 V 产生并公布公钥参数 p_v, g_v，$g_v \in GF(p_v)$，产生秘密数 x，计算 $K_v = g_v^x \bmod p_v$，选择随机数 n_1，验证者 V 发送 (K_v, n_1) 给 Host。

2) Host 产生随机数 $b \in_R [Y - 2^{l_b}, Y + 2^{l_b}]$，$t_2 \in_R \pm\{0,1\}^{\alpha(l_b+l_c)}$，分别计算：$T_1 = E^b \bmod n$，$T_2 = g^b \bmod n$，$d_2 = g^{t_2} \bmod n$。

3) TPM 产生随机数 $t_1 \in_R \pm\{0,1\}^{\alpha(l_s+l_c)}$，计算 $d_1 = T_1^{t_1} \bmod n$，发送 d_1 给 Host。

4）Host 选择秘密数 y，计算 $K_h = g_v^y \bmod p_v$，$K = (K_v)^y \bmod p_v$。

5) Host 计算 $c = H(g \| T_1 \| T_2 \| d_1 \| d_2 \| K \| m)$，$w_2 = t_2 - c(b - Y)$，发送 c 给 TPM。

6) TPM 计算 $w_1 = t_1 - c(s - X)$，发送 w_1 给 Host。

7) Host 计算 $N_1 = \{n_1\}_K$，产生随机数 n_2，发送 $(c, w_1, w_2, T_1, T_2, K_h, N_1, n_2)$ 给验证者 V。

8) 验证者 V 计算 $K = (K_h)^x \bmod p_v$，解密 N_1，验证 n_1 的正确性，验证者 V 计算 $c' = H(g \| T_1 \| T_2 \| T_1^{w_1 - cX} T_2^c \| g^{w_2 - cY} T_2^c \| K \| m)$，接受签名当且仅当 $c = c'$，$w_1 \in \pm\{0, 1\}^{\alpha(l_s+l_c)+1}$，$w_2 \in \pm\{0,1\}^{\alpha(l_b+l_c)+1}$ 同时满足。

9) 验证者 V 计算 $N_2 = \{n_2\}_K$，发送 N_2 给 Host。

DAA-ED 方案同时提供了一种可变匿名认证协议用来实现部分匿名，采用 LCID（linkability class identifier）在所设定的有效时间段内区分不同的 TPM，同样容易遭受重放攻击和平台伪装攻击，其改进方法与上述方法相同。另外，对于失效 TPM 的检测方法与原方案相同，因此不再复述。

4 协议分析

改进方案仍然基于 CM 签名方案构建，只有拥有合法密钥对 (E,s) 的 TPM 及可信计算平台能够提供正确的签名信息，其签名正确性的证明可参考文献[10]。本节重点分析改进方案的安全性，即不可伪造性、匿名性、抗平台伪装攻击和抗重放攻击。

4.1 不可伪造性

定理 1 基于强 RSA 假设，攻击者 A 在不知道合法 TPM 的密钥对 (E,s) 的情况下，不能伪造签名信息。

证明 首先，攻击者 A 可以选择直接猜测的方法，对正确的 TPM 密钥对 (E,s) 进行猜测，进而对消息 m 进行签名，并与验证者进行交互认证。

假设 $P(\cdot)$ 是攻击者 A 构造的概率多项式时间算法，利用该算法攻击者成功的猜测了合法的 TPM 密钥对 (E,s)，接着攻击者 A 就可以利用该密钥对对签名消息进行伪造以欺骗验证者 V，并且由算法 $P(\cdot)$ 猜测的密钥对 (E,s) 必然满足 $E^s \equiv g \bmod n$，且 s 为素数，$s \in (X, X + 2^{l_s})$。由此，利用算法 $P(\cdot)$ 可以在多项式时间内找到数对 $(u = E, v = s)$，满足 $u^v \equiv z \bmod n$，即该算法可以解决 flexible RSA 问题，与强 RSA 假设矛盾，因此，攻击者 A 不能通过直接猜测的方法得到合法的 TPM 密钥对 (E,s)。

其次，攻击者 A 可以在已知多个 TPM 密钥对的基础上，对合法 TPM 的密钥对进行计算与猜测。

假设攻击者 A 以某种方式提前获知多个合法密钥对 $(E_1, s_1), (E_2, s_2), \cdots, (E_k, s_k)$，以此为基础，攻击者成功构造概率多项式时间算法 $P(\cdot)$，从而产生新的满足条件 $E^s \equiv g \bmod n$，$s \neq s_i$，$1 \leqslant i \leqslant k$ 的合法密钥对 (E,s)，那么，A 可以利用新密钥伪造合法的 TPM 签名信息。接下来，给出主要的证明思路，更详细的证明过程由文献[9]给出。

给定随机输入 (u,n)，如果其满足条件 $GCD(u,n) \neq 1$，则可以得到 n 的因子，并容易地解决 flexible RSA 问题。此时，就可以利用该算法成功的解决 flexible RSA 问题。因此需要排除这种情况，并假设 $u \in Z_n^*$，$GCD(u,n) = 1$ 成立。

1) 随机地选择 k 个素数 $s_1, s_2, \cdots, s_k$，满足 $s_i \in [X - 2^{\alpha(l_s+l_c)+1}, X + 2^{\alpha(l_s+l_c+1)}]$，其中 $1 \leqslant i \leqslant k$，并计算 $r = s_1 s_2 \cdots s_k$，$g = u^r = u^{s_1 s_2 \cdots s_k} \bmod n$。由于 s_i 是素数且严格小于 p' 或者 q'，同时满足 $GCD(r, |QR_n|) = 1$。因此，容易得到当且仅当 u 是 QR_n 的生成元，g 是 QR_n 的一个生成元。

2) 利用 s_i 和 E_i 计算可产生 k 组密钥对：$E_1 = u^{s_2 \cdots s_k} \bmod n$，$E_2 = u^{s_1 s_3 \cdots s_k} \bmod n$，…，$E_k = u^{s_1 s_2 \cdots s_{k-1}}$。

$\bmod n$。接着，对于所有的$i=1,\cdots,k$，计算E_i的s_i次方：$E_i^{s_i}=u^{s_1s_2\cdots s_k}=u^r=g \bmod n$。

3) 利用伪造算法$P(\cdot)$，产生一个新的密钥对(E,s)，并且满足$s\in[X-2^{\alpha(l_s+l_c)+1},\ X+2^{\alpha(l_s+l_c)+1}]$，$E^s=g=u^r \bmod n$。

4) 如果伪造算法是成功的，那么$s\neq s_i$，且s不能是s_i,s_j的乘积，其中$1\leqslant i,j\leqslant k$。此时，条件$GCD(s,s_1s_2\cdots s_k)=1$和$GCD(s,s_1s_2\cdots s_k)=s_i$只能有一个成立，$1\leqslant i\leqslant k$。假设$GCD(s,s_1s_2\cdots s_k)=1$成立，则通过计算可以找到$(w,s)$，满足$w^s=u \bmod n$，此时数对$(w,s)$成为解决 flexible RSA 问题的实例。如果$GCD(s,s_1s_2\cdots s_k)=s_i$时，假设$s=v\times s_i$，则$v<X-2^{\alpha(l_s+l_c)+1}$，$GCD\ (v,s_1s_2\cdots s_k)\ =1$（或$GCD(v,r)=1$）成立，于是得到$E^s\equiv E^{vs_i}\equiv u^r \bmod n$。则通过计算可以找到密钥对$(w,v)$，满足$w^v=u \bmod n$，此密钥对是解决 flexible RSA 问题的实例。结合这 2 种情况，攻击者 A 的伪造算法$P(\cdot)$能以不可忽略的概率在多项式时间内解决 flexible RSA 问题，与强 RSA 假设矛盾。

因此，通过直接猜测或者在已知多对合法密钥的基础上，攻击者 A 都不能完成对新的合法 TPM 签名信息的伪造，改进方案满足不可伪造性。

4.2　匿名性

本方案的匿名性是指 TPM 进行远程证明时不暴露其真实身份；同时，验证者不能将产生自同一个 TPM 的 2 个不同的会话进行关联；另外，每次认证交互 TPM 均与验证者产生不同的会话密钥，验证者无法将其进行关联。

定理 2　基于 DDH 假设，改进协议实现了验证者 V 对合法 TPM 的匿名认证。

证明　首先，由于采用群签名和知识证明方法实现对消息的签名和认证，因此，在改进协议中验证者没有获知 TPM 的真实身份。交互认证中验证者 V 通过对签名消息的验证，仅能确认该 TPM 来自正确的颁发者群，而不能揭示或得到其具体的身份。因此，接下来将证明验证者不能将来自同一个 TPM 的多次不同会话进行关联的情况。

其次，为了判断 2 个会话是否与同一个 TPM 关联，验证者 V（或者恶意攻击者）需要判断等式$T_1,T_2\equiv g^b\equiv T_1^s \bmod n$和$T_1^{'},T_2^{'}\equiv g^{b'}\equiv(T_1^{'})^s \bmod n$是否由相同的$E$产生。

基于 DDH 假设，并由于$T_1,T_1^{'}$是QR_n的随机生成元，因此，无法判断是否存在一个s使得$T_1^s\equiv T_2$，$(T_1^{'})^s\equiv T_2^{'}$。所以，验证者不能将来自同一个 TPM 的多次不同会话进行关联。

再次，每次相互认证时可信平台 P 与验证者 V 均协商新的会话密钥K_n。即使是基于相同的公共参数(p_v,g_v)进行协商，新的会话密钥K_n也会完全不同于旧的会话密钥K，具有强的一次一密性，且满足前向保密性要求，此时，即使旧的会话密钥K被验证者 V 获得，也不能将K_n与K进行关联。

4.3　抵抗平台伪装攻击

定理 3　基于 CDH 假设，改进协议能够有效地抵抗可信计算平台伪装攻击。

证明　假设$P(\cdot)$是攻击者 A 构造概率多项式时间算法，利用该算法攻击者成功的完成伪装攻击，那么算法$P(\cdot)$将会按照以下 2 种方式发起对协议的攻击。

1) 非可信计算平台 P’在攻击者 A 控制下诚实地将消息转发给可信计算平台 P 和验证者 V，但不能从消息中获得任何有用的信息，一方面可以通过增加时间戳来避免，不在本文的讨论之中，另一方面，接下来的会话在共享密钥K加密保护下进行，攻击者仍然不会得到有用信息。

假设攻击者 A 所控制的非可信平台 P’分别与 P 和 V 进行的交互过程如下：P’在收到验证者 V 发送来的消息(K_v,n_1)后，诚实地将其转发给 P；P 计算相应的消息并发送$(c,w_1,w_2,T_1,T_2,K_h,N_1,n_2)$给 P’，P’再次将消息如实地转发给 V；V 对消息的正确性验证后，发送N_2给 P’，P’转发N_2给 P，P 验证N_2的真确性。P’作为诚实的消息转发者帮助 P 和 V 完成相互认证，但是，在此过程中攻击者 A 除了如实地转发消息外，没有获得任何有用信息。

随后，如果攻击者 A 利用构造的攻击算法$P(\cdot)$计算出 P 和 V 的共享密钥K，那么仍可以实施平台伪装攻击。但是，基于 CDH 假设，算法$P(\cdot)$在已知K_v和K_h的情况下，不能计算出K。在接下来的会话中，P 与 V 之间的消息由密钥K加密保护，攻击者仍然不能所获任何有用信息，平台伪装攻击失败。

2) 攻击者 A 以中间人角色分别与可信平台 P 以及验证者 V 协商密钥，同时试图发起对协议的伪装攻击，其攻击过程描述如下。

验证者 V 发送消息(K_v,n_1)给 P’，P’选择自己

的秘密数 z，产生随机数 n_a，计算并产生新的密钥 $K_p = g_v^z \bmod p_v$，发送 (K_p, n_a) 给可信平台 P；P 随后计算签名信息 $c = H(g \| T_1 \| T_2 \| d_1 \| d_2 \| K_1 \| m)$，$w_1 = t_1 - c(s - X)$，$w_2 = t_2 - c(b - Y)$，$T_1 = E^b \bmod n$，$T_2 = g^b \bmod n$，$K_1 = (K_p)^y \bmod p_v$，$N_1 = \{n_a\}_{K_1}$，并发送消息 $(c, w_1, w_2, T_1, T_2, K_h, N_1, n_2)$ 给 P’；收到消息后，P’可以按照以下方法计算发送给 V 的消息，并进行伪装攻击。

首先，P’计算与验证者 V 的共享密钥，即计算 $K_2 = (K_v)^z \bmod p_v$，利用共享密钥 K_2 替换 K_1 重新计算 $N_1^{'} = \{n_1\}_{K_2}$。由定理 1 可知，攻击者不能够伪造 P 的签名信息，因此，只能简单的使 $c_1 = c$。随后，P’产生随机数 n_b，并发送消息 $(c_1, w_1, w_2, K_p, N_1^{'}, T_1, T_2, n_b)$ 给验证者 V。

验证者 V 收到消息后，计算其与 P’的共享密钥 $K_2 = (K_p)^x \bmod p_v$，计算签名信息 $c_1^{'} = H(g \| T_1 \| T_2 \| T_1^{w_1 - cX} T_2^c \| g^{w_2 - cY} T_2^c \| K_2 \| m)$，而此时，很明显由于 $c_1^{'} \neq c_1$，验证失败。

4.4 抵抗重放攻击

由于改进的认证协议中增加了双方的密钥协商，因此，能够有效地防范重放攻击。假设攻击者 A 截获了可信计算平台 P 旧的会话消息 $(c, w_1, w_2, T_1, T_2, K_h, N_1, n_2)$。在不知道 K_v 的情况下，攻击者 A 直接将此消息发送给 V，因为验证者 V 每次使用新的 K_v 来完成认证，本次交互协商的会话密钥 K 与旧消息中使用的会话密钥不同，很明显 c 值不满足验证要求，重放攻击不能成功。

假设攻击者 A 以某种方式得到了本次会话中验证者 V 的密钥 K_v，那么 A 可以选择计算新的密钥及验证消息以欺骗 V，这与定理 3 证明中的第一种情况类似，旧的会话消息不能通过验证，重放攻击不能成功。同时，上述消息中引入了随机数 n_1, n_2，且随时数 n_1 由密钥 K 进行加密，也可阻止重放攻击的发生。

5 性能分析

移动计算平台的计算资源有限，因此运算量成为衡量其认证协议性能的重要因素之一。将本文改进方案与 BCC 方案、DAA-ED 方案的运算量进行分析对比，其结果如表 1 所示，分析时仅考虑认证协议的计算代价，且分别计算移动平台中的 Host 与 TPM 的运算量。其中，EX 为模指数运算，M 为乘法运算，EK 为对称加密运算，DK 为对称解密运算，H 为散列运算。

表 1 协议运算量对比

名称	可信计算平台		验证者计算量
	Host 计算量	TPM 计算量	
BCC	14EX+25M+1H	8EX+8M+2H	23EX+5M+4H
DAA-ED	3EX+1M+1H	1EX+1M	4EX+2M+1H
本方案	5EX+1M+1H+1EK	1EX+1M	6EX+2M+1H+1DK

从表 1 可以看出，与 BCC 方案相比，虽然改进方案的认证协议中分别增了 1 次对称加密运算和 1 次对称解密运算，但是协议中对计算资源消耗最为显著的模指数运算和乘法运算次数显著减少。具体地，对于计算平台，改进方案的认证协议中模指数运算次数约是 BCC 方案的 1/4，乘法运算次数约是 BCC 方案的 1/16；对于验证者，改进协议中模指数运算次数约为 BCC 方案的 1/4，乘法运算次数约为 BCC 方案的 1/3。总体上，与 BCC 方案相比在应用于远程证明时，改进方案的认证协议无论在运算量或者交互复杂度上都比 BCC 有显著的减少，适用于笔记本、PDA 等移动计算平台。

由于改进方案的认证协议中增加了计算平台与验证者之间的密钥协商和双向认证，因此与 DAA-ED 方案相比，对于计算平台，改进协议增加了 2 次模指数运算和 1 次对称加密运算，对于验证者，改进协议增加了 2 次模指数元素和 1 次对称解密运算。可信计算环境中，远程证明的验证者一般是运算资源和能力较强的服务器[11]，因此，这里仅考虑改进协议中移动计算平台的运算量和效率。

认证协议中，模指数运算对于计算资源的消耗最为显著，与 DAA-ED 方案相比，本协议在计算平台所增加的模指数运算，可利用重复平方乘算法[12]将其转化为模平方运算和乘法运算的方式以有效地提高计算效率，即给定指数运算，设 m_1 为指数的比特长度，m_2 为二进制表示是“1”的个数，则计算复杂度可以被估算为 m_1 次模平方运算和 m_2 次乘法运算。设改进方案中 x 和 y 的长度均为 512 bit，按照重复平方乘算法，转化后的计算量分别为 1 024 次模平方运算和 512 次乘法运算。计算平台中增加的运算量主要由 Host 承担，不对 TPM 造成计算负担。因此，与 DAA-ED 方案的认证协议比较，改进协议在计算平台中增加的运算量不对协议产生大

的影响，仍然适用于移动计算平台。

改进方案中采用基本 DH 算法来进行密钥协商，而本方案进行实际应用时，可以采用基于椭圆曲线的密钥交换协议来缩减运算量，仍有性能提升的空间。因此，对于移动计算平台如笔记本、PDA 等，改进方案的认证协议完全适用。

6　结束语

本文提出的适用于移动计算平台的直接匿名方案是在原 DAA-ED 方案认证协议的基础上增加基于密钥协商的双向认证功能，即保持方案不可伪造性和匿名性的同时，能够有效地抵抗重放攻击和平台伪装攻击，性能分析表明，改进协议适用于移动计算平台的远程证明。进一步的工作，包括可实际应用的基于椭圆曲线的密钥交换协议的方案以及移动切换场景中的远程证明方案设计与实现。

参考文献：

[1] Trusted Computing Group. Summary of features under consideration for the next generation of TPM[EB/OL]. http://www. trustedcomputinggroup.org, 2009.

[2] BALFE S, GALLERY E, MITCHELL C J, *et al*. Challenges for trusted computing[J]. IEEE Security & Privacy, 2008,6(6):60-66.

[3] Trusted Computing Group. Trusted computing platform alliance (TCPA) main specification version 1.1b[EB/OL]. http://www. trustedcomputinggroup.org, 2001.

[4] BRICHELL E, CAMENISCH J, CHEN L Q. Direct anonymous attestation[A]. Proceedings of the 11th ACM Conference on Computer and Communications Security[C]. New York, NY, USA, 2004. 132-145.

[5] EMANUELE C, HANS L, GIANLUCA R, *et al*. Anonymous authentication with TLS and DAA[A]. TRUST 2010, LNCS 6101[C]. 2010. 47-62.

[6] WALKER J, LI J T. Key exchange with anonymous authentication using DAA-SIGMA protocol[A]. INTRUST 2010, LNCS 6802[C]. 2011. 108-127.

[7] CAMENISCH J, LYSYANSKAY A. Dynamic accumulators and application to efficient revocation of anonymous credentials[A]. Cryptology — CRYPTO 2002[C]. Springer Verlag, 2002. 61-76.

[8] CAMENISCH J, STADLER M. Efficient group signature schemes for large groups[A]. CRYPTO '97[C]. Springer Verlag, 1997. 410-424.

[9] GE H, TATE S R. A direct anonymous attestation scheme for embedded devices[A]. PKC 2007[C]. Springer, Heidelberg, 2007.

[10] CAMENISCH J, MICHELS M. A Group Signature Scheme Based on an RSA-Variants[R]. Technical Report RS-98-27, BRICS, University of Aarhus, 1998.

[11] REHBOCKA S, HUNT R. Trustworthy clients: extending TNC to Web-based environments[J]. Computer Communications, 2009,32(5): 1006-1013.

[12] MENEZES A J, OORSCHOT P C, VANSTONE S A. Handbook of Applied Cryptography[M]. CRC Press, Inc, 1997. 613-619.

作者简介：

杨力（1977-），男，陕西乾县人，博士，西安电子科技大学副教授，主要研究方向为密码学、可信计算及网络安全等。

张俊伟（1982-），男，陕西西安人，博士，西安电子科技大学副教授，主要研究方向为密码学、安全协议等。

马建峰（1963-），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为网络与信息安全、密码学等。

刘志宏（1967-），男，湖南常德人，博士，西安电子科技大学副教授，主要研究方向为密码学、安全协议等。