基于特定区间承诺值证明机制改进的DAA认证方案

莫家庆[1] 胡忠望[1] 林瑜华[2]
(肇庆学院计算机学院 肇庆 526061)[1] (肇庆学院教育技术与计算机中心 肇庆 526061)[2]

摘 要 针对目前可信计算平台直接匿名认证(DAA)机制的不足,提出一种改进的匿名认证方案。该方案先采用CA验证示证者的EK证书,协助示证者和DAA颁布者各自生成会话密钥,使DAA颁布者能够为示证者颁发秘密的DAA证书;然后示证者用两承诺值相等协议及CFT证明协议来证明承诺值位于某个特定区间的方法,向验证者证明其平台的真实合法性。分析表明,该方案具有较高的安全性,还具备不可欺骗性、匿名性、撤消性,效率更高。

关键词 直接匿名认证,可信计算,零知识证明,网络安全
中图法分类号 TP309 **文献标识码** A

Improved Scheme of DAA Authentication Based on Proof Mechanism of a Committed Number Lying in a Specific Interval

MO Jia-qing[1] HU Zhong-wang[1] LIN YU-hua[2]
(School of Computer, Zhaoqing University, Zhaoqing 526061, China)[1]
(Education Technology and Computer Center, Zhaoqing University, Zhaoqing 526061, China)[2]

Abstract An improved scheme was proposed against the shortage of current mechanism of direct anonymous attestation(DAA) in trusted computing platform. This scheme firstly adopted the CA to verify the EK certificate of prover to help prover and DAA issuer building the session key respectively. The DAA issuer can issue the secret certificate to the prover with the key. Then the prover used a committed number lying in a specific interval to attest the validity to the verifier by integrating the protocol that two committed numbers are equal with the protocol of the CFT proof. The analysis shows that this scheme not only has a higher security, but also is non-fraudulence, anonymity, can be withdrawed and more efficiency.

Keywords Direct anonymous attestation, Trusted computing, Zero-knowledge proof, Network security

1 引言

传统的防病毒技术、防火墙、入侵检测不能从根本上解决网络安全问题,而可信计算试图从根本上解决计算机和网络结构的不安全,提高终端的安全性和计算机自身的免疫力。目前,欧美地区的大计算机公司以及相关机构在国际可信计算组织(TCG)的协调下,正在不断地推动可信平台模块(Trusted Platform Module, TPM)相关标准的发展。

TPM的一个基本问题是可信平台认证。可信平台认证是指TPM用户向验证者证明自己拥有一个真实合法的TPM,而又不暴露自己是具体哪一个TPM,也就是TPM在不暴露自己身份的情况下向验证者证明自己身份的合法性,这就产生了匿名认证的思想。目前可信计算组织提出两种身份认证协议:一是TPM v1.1的可信第三方协议(Privacy Certificate Authorities, PCA)[1],二是TPM v1.2中的直接匿名认证(Direct Anonymous Attestation, DAA)[2]。在PCA方案中,TPM生成一对AIK密钥的RSA公私钥对,以代替EK身份密钥签署完整性度量值,然后TPM将AIK公钥发送给PCA,由PCA验证EK密钥并生成AIK证书,用于证明TPM拥有真实的EK。因此PCA方案可使验证平台在通信过程中隐藏身份信息。然而该方案的缺陷在于通信过程都需要依赖PCA,使PCA成为瓶颈。另外,PCA可能与验证者相勾结,使得验证者仍然能识别TPM来自哪个平台。DAA方案由Brickell等人提出[2],使用DAA证书代替原有的AIK证书,DAA证书一次生成就可多次使用,在保证TPM所在平台的匿名性的同时,尽量减少了对可信第三方的依赖。DAA方案克服了PCA方案的瓶颈问题,但方案复杂,计算量大,这对自身资源和计算能力都有限的TPM芯片造成极大负担。另外,其还存在DAA Issuer与验证者合谋共同欺骗示证者的安全隐患[3]。

为解决TPM v1.2所存在的问题,已有学者对该方案进行改进研究[3,4]。文献[5]运用决策Diffie-Hellman和q-SDH假设对DAA方案进行改进,缩短私钥和签名长度,提高了方案的安全性。文献[6]提出基于椭圆曲线和双线性映射的

到稿日期:2011-09-10 返修日期:2011-11-22 本文受广东省高等学校人才引进专项资金项目(粤财教[2010]343号),肇庆市科技创新计划项目(2011G212)资助。

莫家庆(1973-),男,硕士,副教授,CCF会员,主要研究方向为信息安全、数据库,E-mail:mojiaqing@126.com;胡忠望(1965-),男,硕士,教授,主要研究方向为计算机网络与安全、信息技术教育;林瑜华(1972-),实验师,主要研究方向为计算机安全。

BCL-DAA 方案，减少了 TPM 运算的时间复杂度，提高了安全性。文献[7]运用新型的 XTR 公钥体制对 DAA 方案进行改进，提高了方案的安全性和认证效率。总体而言，这些解决方案都是基于公认的数学难题来求解的，相对而言，其运算量比较大，认证效率还有提升的空间。

文献[8]对于证明承诺值 x 在特定区间$[a,b]$的问题，提出了一种运用统计零知识证明并结合两承诺值相等协议以及 CFT 证明协议的新方法，该方法具有计算量少、通信量小、安全性强的特点。本文将该方法引入到可信计算的匿名认证中，同时引入可信第三方 CA，提出一种改进的匿名认证方案。由于新方案的 join 协议引入可信第三方 CA 以协助在 DAA Issuer 和示证者之间实现密钥交换，使 DAA Issuer 能安全地向示证者发送 DAA 证书。另外，在 sign 协议中运用上述证明承诺值 x 在特定区间$[a,b]$的新方法，使得新方案的安全性和认证效率都有较大提高。

2 DAA 认证协议

TCG 的 DAA 认证协议结合了群签名、身份托管和证书系统技术。DAA 认证协议中的 TPM 在 PrivCA 的帮助下，向远程服务器证实它的真实性。该方案涉及 DAA 颁发者(DAA Issuer)、验证者(Verifier)、TPM、HOST(TPM 所在平台) 4 个实体，以及 join 和 sign 两个协议。其中 join 协议表示 TPM 创建 DAA 私钥 privDK，使用 EK 向 DAA 颁发者签发自己，如果 DAA 颁发者验证成功，DAA 颁发者将向 TPM 及其所在平台签发 DAA 证书 certDK。sign 协议表示示证者产生一个 RSA 密钥对 AIK，使用 privDK 和 certDK 对该 AIK 的公钥签名，发送给验证者，验证者使用 IKEY 检验该签名是否合法，如果检验通过，验证者则可以确定 TPM 平台是真实可信的，就可以向 TPM 及其所在平台提供服务。图 1 为 DAA 认证协议的简单描述。

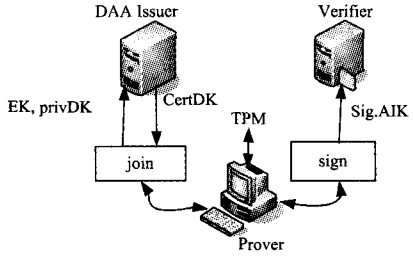

图 1 DAA 认证协议的简单描述

文献[9]指出，DAA Issuer 由长期公钥 PK_I 计算出本次使用的 PK_I'，通过验证 EK 公钥是否正确来决定是否为 Prover 发布使用 PK_I' 生成的 DAA 证书，因此 DAA Issuer 可以建立 PK_I' 和 EK 的映射表。如果 Verifier 与 DAA Issuer 合谋，则 Verifier 获取 prover 的 PK_I' 提供给 DAA Issuer，DAA Issuer 查询映射表就可以了解相应的 EK。因此，DAA 方案虽然解决了 PCA 方案的缺陷，但在隐私保护上仍然比较薄弱，存在安全隐患。

3 假设与定义

在以下定义中，n 为安全的强 RSA 模数，h 是以 g 为生成元的循环群中的元素，g 和 h 为大于 160 比特的素数；l,t,s 为安全参数；$a \| b$ 表示两个二进制数的级联；$H()$ 表示输出 $2t$ 比特的无碰撞哈希函数，$|n|$表示 n 的二进制长度，$x \in_R [a,b]$ 表示 x 是$[a,b]$中的随机整数。

假设 1(强 RSA 假设) 存在一个有效算法，输入 $|n|$ 时，输出 RSA 模数 n 和一个元素 $z \in Z_n^*$，使得不能找到 $e \notin \{-1, 1\}$ 和 u 满足 $z = u^e \bmod n$。

定义 1(FO 承诺) Alice 和 Bob 都不知如何分解 n，在循环群中计算离散对数是不可行的。Alice 不知 $\log_g h$ 和 $\log_h g$。Alice 在$\{-2^s n+1, 2^s n-1\}$中选取 r，计算 $E(x,r) = g^x h^r \bmod n$，并把 $E(x,r)$作为对 x 的承诺发送给 Bob。因为 Alice 不能分解 n，且不知 $\log_g h$ 和 $\log_h g$，所以她不能找到 $x_1 \neq x_2$ 使得 $E(x_1,r_1) = E(x_2,r_2)$。称这个承诺方案为 FO 承诺[10]。这说明这个承诺方案是统计安全的，具体分析过程见文献[10]。

定义 2(协议 $PK(x,r;E = g^x h^r \wedge x \in [-2^{t+l}b, 2^{t+l}b])$) Alice 运用 FO 承诺随机选择 $x \in [0,b]$以及 $r \in [-2^s n+1, 2^s n-1]$，通过使用零知识协议证明 $x \in [-2^{t+l}b, 2^{t+l}b]$。(1) Alice 随机选取 $\omega \in_R [0, 2^{t+l}b]$和 $\eta \in_R [-2^{l+t+s}n+1, 2^{l+t+s}n-1]$；(2)Alice 计算 $W = g^{\omega} h^{\eta} \bmod n$，$C = H(W)$，$c = C \bmod 2^t$；(3) $D_1 = \omega + cx$，$D_2 = \eta + cr$，如果 $D_1 \in [cb, 2^{l+t}b-1]$，则 Alice 把(c, D_1, D_2)发送给 Bob，否则 Alice 重复上述过程。(4)Bob 检验 $D_1 \in [cb, 2^{l+t}b-1]$和 $C = H(g^{D_1} h^{D_2} E^{-c})$，如果检验通过，则 Bob 确信 $x \in [-2^{t+l}b, 2^{t+l}b]$。该协议在随机预言下是安全的，且 Bob 不能获得 x 的相关信息[11]。

定义 3(协议 $PK\{x, r_1, r_2; E = E_1(x, r_1) \wedge F = E_2(x, r_2)\}$) 其中 $r_1 \in [-2^{s_1} n+1, 2^{s_1} n-1]$，$r_2 \in [-2^{s_2} n+1, 2^{s_2} n-1]$，$s_1$、$s_2$ 是安全参数，Alice 向 Bob 证明 E 和 F 都是对 x 的承诺。(1) Alice 随机选取 $\omega \in_R [1, 2^{t+l}b-1]$，$\eta_1 \in [1, 2^{l+t+s_1}b-1]$，$\eta_2 \in [1, 2^{l+t+s_2}b-1]$，然后计算 $W_1 = g_1^{\omega} h_1^{\eta_1} \bmod n$，$W_2 = g_2^{\omega} h_2^{\eta_2} \bmod n$，$c = H(W_1 \| W_2)$，$D = cx + \omega$，$D_1 = cr_1 + \eta_1$，$D_2 = cr_2 + \eta_2$，发送$(c, D, D_1, D_2)$给 Bob。(2)Bob 验证 $c = H(g_1^D h_1^{D_1} E^{-c} \bmod n \| g_2^D h_2^{D_2} F^{-c} \bmod n)$。该协议在随机预言下是安全的，具体分析过程见文献[10]。

4 改进的 DAA 认证方案

结合前面的分析，从 join 协议和 sign 协议两方面入手，对 TCG 的 DAA 认证协议进行改进：(1)在 join 协议方面，加入可信第三方 CA，用于检验示证者的 EK 证书是否有效，并协助在 DAA Issuer 和 TPM 之间生成会话密钥，使两者之间能进行安全、有效的通信。通过这种方式，TPM 平台避免向 DAA Issuer 暴露自己的 EK 公钥，解决 DAA Issuer 与 Verifier的共谋问题。(2)在 sign 协议方面，在示证者和验证者之间运用随机预言模式下的统计零知识证明，以证明承诺值在特定区间，且(x,r)是一个有效的密钥对。

改进的 DAA 方案如图 2 所示，图中涉及有 4 个实体：DAA Issuer(DI)，CA，Prover(即 Alice，用 A 表示)，Verifier(即 Bob)。

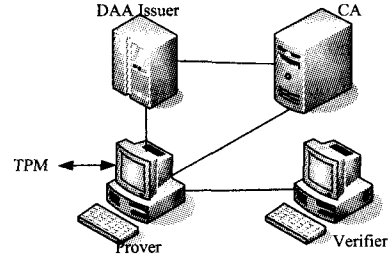

图 2 改进后的 DAA 认证架构

4.1 参数设置及 AAK 生成

管理员生成系统参数(n,g,h,l,t,s)，其中 n 为安全的 RSA 模数，g 和 h 为大于 160bit 的素数；l,t,s 为安全参数。

本方案中，在 TPM 生产制造的同时生成匿名认证密钥 AAK[12]。管理员将系统参数传给 TPM 的安全单元(Secure Unit，SU)，用于生成 AAK 和匿名认证所需的信息。在此过程中，外界无法获取 SU 内部信息且无法干涉其运算过程。

SU 随机选取 $r\in\{-2^s n+1,\cdots,2^s n-1\}$，再随机选定在区间$[a,b]$的一个承诺值 x，把(x,r)发送给 TPM，TPM 将(x,r)作为 AAK 加以保存。

4.2 join 协议

join 协议的形式化定义如图 3 所示。在该协议中，示证者 Alice 和 DAA Issuer 在 CA 的协助下，各自生成会话密钥。

1.1 A:Create a non-predictable 160bit $Nonce_A$

1.2 A→DI:$Msg_{A,1}=(TS_{A,1},S_{A\to DI,1},Nonce_A)$

2.1 DI:Create a non-predictable 160bit $Nonce_{DI}$

2.2 DI→A:$Msg_{DI,1}=(TS_{DI,1},S_{DI\to A,1},Nonce_{DI},Msg_{A,1})$

3.1 A:Create Mssage:$Msg_{tmp1}=(TS_{A,2},S_{A\to CA,1},Msg_{DI,,1},E_{KP}$(CertEK))

3.2 A→CA:$Msg_{A,2}=(Msg_{tmp1},M_{KP}(Msg_{tmp1}))$

4.1 CA:Validate $Msg_{A,2}$

4.2 CA:Create a non-predictable 160bit $Nonce_{CA}$

4.3 CA:Create Mssage:$Msg_{tmp2}=(TS_{CA,2},S_{CA\to DA,1},E_{KI}(Nonce_{CA}))$

4.4 CA→DI,$Msg_{CA,1}=(Msg_{tmp2},M_{KI}(Msg_{tmp2}))$

5.1 DI:Validate $Msg_{CA,1}$

5.2 DI:$KEY_{DI\text{-}A}$=CreateSKey($Nonce_A,Nonce_{DI},Nonce_{CA}$)

5.3 DI:Create Mssage:$Msg_{tmp3}=(TS_{DI,2},S_{DI\to CA,1},Nonce_A,Nonce_{DI})$

5.4 DI→CA:$Msg_{DI,2}=(Msg_{tmp3},M_{KI}(Msg_{tmp3}))$

6.1 CA:Validate $Msg_{DI,2}$

6.2 CA:Create Mssage:$Msg_{tmp4}=(TS_{CA,3},S_{CA\to A,1},E_{KP}(Nonce_{CA}))$

6.3 CA→A,$Msg_{CA,2}=(Msg_{tmp4},M_{KP}(Msg_{tmp4}))$

7.1 A:Validate $Msg_{CA,2}$

7.2 A:KEY $_{DI-A}$=CreateSKey($Nonce_A,Nonce_{DI},Nonce_{CA}$)

图 3 join 协议的形式化定义

第 1.1 步 Alice 生成不可预知的 160bit 随机数 $Nonce_A$。

第 1.2 步 Alice 把消息 $Msg_{A,1}$ 发送给 DAA Issuer。其中 $Msg_{A,1}$ 表示 Alice 所发送的第一个消息，$TS_{A,1}$ 表示发送第一条消息时的时间戳，$S_{A\to DI,1}$ 表示消息由 Alice 发送至 DAA Is-suer的第一个会话 ID，后面的符号含义类似。生成的随机数和时间戳用于防止重放攻击。

第 2.1、2.2 步 DAA Issuer 生成不可预知的 160bit 随机数 $Nonce_{DI}$，然后向 Alice 发送消息 $Msg_{DI,1}$。

第 3.1、3.2 步 Alice 生成消息 Msg_{tmp1}，该消息包含 $Msg_{DI,1}$，使用 KP 加密后的 Alice 所在 TPM 平台的 EK 证书为 CertEK。Alice 把 $Msg_{A,2}$ 发给 CA，$Msg_{A,2}$ 包含 Msg_{tmp1} 以及 Msg_{tmp1} 对应的消息认证码。KP 是 Alice 与 CA 之间的通信密钥，$M_{KP}(\cdot)$表示运用 KP 加密得到的消息认证码。

第 4.1、4.2 步 CA 检验 $Msg_{A,2}$，如果通过，则生成不可预知的 160bit 随机数 $Nonce_{CA}$。

第 4.3、4.4 步 CA 使用 KI 对 $Nonce_{CA}$ 进行加密，并将其加入到消息 Msg_{tmp2} 中。然后生成消息 $Msg_{CA,1}$，并发给 DAA Issuer。KI 是 CA 与 DAA Issuer 之间的通信密钥。$Msg_{CA,1}$ 由 Msg_{tmp2} 和 Msg_{tmp2} 的消息认证码组成。

第 5.1、5.2 步 DAA Issuer 检验 $Msg_{CA,1}$，如果通过，则以 $Nonce_A$、$Nonce_{DI}$ 和 $Nonce_{CA}$ 为参数，生成与 Alice 之间的通信密钥 $KEY_{DI\text{-}A}$。$CreateSKey()$函数用于生成通信密钥。

第 5.3、5.4 步 DAA Issuer 创建消息 Msg_{tmp3}，该消息包含 $Nonce_A$ 和 $Nonce_{DI}$。然后生成消息 $Msg_{DI,2}$，并将其发送给 CA。消息 $Msg_{CA,1}$ 由 Msg_{tmp3} 和 Msg_{tmp3} 的消息认证码组成。

第 6.1、6.2、6.3 步 CA 检验消息 $Msg_{DI,2}$，如果通过，则使用 KP 对 $Nonce_{CA}$ 进行加密，并加入到消息 Msg_{tmp4} 中，再把由 Msg_{tmp4} 和其对应消息认证码构成的消息 $Msg_{CA,2}$ 发送给 Alice。

第 7.1、7.2 步 Alice 检验消息 $Msg_{CA,2}$，如果通过，则 Alice 以 $Nonce_A$、$Nonce_{DI}$ 和 $Nonce_{CA}$ 为参数，计算与 DAA Is-suer 之间的通信密钥 $KEY_{DI\text{-}A}$。

Alice 和 DAA Issuer 在 CA 协助下生成共享对称密钥 $KEY_{DI\text{-}A}$，此后双方运用 $KEY_{DI\text{-}A}$ 进行直接通信，Alice 安全地从 DAA Issuer 处取得秘密的 DAA 证书。

4.3 sign 协议

第 1 步 Alice 向 Bob 承诺 $E(x,r)=g^x h^r \bmod n$，并与 Bob 执行 $PK\{x,r:E(x,r)=g^x h^r \bmod n\}$，令 $y_1=x-a,y_2=b-x$，Alice 计算 $E_1=g^{y1}h^r \bmod n,E_2=g^{y2}h^r \bmod n$。

第 2 步 Alice 选取随机 α,ω,T，使 $u=\alpha^2 y_1 y_2+\omega>2^{t+l+s+T}$，其中 $\alpha\neq 0;\omega\in(0,2^{s+T});1\leqslant|a|,|b|,|a-b|\leqslant T$。同时选取 $r_1,r_2,r_3,r_4\in[-2^s n+1,2^s n-1]$，并满足以下条件：

$$(ry_2+r_1)\alpha^2+r_2\alpha+r_3\in[-2^s n+1,\cdots,2^s n-1]$$

计算 $E_3=E_1^{y2}h^{r1} \bmod n,E_4=E_3^{y}h^{r2} \bmod n,E_5=E_4^{y}h^{r3} \bmod n,F=g^{\omega}h^{r4} \bmod n,u=g^{\omega}h^{-(ry_2\alpha^2+r_1\alpha^2+r_2\alpha+r_3)} \bmod n$，将$(u,E_3,E_4,E_5,F)$发送给 Bob。

第 3 步 Bob 计算 $E_1=E(x,r)/g^a,E_2=g^b/E(x,r),U=g^a/E_5$。

第 4 步 Alice 与 Bob 执行：

$$PK\{y_2,-r,r_1:E_2=g^{y_2}h^{-r} \bmod n\wedge E_3=E_1^{y_2}h^{r_1} \bmod n\} \quad (1)$$

$$PK\{\alpha,r_2,r_3:E_4=E_3^{\alpha}h^{r_2} \bmod n\wedge E_5=E_4^{\alpha}h^{r_3} \bmod n\} \quad (2)$$

$$PK\{\omega,r_4,-(ry_2+r_1\alpha^2+r_2\alpha+r_3):F=g^{\omega}h^{r_4} \bmod n\wedge U=g^{\omega}h^{-(ry_2+r_1\alpha^2+r_2\alpha+r_3)} \bmod n\} \quad (3)$$

$$PK\{\omega,r_4:F=g^{\omega}h^{r_4} \bmod n\wedge -2^{t+l+s+T}\leqslant\omega\leqslant 2^{t+l+s+T}\} \quad (4)$$

第 5 步 Bob 核实式(1)－式(4)的正确性，并验证 $u>2^{t+l+s+T}$，如果成立，则 Bob 确信 $x\in[a,b]$，认为 Alice 的可信平台是真实合法的。

5 安全性及效率分析

本方案引入可信第三方 CA，作用是在 join 阶段中验证 Prover 可信平台 EK 证书的合法性、DAA Issuer 和 Veri-fier 身份的合法性，以及协助 Prover 和 DAA Issuer 双方生成通信密钥，避免了 DAA Issuer 和 Verifier 共谋去欺骗 Prover 的安全隐患。零知识性保证不会泄露 x 的任何信息。sign 协议的各步骤运用了具备零知识性的 PK 协议，因而其具备很高的安全性。另外，sign 协议引入时间戳和会话 ID，防止协商过程中的重放攻击，进一步提高了本方案的安全性。

本方案还满足不可欺骗性、匿名性、撤消性。

1)不可欺骗性：如果 Alice 向 Bob 承诺的 $E(x,r)=g^x h^r$

mod n 中 $x \notin [a,b]$，Alice 可以通过如下方法来欺骗 Bob：一是找到一个 x'，r' 且 $x' \in [a,b]$ 使得 $g^{x'}h^{r'} \bmod n = g^x h^r \bmod n$，再用 x' 代替 x 执行零知识证明式(1)－式(4)，这需要解离散对数，在计算上是不可能的；二是找到一个 $x' \in [a,b]$ 且 $g^x \bmod n = g^{x'} \bmod n$，由于 Alice 不知道 n 的分解，因此这也是不可能的，否则与强 RSA 假设矛盾。在上两项都不可能被攻破的情况下，Alice 要欺骗成功，则需要攻击式(1)－式(4)。因为攻破每一个公式的成功概率均小于 2^{-t+1}[10]，所以 Alice 成功欺骗的概率小于 $4 \times 2^{-t+1} = 2^{-t+3}$。例如，当安全参数 t 取值 80 时，Alice 成功欺骗的概率小于 2^{-77}。

2)匿名性：sign 协议的式(1)－式(4)都是统计零知识证明，具有无限计算能力的攻击者也不能求解出相应的离散对数。Bob 从 Alice 获得的公开数据有 $E(x,r)$、E_1、E_2、U、E_3、E_4、E_5、F、u，其中包含 x、y_1、y_2、α、ω、r、r_1、r_2、r_3、r_4，未知数共 10 个，而方程却有 9 个，攻击者可以猜测出一个未知数，再决定其他随机数，它们都是合法解。因而 Bob 不能从此过程中获取 TPM 的相关信息，这保障了匿名性。

3)撤消性：在本方案中，如果 Prover 所在 TPM 泄露了匿名认证密钥(x,r)，则(x,r)将被加入至撤消列表中。当 Verifier接到请求时，检查是否存在(x',r')，使得 $E(x',r') \stackrel{?}{=} E(x,r)$，如果相等，则可以判断事务请求来自一个被撤消的无效 TPM，Verifier 拒绝为其提供服务。

在本方案中，Prover 共执行 1 次签名，生成和验证消息认证码各 1 次，生成密钥 1 次；CA 执行 1 次签名验证，生成和验证消息认证码各 2 次；DAA Issuer 共执行 1 次签名，1 次签名验证，生成和验证消息认证码各 1 次，生成密钥 1 次；共需要执行 24 个复合模指数运算及 8 个 hash 运算。而在原 DAA 方案中，Issuer 生成密钥 1 次，Prover 签名 3 次，共执行 43 次复合模指数及 20 个 hash 运算。可以看到，本方案的 join 协议比 DAA 方案的复杂不少，但是本方案的 join 协议解决了 Issuer 与 Verifier 的共谋问题，而且 Prover 获得 DAA 证书后，CA 不再参与 sign 过程，因此 CA 不会成为性能瓶颈；而本方案的复合模指数运算和 hash 运算数量比原 DAA 方案少得多，因而总体运算效率有较大提高。

对于选择的参数，假设 $|n| = 1024$bit，$|b-a| = 512$bit，$T = 512$，$l = 40$，$t = 80$，$s = 40$，$s_1 = 40$，$s_2 = 552$。根据文献[10]，sign 协议仅需要发送 13222bit 数据。因此，本方案的 sign 协议通信量也是比较少的。

结束语 直接匿名认证是可信计算平台的重要功能。面对复杂的网络环境和不断涌现的各种攻击手段，设计具有高安全性和高效率的直接匿名认证方案具有重要意义。本文通过引入可信第三方以及使用特定区间承诺值证明机制，使改进的 DAA 认证方案具有较高的安全性和效率，解决了已有协议的安全隐患。

参 考 文 献

[1] Trusted Computing Group. Trusted Computing Platform Alliance(TCPA) Main Specification Version 1. 1b[EB/OL]. http://www.trustedcomputinggroup.org,2011-08-20

[2] Brickell E, Camenisch J, Chen L. Direct anonymous attestation [EB/OL]. http://eprint.iacr.org/2004/205.pdf,2011-08-20

[3] Brickell E, Chen L, Li J. A new direct anonymous attestation scheme from bilinear maps[C]//Proceedings of the 1st International Conference on Trusted Computing and Tpust in Information Technologies. Berlin: Springer-Verlag, 2008: 166-178

[4] He Ge, Tate S R. A direct anonymous attestation scheme for embedded devices[C]//Proc of the 10th International Conference on Practice and Theory in Public-key. Springer-Verlag, 2007: 16-30

[5] 陈小峰，冯登国. 一种基于双线性映射的直接匿名证明方案[J]. 软件学报，2010，21(8)：2070-2078

[6] Brickell E, Chen Li-qun, Li Jiang-tao. Simplified security notions of direct anonymous attestation and a concrete scheme from pairings[C]//The Conference on Trusted Computing(TRUST 2008). Villach, Austria, 2008: 315-330

[7] 杨亚涛，曹陆林，李子臣，等. 基于 XTR 机制改进的直接匿名认证方案[J]. 计算机科学，2011，38(4)：141-144

[8] 张京良，马育珍，王育民. 承诺值在特定区间的高效证明[J]. 西安电子科技大学学报：自然科学版，2006，33(6)：949-952

[9] Rudolph C. Covert identity information in direct anonymous attestation[C]//Proceedings of the 22nd IFIP TC-11 International Information Security Conference(SEC2007) on New Approaches for Security, Privacy and Trust in Complex Environments. Springer, Boston, 2007: 443-448

[10] Fujisaki E, Okamoto T. Statistical zero knowledge protocols to prove modular polynomial relations[C]//Proceedings of CRYPTO' 97. Berlin: Springer-Verlag, 1997: 16-30

[11] Boudot F. Efficient Proofs That a Committed Number Lies in an Interval[C]//EUROCRYPT 2000, LNCS l 807. Berlin Heidelberg: Springer-Verlag, 2000: 431-444

[12] Ge He. An Anonymous Authentication Scheme for Trusted Computing Platform[EB/OL]. http://eprint.iacr.org/2005/445.pdf,2011-08-20

(上接第 91 页)

[11] Jaggi S, Langberg M, Katti S, et al. Resilient Network Coding in the Presence of Byzantine Adversaries [J]. IEEE Transactions on Information Theory, 2008, 54(6): 2596-2603

[12] 周亚军，李晖，马建峰. 一种安全的纠错网络编码[J]. 电子与信息学报，2009，31(9)：2237-2241

[13] Bhattad K, Narayanan K R. "Weakly Secure Network Coding" [EB/OL]. http://netcod.org/papers /06Bhattad N-final.pdf, 2007-05-22

[14] 周亚军，李晖，马建峰. 一种防窃听的随机网络编码[J]. 西安电子科技大学学报，2009，36(4)：696-701

[15] 申肖肖，李晖. P2P 网络编码技术研究[D]. 西安：西安电子科技大学，2010

[16] 徐光宪，付晓. 基于稀疏矩阵的低复杂度安全网络编码算法[J]. 计算机工程，38(9)：55-57

[17] 周亚军，李晖，马建峰. 防污染和防窃听的网络编码[D]. 西安：西安电子科技大学，2009

[18] 张岩. 一种改进的安全网络编码方案的研究[J]. 南京邮电大学学报，2009：962-966

[19] 马松雅，罗明星，杨义先. 抗 Byzantine 攻击的安全网络编码研究综述 [C]//中国电子学会第十五届信息论学术年会暨第一届全国网络编码学术年会论文集(下册). 2008

[20] 董学文，牛文生，马建峰，等. Ad-hoc 路由协议的串空间安全性扩展[J]. 计算机科学，2011，38(7)：51-54