基于非对称双线性对的直接匿名认证方案

甄鸿鹄[1,2]，陈越[1]，谭鹏许[1]，郭渊博[1]
(1. 解放军信息工程大学 电子技术学院，河南 郑州，450004；2. 解放军 63612 部队，甘肃 瓜州 736100)

摘 要：根据国产可信密码模块(TCM, trusted cryptography module)的直接匿名认证需求，基于非对称双线性对(ABP, asymmetric bilinear pairing)，提出了一种全新的 DAA 方案——ABP-DAA 方案，与已有 DAA 方案相比，其不仅能够适用于 TCM 的直接匿名认证，而且更加安全、简单、高效。

关键词：可信计算；可信平台认证；直接匿名认证；双线性对；椭圆曲线密码算法
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2010)8A-0037-07

Asymmetric bilinear pairing based direct anonymous attestation scheme

ZHEN Hong-hu[1,2], CHEN Yue[1], TAN Peng-xu[1], GUO Yuan-bo[1]
(1. Institute of Electronic Technology, The PLA Information Engineering University, Zhengzhou 450004, China;
2. PLA No.63612 Unit, Guazhou 736100, China)

Abstract: In order to achieve the direct anonymous attestation need of chinese domestic trusted cryptography module (TCM), based on asymmetric bilinear pairings, a presentation of the bran-new DAA scheme: ABP-DAA scheme was given. Comparing with the existing DAA schemes, ABP-DAA scheme is not only adaptable for TCM, but also more secure, more simple and efficient.

Key words: trusted computing; trusted platform attestation; direct anonymous attestation (DAA); bilinear pairing; elliptic curve cryptography

1 引言

可信计算[1]的概念由可信计算组织(TCG, trusted computing group)提出，TCG 对于可信的定义是：一个实体是可信的，如果它的行为总是以预期的方式达到预期的目标。TCG 实现可信计算的核心是可信平台模块(TPM, trusted platform module)，TPM 是一个具有物理防篡改、能进行密码运算等功能的安全微控制器（密码芯片），内部集成了 CPU、RAM、ROM、Flash、加密算法协处理器、随机数产生器、安全防护等模块。每个 TPM 具有一个唯一的凭证密钥(EK, endorsement key)与之对应，EK 是非对称密钥，一般由 TPM 的生产厂家植入其中，EK 私钥将秘存于 TPM 内部，而其公钥及证书可作为 TPM 芯片的身份标识。

可信计算中的一个基本问题是可信平台认证，可信平台认证是指一个计算平台（如 PC 机）向远程系统提供自己的安全属性的证明，也即证明其是可信的。TCG 基于可信平台模块来实现平台的可信认证：1) TPM 对平台的完整性（也即可信性）进行度量，并将完整性度量值保存在 TPM 内部的平台配置寄存器(PCR, platform configuration register)中；2) 通过 TPM 向远程系统（验证方）证明平台的身份是可信的；3) TPM 将 PCR 中的值及平台对其的签名发送给验证方进行验证，验证通过则平台就是可信的。

收稿日期：2010-06-05

实现可信平台认证的最直接的办法是用 EK 来标示平台身份，并用 EK 对 PCR 中的值进行签名。但是，EK 可以唯一地标识一个 TPM，每次认证中都使用固定的 EK，极易造成平台用户行为被人跟踪，造成隐私的泄露，从而增加平台用户对使用 TPM 的顾虑，不利于可信认证的应用推广。因此，在认证的过程中保持平台身份的匿名（也即实现在证明自己身份可信的同时，不让验证方知道自己具体是谁）是非常重要的。

2 研究现状及意义

为了实现可信平台的匿名认证，TCG 在其 TPM v1.1b 标准中给出了 Privacy CA 匿名认证方案，在 TPM v1.2 标准中给出了直接匿名认证(DAA, direct anonymous attestation)方案。

Privacy CA 方案[2]采用一次一密的签名方式实现认证过程的匿名性。TPM 为每次认证产生不同的身份认证密钥(AIK, attestation identity key)，并将 AIK 公钥连同 EK 的公钥发送给叫做 Privacy CA 的可信第三方，Privacy CA 对 AIK 公钥颁发证书以实现对其合法性的证明。这样，每次认证时 TPM 使用 AIK 代替 EK 对 PCR 的值进行签名。由于每次认证时 TPM 向验证者出示的 AIK 公钥各不相同，因而验证者无法分辨对方是否是同一 TPM，平台用户的行为也就无法被跟踪。Privacy CA 方案简单易行，但也存两个比较明显的缺点：1) 由于每个 TPM 的每次认证均要向 Privacy CA 申请证书，Privacy CA 成为影响认证效率的瓶颈；2) 如若验证者与 Privacy CA 串通，则认证的匿名性无法确保。

DAA 方案[3]在实现身份合法性证明的同时，对 AIK 公钥进行了签名，也使得 AIK 成为 EK 的替代。DAA 方案有效克服了 Privacy CA 方案的缺点，具有如下特性。1) 直接：平台与可信发布方（Issuer，功能类似 Privacy CA）运行完 Join 协议后，平台获得一个 DAA 证书，之后的每次认证平台将直接向验证方进行认证，不再需要 Issuer 的参与，故可解决 Privacy CA 响应瓶颈的问题；2) 匿名：平台通过零知识证明协议证明其拥有一个合法的 DAA 证书，同时不泄露 DAA 证书的内容，这在验证者与证书发布方串通起来情况下，也能确保平台的匿名性；3) 认证：假设发布方是可信的，那么发布方只有在验证了平台 TPM 的 EK 公钥是可信或合法的之后，才向平台颁发 DAA 证书，故一个平台拥有 DAA 证书就证明平台拥有一个可信的 TPM。

但是，DAA 方案要比 Privacy CA 方案复杂的多，大量的指数计算和零知识证明使得方案计算开销较大，这将不利于其实际的应用。DAA 方案协议复杂、时间开销过大的问题已成为其面临最为主要的问题，因此研究更加简单，更加高效的 DAA 方案将是非常有意义的。

更为重要的是，根据我国国家密码管理局颁布的《可信计算密码支撑平台功能与接口规范》[4]，我国拥有自主知识产权的可信计算密码模块（TCM, trusted cryptography module，功能类似 TPM），采用的是 Privacy CA 方案，目前还没有直接匿名认证方案。而现有 DAA 方案主要是针对 TPM 设计的，对于完全采用椭圆曲线密码算法的 TCM 难以适用。故而研究可适用于 TCM 的 DAA 方案具有十分重要的现实意义。

为此，本文基于非对称双线性对，提出了一种全新的 DAA 方案——ABP-DAA 方案，并就其性能及对于 TCM 的适用性进行了详尽的分析。

3 预备知识

3.1 双线性对及困难性问题假设

双线性对[5,6]的定义如下。

设 2 个加法循环群 G_{1+}、G_{2+} 和一乘法循环群 $G_{\times}$ 的阶均为素数 q，G_{1+}、G_{2+} 及 $G_{\times}$ 中的离散对数问题都是困难的，映射 ： $G_{1+}\times G_{2+}\to G_{\times}$ 如果满足如下条件。

1) 双线性：对于任意 $P_{1-1}, P_{1-2}\in G_{1+}$, $P_2\in G_{2+}$, 满足 $(P_{1-1}+P_{1-2}, P_2)= (P_{1-1}, P_2)\ (P_{1-2}, P_2)$，对于任意 $P_1\in G_{1+}$，P_{2-1}，$P_{2-2}\in G_{2+}$，满足 $(P_1, P_{2-1}+P_{2-2})= (P_1, P_{2-1})\ (P_1, P_{2-2})$；

2) 非退化性：存在 $P_1\in G_{1+}$，$P_2\in G_{2+}$，使得 $(P_1, P_2)\neq 1$，其中 1 为 $G_{\times}$ 的幺元；

3) 可计算性：任取 $P_1\in G_{1+}$, $P_2\in G_{2+}$，存在有效算法计算 (P_1, P_2)。

则称映射 ： $G_{1+}\times G_{2+}\to G_{\times}$ 为一双线性对，或称之为一个双线性映射。

上述定义中，如果 $G_{1+}\neq G_{2+}$，则称映射 ： $G_{1+}\times G_{2+}\to G_{\times}$ 为非对称双线性对(ABP, asymmetric bilinear pairings)，而如果 $G_{1+}=G_{2+}=G_{+}$，则称映射 ： $G_{1+}\times G_{2+}\to G_{\times}$ 为对称双线性对(SBP, symmetric bilinear pairings)。对称双线性对可视为非对称双线性对的特殊情形。

目前，很多密码方案都采用的是对称性双线性对，因为对称双线性对相较非对称双线性对简单，也易于计算；但对称双线性对通常仅能从超奇异椭圆曲线上的 Weil 对或 Tate 对等得到，由于超奇异椭圆曲线的安全系数 K 最大为 6，在 MOV 攻击[7]之下，可将其上离散对数问题转换为其一个扩展有限域上的离散对数问题，故其安全性不够理想，其理论安全性要低于非对称双线性对的安全性。而非对称双线性对可以从一些普通椭圆曲线上构造，因而具有更好的安全性。而这也是本文之所以采用非对称双线性对而不采用对称双线性对来构造新 DAA 方案的主要原因。

双线性对相关密码学问题请参阅相关文献，在假定 $a, b, c, d \in Z_q^*$ 的情况下，对于与本文密切相关的几个问题定义如下。

DL 问题：对于 $P \in G_{1+}$ 或 G_{2+}，给定 aP，计算 a。

CDH 问题：对于 $P \in G_{1+}$ 或 G_{2+}，给定 aP, bP，计算 abP。

DDH 问题：对于 $P \in G_{1+}$ 或 G_{2+}，区分三元组 (aP, bP, abP)与(aP, bP, cP)。

co-CDH 问题：对于 $P_1 \in G_{1+}$、$P_2 \in G_{2+}$，给定 aP_1, bP_2，计算 abP_1。

其中，DL 问题与 CDH 问题，无论对于对称双线性对还是非对称双线性对，无论对于群 G_{1+} 还是群 G_{2+}，都是困难的。co-CDH 问题仅针对非对称双线性对，是公认困难的。DDH 问题，在对称双线性对下，其是容易的（因为 $(aP, bP) = (P, cP) \Leftrightarrow (P, P)^{ab} = (P, P)^c \Leftrightarrow ab = c \Leftrightarrow abP = cP$）；在非对称双线性对下，群 G_{2+} 中的 DDH 问题被认为是容易的，而群 G_{1+} 中的 DDH 问题通常被认为是困难的，但也有文献[8~10]指出将非对称性双线性对下 G_{1+} 中的 DDH 问题视为困难性问题存在一定的风险，因为截止目前对于其是否真正困难还知之甚少。

3.2　目前已有的几种 DAA 方案

DAA 方案（为了与其他方案作区分，以下称 DAA 方案也即原 DAA 方案为 BCC-DAA 方案，凡本文中无特殊说明，所有 DAA 方案均指 BCC-DAA 方案）在 2004 年正式提出之后，其原作者于 2008 年又给出了 2 种改进 DAA 方案（BCL-DAA 方案与 CMS-DAA 方案），2006 年文献[17]还给出了一种基于不经意传输的 DAA 方案（OT-DAA 方案），现将这几个方案简介如下。

1) BCC-DAA 方案[11]：是最初始的 DAA 方案，并被 TCG 所提 TPM v 1.2 标准[3]采用且沿用至今，主要基于强 RSA 假设的 C-L 签名[11]和零知识证明技术实现。基本的思想是：可信平台产生秘密数据 (f_0, f_1)，然后基于 TPM 的 EK 公钥向可信发布方(Issuer)申请有关(f_0, f_1)的 DAA 证书，之后可信平台在向验证方零知识证明自己拥有Issuer颁布的DAA证书的同时，实现验证方对于平台 AIK 公钥的认证。BCC-DAA 方案自发布后受到了很多研究人员的关注，文献[12]应用其以实现 Mobile Ubiquitous Environment 中设备(如无线电话)的认证，而在文献[13]中，陈小峰与冯登国对其进行了扩展，提出了一种跨域的直接匿名认证方案。

2) BCL-DAA 方案[14,15]：与 BCC-DAA 方案的基本原理一致，该方案保存了原 DAA 方案的基本框架流程，将 BCC-DAA 方案（原 DAA 方案）中基于 RSA 的密码运算改为基于对称双线性对的运算，实现了密钥长度的减小和整体计算量的减少。

3) CMS-DAA 方案[16]：该方案可视为对 BCL-DAA 方案的改进方案。主要将 BCL-DAA 方案中的对称双线性对改为非对称双线性对，以提高方案的安全性，且 CMS-DAA 方案在性能上要优于 BCL-DAA 方案。

4) OT-DAA 方案[17]：这个方案与前 3 个方案有很大的不同，前 3 个方案主要基于零知识证明以及不同形式的 C-L 签名技术来实现，三者有着相似的结构流程，可视为是一个系列的方案（由相同作者先后提出）。OT-DAA 方案打破了前 3 个方案的框架结构，提供了一种独特的 DAA 构造方法，但是这个方案中所用不经意传输及离散对数上的 3 种零知识证明技术都比较复杂，使得方案在整体性能上难有突破。

3.3　基于非对称双线性对的 C-L 签名及 CMS-DAA 方案可能面临的问题

CMS-DAA 方案[16]的理论基础是非对称双线性对：$G_{1+} \times G_{2+} \to G_\times$ 上的 C-L 签名，其具体过程如下。

1) 密钥生成：对于 G_{2+} 的元素 P_2（P_2 是公开的），选取 $x, y \in Z_q^*$ 作为签名私钥，计算 $X = xP_2$ 及 $Y = yP_2$ 作为签名的公钥。

2) 签名：对于 $A \in G_{1+}$，计算 $B = yA$，$C = (x + mxy)A$，其中 m 为需要签名消息或数据，则对于 m 签名为(A, B, C)。

3) 验证：如果等式 $(A, Y) = (B, P_2)$与 (A, X)

$(mB, X)= (C, P_2)$成立，则(A, B, C)就是对于m的签名。

CMS-DAA 方案采用非对称双线性对，相较采用对称双线性对的 BCL-DAA 方案，从理论上讲具有更高的安全性；且文献[16]通过分析比较，认为 CMS-DAA 方案在性能上要优于 BCL-DAA 方案，当然更是远优于 BCC-DAA 方案。因此，CMS-DAA 方案被视为是目前最优的 DAA 方案。但是 CMS-DAA 方案可能面临如下问题（鉴于篇幅，其中涉及的参数及流程将不再赘述，请参见 CMS-DAA 方案[16]本身）。

CMS-DAA 方案中假设了非对称双线性对 $: G_{1+} \times G_{2+} \to G_{\times}$的群$G_{1+}$中的 DDH 问题是困难的，而群$G_{1+}$中的 DDH 问题是否真正困难，目前尚有人持怀疑态度，一旦其是容易的（对于群G_{1+}而言，如果存在群G_{1+}到群G_{2+}的同态映射，或群G_{1+}上同时还存在对称双线性对 $: G_{1+} \times G_{1+} \to G'_{\times}$，则群$G_{1+}$中 DDH 问题必定是容易的），则 CMS-DAA 方案将存在如下问题：验证方与证书发布方串通的情况下不能确保方案的匿名性。因为证书发布方可以对于所有 TPM 的 EK 对应的 F，分别计算 yF，然后对于全部 yF，逐一验证等式 $(A', yF)= (E', P_1)$是否成立，如果成立则可反推出当前进行认证的平台对应 TPM 的 EK 是什么，因而认证的匿名性将不能确保。具体而言，在 CMS-DAA 方案中，$(A', yF)= (E', P_1) \Leftrightarrow (r'rP_1, fyP_1)= (r'fyrP_1, P_1)$，而 $(r'rP_1, fyP_1)= (r'fyrP_1, P_1)$是群$G_{1+}$中的 DDH 问题。

4 基于非对称双线性对的新 DAA 方案——ABP-DAA 方案

为进一步简化 DAA 方案的流程，提高 DAA 方案的性能，本文提出了一种新的 DAA 方案——ABP-DAA 方案。ABP-DAA 方案的参于方与所有 DAA 方案相同，主要有：可信平台模块(TPM)，平台主机(Host)，证书发布方(Issuer)、验证方(Verifier)，且由于 TPM 与 Host 通常是相绑定的，故有时也将其共同视为一方。整个方案分为以下几个步骤。

4.1 初始化（Issuer 公开系统参数）

Issuer 选择有限域F_q上一可构造非对称双线性对的普通椭圆曲线，对于 $P_1 \in G_{1+}$，$P_2 \in G_{2+}$，选取 $x, y \in F_q$作为其私钥，计算 $X=xP_2$及 $Y=yP_2$作为其公钥，并且公开该椭圆曲线参数以及 $A=P_1$、$B=yP_1$、P_2。

4.2 TPM 与 Host 向 Issuer 申请 DAA 证书

1) TPM 任选$f \in F_q$，作为其内部秘密数据，并任选 $k \in F_q$，计算 $K=kP_1$，$fK=fkP_1$，并基于其 EK 公钥（通过 Host）将 K 与 fK 发送给 Issuer（具体方法同文献[11] Appendix B）。

2) Issuer 进行泄露检测：Issuer 对于黑名单上的所有f_i逐一计算f_iK，如果所有f_iK都不等于fK则进入下一步，否则中断。

3) Issuer 在判定 EK 公钥可信或合法的情况下，计算 $\tilde{C}=xK+xyfK=(x+fxy)K$，发送 $\tilde{C}$ 给 TPM。

4) TPM 计算 $C=k^{-1}\tilde{C}=k^{-1}(x+fxy)K=k^{-1}(x+fxy)kP_1=(x+fxy)P_1$，则$(A, B, C)$就是 Issuer 对于 f 的基于非对称双线性对的 C-L 签名，也即 Issuer 对于 f 颁布的 DAA 证书，TPM 在其内部秘密保存证书(A, B, C)中的 C，销毁 k，使之均不得外泄。

4.3 TPM 与 Host 向 Verifier 认证

TPM 任选 $d_i \in F_q$，计算 $A_i=d_iA$，$B_i=d_iB$，$B_i^f=d_ifB$，$C_i=d_iC$，并将 A_i、B_i、B_i^f、C_i（通过 Host）发送给 Verifier，而秘密保存 d_i。

4.4 Verifier 进行验证

1) Verifier 进行泄露检测：Verifier 对于泄露黑名单上的所有f_i逐一计算f_iB_i，如果所有f_iB_i都不等于B_i^f则进入下一步，否则中断。

2) Verifier 验证等式 $(A_i, Y)= (B_i, P_2)$与 $(A_i, X)(B_i^f, X)= (C_i, P_2)$是否成立，如果均成立，则 Verifier 接受 TPM 以 $A_i=d_iA=d_iP_1$作为 AIK 公钥，以 d_i为 AIK 私钥。

至此，整个 ABP-DAA 方案结束，并且已经达到预期目的，也即在证明身份可信或合法的同时，为一个 AIK 公钥提供了认证。事实上，等式 $(A_i, Y)= (B_i, P_2)$与 $(A_i, X)(B_i^f, X)= (C_i, P_2)$成立，说明 TPM 拥有 Issuer 颁布的 DAA 证书(A, B, C)，故 Verifier 相信该 TPM 的身份是可信或合法的，并接受其产生的 AIK 公钥，由于每次认证中 d_i不同，故而相应 A_i也是每次不同的。

之后 TPM 可以 $A_i=d_iA=d_iP_1$作为其 AIK 的公钥，以 d_i作为 AIK 的私钥，以 $A=P_1$作为基点，对消息 m（如果是可信计算平台的认证，则 m 为 PCR 中存储的平台完整性度量值）按照常规椭圆曲线签名算法进行如下签名：假定 $H()$为一散列函数，A 的阶为 q，TPM 随机选择一个整数 l，$1<l<q$，计算 $l=(x, y)$，$a=x \bmod q$，$b=l^{-1}(H(m)+ad_i) \bmod q$，则 TPM 对消息 m 的签名为(a, b)。而 Verifier 对签名(a, b)

如此验证：计算$(x', y')= H(m)b^{-1}A+ab^{-1}A_i$，$a'=x' \bmod q$，之后判断 $a'=a$ 是否成立，事实上，$(x', y')=H(m)b^{-1}A+ab^{-1}A_i=l(H(m)+ad_i)^{-1}(H(m)+ad_i)A=lA=(x, y)$，故若 $a'=a$ 成立，则 Verifier 接受这个签名。

5　方案分析

5.1　正确性

方案的正确性在于等式 $(A_i, Y)= (B_i, P_2)$与 $(A_i, X)(B_i^f, X)= (C_i, P_2)$是必定成立的，这是因为 $(A_i, Y)= (d_iA, yP_2)= (d_iP_1, yP_2)= (d_iyP_1, P_2)= (d_iB, P_2)= (B_i, P_2)$，$(A_i, X)(B_i^f, X)= (d_iA, xP_2)(d_ifB, xP_2)= (d_iP_1, xP_2)(d_ifyP_1, xP_2)= (d_iP_1+d_ifyP_1, xP_2)= (d_i(x+fxy)P_1, P_2)= (d_iC, P_2)= (C_i, P_2)$。

5.2　安全性

定理 1　在 TPM 没有泄露秘密数据 f 及其证书的情况下，ABP-DAA 方案是安全的。

证明（反证）：TPM 泄露其秘密数据 f 及其证书(A, B, C)的情况下，攻击者当然可以冒充该 TPM，这是不言而喻的。在 TPM 没有泄露秘密数据 f 及其证书的情况下，先假设攻击者可以不经过发布方颁布证书而自己提供 A_i、B_i、B_i^f、C_i 使得上述需要验证的两个双线性等式成立而通过认证，则 $B_i=yA_i$，$C_i=x(A_i+B_i^f)$必定成立，理由如下：

不妨令 $A_i=\alpha P_1$，$B_i=\beta P_1$，$B_i^f=\gamma P_1$，$C_i=\delta P_1$。

如果等式 $(A_i, Y)= (B_i, P_2)$成立，则 $(P_1, P_2)^{\alpha y}= (\alpha P_1, yP_2)(A_i, Y)= (B_i, P_2)= (\beta P_1, P_2)= (P_1, P_2)^{\beta}$，所以 $\alpha y=\beta$，故而 $B_i=\beta P_1=\alpha yP_1=y\alpha P_1=yA_i$，也即 $B_i=yA_i$ 必定成立。

如果等式 $(A_i, X)(B_i^f, X)= (C_i, P_2)$成立，则 $(P_1, P_2)^{(\alpha+\gamma)x}= (\alpha P_1+\gamma P_1, xP_2)= (\alpha P_1, xP_2)(\gamma P_1, xP_2)= (A_i, X)(B_i^f, X)= (C_i, P_2)= (\delta P_1, P_2)= (P_1, P_2)^{\delta}$，所以$(\alpha+\gamma)x=\delta$，故而 $C_i=\delta P_1=(\alpha+\gamma)xP_1=x(\alpha P_1+\gamma P_1)= x(A_i+B_i^f)$，也即 $C_i=x(A_i+B_i^f)$必定成立。

而如果 $B_i=yA_i$ 成立，则说明 Adversary 在已知 $A_i=\alpha P_1$，$B=yP_1$ 的情况下，可计算 $B_i=yA_i=y\alpha P_1= \alpha yP_1$，也即在已知 αP_1 与 yP_1 的情况下可计算 αyP_1，因而可以得出结论：非对称双线性对之群 G_{1+} 中的 CDH 问题是容易的。

而如果 $C_i=x(A_i+B_i^f)$成立，则说明 Adversary 在已知 $A_i+B_i^f=(\alpha+\gamma)P_1$，$X=xP_2$ 的情况下，可计算 $C_i=x(A_i+B_i^f)= x(\alpha+\gamma)P_1=(\alpha+\gamma)xP_1$，也即在已知 $(\alpha+\gamma)P_1$ 与 xP_2 的情况下可计算$(\alpha+\gamma)xP_1$，因而可以得出结论：非对称双线性对中的 *c*o-CDH 问题是容易的。

但事实上 CDH 问题与 *c*o-CDH 问题都是公认的困难问题，故而假设不成立，攻击者(Adversary)不可能不经过发布方颁布证书而自己提供 A_i、B_i、B_i^f、C_i 使得需要验证的 2 个双线性对等式成立而通过认证。

此外，攻击者 Adversary 可进行如下“中间人”攻击：Adversary 截获合法 TPM 发送给 Verifier 的 A_i、B_i、B_i^f、C_i 之后，任选 $r\in F_q$，计算 $A_i'=rA_i$，$B_i'=rB_i$，$B_i'^f=rB_i^f$，$C_i'=rC_i$，然后将 A_i'、B_i'、$B_i'^f$、C_i' 发送给 Verifier，而 Verifier 验证等式 $(A_i', Y)= (B_i', P_2)$与 $(A_i', X)(B_i'^f, X)= (C_i' P_2)$成立，这是因为 $(A_i', Y)= (A_i, Y)^r= (B_i, P_2)^r= (B_i', P_2)$，$(A_i', X)(B_i'^f, X)= (A_i, X)^r(B_i^f, X)^r=((A_i, X)(B_i^f, X))^r= (C_i, P_2)^r= (C_i', P_2)$。但是就这种攻击而言，Adversary 根本无法知道 AIK 的私钥 d_i，故其无法知道 rd_i，这也意味着对于攻击者作为假 AIK 的公钥的 A_i'而言，Adversary 不知道其对应的私钥 rd_i，也就无法给出后续的签名。因此，这种“中间人”攻击是无用的。

5.3　DAA 特性

ABP-DAA 方案具备 DAA 方案“直接”、“匿名”、“认证”的特性，而且其可以克服 CMS-DAA 方案可能存在的问题：

直接：TPM 从 Issuer 处获得的其内部秘密数据 f 的 DAA 证书(A, B, C)之后，不再需要 Issuer 的参与，就可每次直接向 Verifier 进行认证，可克服 Privacy CA 方案系统瓶颈的问题。

匿名：在向 Verifier 认证中 TPM 的身份匿名，这是因为每次认证中 TPM 提供给 Verifier 的 A_i、B_i、C_i 都可视为是对 DAA 证书的(A, B, C)的盲化，B_i^f 同样也是对于秘密数据 f 或 fB 的盲化。在 Verifier 与 Issuer 串通的情况下，即使假定非对称双线性对的群 G_{1+} 中的 DDH 问题是容易的，ABP-DAA 方案也能保证匿名，因为假如在证书申请时，TPM 向 Issuer 提供的是 fP_1，则 Issuer 还可通过验证等式 $(B_i, fP_1)= (B_i^f, P_1)$是否成立而判断出该 TPM 具体身份，但是在 ABP-DAA 方案中，TPM 向 Issuer 提供的是 kfP_1 而非 fP_1，而 kfP_1 实质上是用随机数 k 对 fP_1 的一种盲化，且 Issuer 在整个方案的自始至终都不能获知 fP_1，也无法判断出该 TPM 的具体身份。

认证：在没有泄露其秘密数据 f 及其证书的情况下，等式 $(A_i, Y)= (B_i, P_2)$与 $(A_i, X)\ (B_i^f, X)= (C_i, P_2)$成立，说明该TPM拥有Issuer颁布的DAA证书，便可通过认证。

5.4 性能

若用如下的符号来表示方案中的各种运算及相关参数。

G_+：双线性映射 $G_{1+}\times G_{2+}\to G_\times$ 中群 G_{1+} 或 G_{2+} 中的运算，诸如对于 $P\in G_{1+}$，计算 aP；

G_+^2：$G_{1+}\times G_{2+}\to G_\times$ 中群 G_{1+} 或 G_{2+} 中的运算，诸如对于 $P,Q\in G_{1+}$，计算 $aP+bQ$；

$G_\times$：双线性映射 $G_{1+}\times G_{2+}\to G_\times$ 中群 $G_\times$ 中的运算，诸如对于 $\lambda\in G_\times$，计算 λ^a；

$G_\times^2$：双线性映射 $G_{1+}\times G_{2+}\to G_\times$ 中群 $G_\times$ 中的运算，诸如对于 $\lambda,\omega\in G_\times$，计算 $\lambda^a\omega^b$；

P：双线性对运算，例如对于 $P_1\in G_{1+}, P_2\in G_{2+}$，计算 (P_1,P_2)；

H：散列运算，不区别具体是哪种散列运算；

n：黑名单列表中无赖或泄露证书的 TPM 总数目。

那么 CMS-DAA 方案[16]的主要计算开销（还存在取模数诸如 $a+b(\mathrm{mod}\,q)$ 等一些不便比较与统计的计算开销）与本文所给 ABP-DAA 方案的全部计算开销分别见表 1 与表 2 所示。

表 1 CMS-DAA 方案主要计算开销

阶段	参与方	主要计算开销
申请加入(Join)	TPM	$3G_+ + 2H$
	Issuer	$(2+n)G_+ + 2G_+^2$
	Host	$6P + H$
进行签名(Sign)	TPM	$G_+ + 2H$
	Host	$4G_+ + 3G_\times + P + H$
签名验证(Verify)	Verifier	$nG_+ + G_+^2 + G_\times^2 + 5P + 2H$

表 2 ABP-DAA 方案全部计算开销

阶段	参与方	全部计算开销
申请证书(Apply)	TPM	$3G_+$
	Issuer	$nG_+ + G_+^2$
	Host	0
进行认证(Attest)	TPM	$4G_+$
	Host	0
认证验证(Verify)	Verifier	$nG_+ + G_\times^2 + 5P$

由表 1 与表 2 可知，ABP-DAA 方案的计算开销要远小于 CMS-DAA 方案的计算开销，其整体性能要优于 CMS-DAA 方案；从方案协议流程的简洁程度来比较，其要比 CMS-DAA 方案简单得多；且 ABP-DAA 方案中没有使用零知识证明，其框架与已有几种 DAA 方案都不同。

5.5 对 TCM 的适用性

由于 BCC-DAA 方案采用的是基于 RSA 密码算法，其根本不适用于采用 ECC 密码算法的 TCM。而 BCL-DAA 与 CMS-DAA 方案也都主要针对 TPM 设计，方案要求 TPM 除了进行 G_+ 或 $G_\times$ 运算之外，还需进行各种散列运算，指数运算，取模数运算（诸如 $a+b(\mathrm{mod}\,q)$）等的运算，因此对于 TCM 也不适用；而本文所给 ABP-DAA 方案在计算上对于 TCM 基本没有特殊要求，除要求 TCM 内部存在一条可构造非对称双线性对的椭圆曲线外，其仅需要 TCM 进行几次 G_+ 运算，而 G_+ 运算 TCM 本身可以实现，因此 ABP-DAA 方案对于 TCM 具有良好的适用性。

如果在文献[4]规定的 TCM 所采用 SM2 类椭圆曲线中可以找到可构造非对称双线性对的椭圆曲线，那么 ABP-DAA 方案就可以直接应用于 TCM 的直接匿名认证。而如果 SM2 类椭圆曲线中找不到这样的椭圆曲线，则只需在 TCM 中引入一条可构造非对称双线性对普通椭圆曲线即可（有关椭圆曲线与双线性对的详细论述还可参考文献[18, 19]）。

值得说明的是，SM2 类椭圆曲线的定义为 E/F_q：$y^2=x^3+ax+b$，其中 q,a,b 长度均为 256bit，且 a、b 满足 $4a^3+27b^2\neq 0$。而文献[20]早就已经给出了 $E/F_q: y^2=x^3+ax+b$ 类椭圆曲线中可构造双线性对的具体椭圆曲线的例子，只是其参数 q,a,b 长度不满足 SM2 类椭圆曲线中 q,a,b 长度均为 256bit 的要求，因此 SM2 类椭圆曲线中极有可能存在可构造非对称双线性对的具体椭圆曲线，使得本文所提 ABP-DAA 方案直接适用于 TCM。故而 SM2 类椭圆曲线中是否真正存在以及如何找到满足需要的椭圆曲线将是一个非常值得进一步研究的问题。

6 结束语

本文基于非对称双线性对，提出了一种全新的 DAA 方案——ABP-DAA 方案。ABP-DAA 方案具有直接、匿名、认证的特性。其突破了已有的 DAA 方案使用零知识证明而使得方案整体计算开销较大的局限，整体具有简单高效且更加安全的特点。更为重要的是，其对于我国自主知识产权的 TCM

密码芯片实现直接匿名认证没有计算上的特殊要求，具有很好的适用性。

参考文献：

[1] 沈昌祥, 张焕国, 冯登国等. 信息安全综述 [J]. 中国科学 E 辑: 信息科学, 2007, 37(2): 129-150.
SHEN C X, ZHANG H G, FENG D F, *et al*. Summary of information safety[J]. Science in China (Series E) 2007. 37(2): 129-150.

[2] Trusted Computing Group. Trusted Computing Platform Alliance (TCPA) Main Specification Version 1.1b[S]. 2001.

[3] Trusted Computing Group. TCG TPM Specification Version 1.2 [S]. http://www.Trustedcomputinggroup.org. 2005.6.

[4] 国家密码管理局.可信计算密码支撑平台功能与接口规范[S]. 2007.
China Crypto Management office. Functionality and Interface Specification of Cryptographicsupport Platform for Trusted Computing[S]. 2007.

[5] 程相国. 基于双线性对的签名体制的研究[D]. 西安电子科技大学, 2006.
CHENG X G. Study on Digital Signatures from Bilinear Pairing [D]. Xidian University, 2006.

[6] LYNN B. On the Implementation of Pairing-based Cryptosystems[D]. The department of computer science and the committee on graduate studies of Stanford University, 2007.

[7] Menezes A J, OKAMOTO T, VANSTONE S A. Reducing elliptic curve logarithms to logarithms in a finite field [J]. IEEE Trans Inf Theory, 1993, 39(5): 1639-1646.

[8] BONEH D, BOYEN X, SHACHAM H. Short group signatures[A]. CRYPTO 2004[C]. California, USA, 2004. 41-55.

[9] LIBERT B. New Secure Applications of Bilinear Maps in Cryptography[D]. Universite Catholique de Louvain, 2006.

[10] SCOTT M, BENGER N, CHARLEMAGNE M, *et al*. Fast hashing to G2 on pairing-friendly curves[A]. Pairing-Based Cryptography-Pairing 2009: Third International Conference[C]. Palo Alto, CA, USA, 2009, 102-113.

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

[12] LEUNG A, MITCHELL C J. Ninja: non identity based, privacy preserving authentication for ubiquitous environments[A]. Proceedings of 9th International Conference on Ubiquitous Computing[C]. Innsbruck, Austria, 2007, 4717: 73-90.

[13] 陈小峰, 冯登国. 一种多信任域内的直接匿名证明方案[J]. 计算机学报, 2008, 31(7): 1122-1130.
CHEN X F, FENG D G. A direct anonymous attestation scheme in multi-domain environment[J]. Chinese Journal of Computers, 2008, 31(7): 1122-1130.

[14] BRICKELL E, CHEN L Q, LI J T. Simplified security notions of direct anonymous attestation and a concrete scheme from pairings[A]. The Conference on Trusted Computing (TRUST 2008)[C]. Villach, Austria, 2008.

[15] BRICKELL E, CHEN L Q, LI J T. A new direct anonymous attestation scheme from bilinear maps[A]. Trust 2008[C]. Berlin Heidlberg, 2008.166-178.

[16] CHEN L Q, MORRISSEY P, SMART N P. Pairing in trusted computing[A]. Pairing in Cryptography-Pairing 2008[C]. CA, USA, 2008.1-17.

[17] 汪涛, 杨义先. 基于 OT 的 DAA 方案[A]. 第十一届全国青年通信学术会议[C]. 中国绵阳, 2006.
WANG T, YANG Y X. OT based DAA protocol[A]. 1994-2008 China Academic Journal Electronic Publishing House[C]. Mianyang, China, 2006.

[18] FREEMAN D, SCOTT M, TESKE E. A taxonomy of pairing-friendly elliptic curves[EB/OL]. http://eprint.iacr. org/ 2006/372, 2006.

[19] SCOTT M, BENGER N, CHARLEMAGNE M, *et al*. On the final exponentiation for calculating pairings on ordinary elliptic curves[A]. Pairing-Based Cryptography-Pairing 2009 Third International Conference[C]. Palo Alto, CA, USA, 2009. 78-89.

[20] MIYAJI A, NAKABAY M, TAKANO S. New explicit conditions of elliptic curve traces for FR-reduction[J]. IEICE Transformations on fundamentals, 2001, E84-A(5): 1234-1242.

作者简介：

甄鸿鹄（1983-），男，甘肃渭源人，解放军信息工程大学工程师，主要研究方向为可信计算、网络信息安全。

陈越（1965-）男，河南开封人，博士，解放军信息工程大学教授、博士生导师，主要研究方向为网络信息安全、对等通信。

谭鹏许（1983-），男，河南许昌人，解放军信息工程大学博士生，主要研究方向为网络通信、网络信息安全。

郭渊博（1975-），男，陕西周至人，博士，解放军信息工程大学副教授、硕士生导师，主要研究方向为网络信息安全、分布式容忍入侵。