ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.21, No.8, August 2010, pp.2070−2078
doi: 10.3724/SP.J.1001.2010.03579

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

一种基于双线性映射的直接匿名证明方案*

陈小峰[1,2+], 冯登国[1,2]

[1](中国科学院 研究生院 信息安全国家重点实验室,北京 100049)

[2](中国科学院 软件研究所 信息安全国家重点实验室,北京 100190)

Direct Anonymous Attestation Based on Bilinear Maps

CHEN Xiao-Feng[1,2+], FENG Deng-Guo[1,2]

[1](State Key Laboratory of Information Security, The Chinese Academy of Sciences, Beijing 100049, China)

[2](State Key Laboratory of Information Security, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

+ Corresponding author: E-mail: loiscxf@hotmail.com

Chen XF, Feng DG. Direct anonymous attestation based on bilinear maps. *Journal of Software*, 2010,21(8): 2070−2078. http://www.jos.org.cn/1000-9825/3579.htm

Abstract: This paper proposes a Direct Anonymous Attestation (DAA) scheme from the bilinear maps based on the decisional Diffie-Hellman (DDH) assumption and *q*-SDH assumption. Compared to other schemes, the scheme's signature length is much shorter. Meanwhile, the scheme reduces the computational cost of the Trusted Platform Module (TPM) in the signing process. It gives a practical solution to ECC-based TPM in protecting the privacy of the TPM. This paper gives a detailed security proof of the proposed scheme in ideal-system/real-system security model which shows that the scheme meets the security requirements of unforgeability, variable anonymity and unlinkability.

Key words: direct anonymous attestation; bilinear map; trusted platform module; trusted computing platform

摘 要: 基于 DDH(decision Diffie-Hellman)假设和 *q*-SDH 假设,给出了一种基于双线性映射的直接匿名证明(direct anonymous attestation,简称 DAA)方案.与其他方案相比,该方案极大地缩短了签名长度,降低了签名过程中可信平台模块(trusted platform module,简称 TPM)的计算量.同时,为基于椭圆曲线的 TPM 提供了可行的隐私性保护解决方案.利用理想系统/现实系统模型对该方案的安全性进行分析和证明,分析表明,该方案满足不可伪造性、可变匿名性和不可关联性.

关键词: 直接匿名证明;双线性映射;可信平台模块;可信计算平台

中图法分类号: TP309 **文献标识码**: A

在可信计算组织(Trusted Computing Group,简称 TCG)给出的可信计算平台实现方案中,可信平台模块(trusted platform module,简称 TPM)是可信计算平台的核心和基础.TPM 是嵌入在主机中的一个防篡改的安全

* Supported by the National Natural Science Foundation of China under Grant Nos.60673083, 60603017 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant Nos.2007AA01Z412, 2006AA01Z454 (国家高技术研究发展计划(863)); the National Key Technology R&D Program of China under Grant No.2006BAH02A02 (国家科技支撑计划)

Received 2007-12-17; Revised 2008-09-03; Accepted 2008-12-29

芯片,该安全芯片唯一标识了可信计算平台的身份.TPM 出厂时都会绑定一个根密钥(EK 密钥),不同的 TPM 拥有不同的根密钥.如果所有的远程认证都基于该根密钥,可信计算平台的隐私性则无法得到保障.因此,在可信计算平台与远程通信方交互时,需要提供一种远程匿名认证机制来保护可信计算平台的隐私性,在不暴露可信计算平台身份的同时进行远程认证.其中,在 TPM 规范中提出了两种方案来解决可信计算平台的隐私性保护问题.TPM v1.1 规范提出的方案基于一个称为隐私 CA(privacy-CA)的可信第三方.其实现方案如下:TPM 首先产生一对称为 AIK 的非对称公私钥对.然后,TPM 将 AIK 公钥发送给 Privacy-CA,请求产生 AIK 的公钥证书;同时,TPM 向 Privacy-CA 证明其拥有一个真实的 EK 根密钥(身份密钥). Privacy-CA 给 AIK 签发证书.在验证阶段,TPM 将 AIK 证书发送给验证者.通过这种方式,可信计算平台可以在通信过程中隐藏自己的真实身份.该方案的最大缺点就是每次通信过程都需要经过 Privacy-CA,因此 Privacy- CA 成为系统的瓶颈.同时,攻击方如果攻陷了 Privacy-CA,可信计算平台的隐私性就无从谈起.

为了弥补以上的不足,TPM v1.2 规范采纳了 Brickell 等人首次提出的直接匿名证明(direct anonymous attestation,简称 DAA)方案[1].在这个方案中,TPM 无需 Privacy-CA 的帮助就可以直接向远程验证者证明可信计算平台的真实性.在下文的讨论中,将 Brickell 等人提出的 DAA 方案称为 BCC 方案.直接匿名证明方案是在群签名方案[2,3]的基础上发展起来的,与群签名方案不同的是:在直接匿名证明方案中,管理员不能对成员进行匿名性的撤销,成员签名对管理员也是匿名的;在直接匿名证明方案中必须提供一种假冒 TPM 的检测机制,防止假冒 TPM 的欺骗.

目前,直接匿名证明的研究方向主要集中在以下 3 个方面:

(1) 对现有的 BCC 方案的安全性和隐私性的改进.Camenisch 提出了安全性改进方案[4],Brickell 对 BCC 方案进行了有效的扩展,使得它能够支持更加灵活的撤销机制[5].Smyth,Chen 和 Ryan 讨论了如何在攻陷管理员的情况下保证 BCC 方案的隐私性[6].Backes 等人对 BCC 方案进行了形式化的自动分析[7].

(2) 直接匿名证明方案在系统认证方面的应用.Camenische 提出了一种方案,将 DAA 方案应用于保护匿名证书[8].Leung 和 Mitchell 利用 DAA 方案在移动普适环境中构建了一个不是基于身份的认证方案[9].

(3) 在不同的计算环境中实现 DAA.由于现有的 DAA 方案过于复杂,在移动平台上很难实现,因此,研究人员展开了对移动平台上 DAA 方案的研究.2007 年,Ge 等人提出了更适合于嵌入式设备的直接匿名证明方案(简称 HS 方案)[10].在签名效率上,HS 方案比 BCC 方案有了较大的提高.

本文的研究成果主要体现在不同的计算环境中实现 DAA 方案,由于目前基于 ECC(elliptic curve cryptography)的 TPM 缺少一种隐私性保护方案,因此迫切需要展开对基于 ECC 的 TPM 的隐私性保护方案研究.本文在短群签名方案[11,12]的基础上,提出了一种基于双线性映射的直接匿名证明方案(简称 BM-DAA 方案),本文的方案与 BCC 方案、HS 方案相比,签名长度(为 2 044 比特)更短,并且在签名过程中计算效率更高.

1 预备知识

双线性群.设 G_1,G_2 和 G_T 是阶为素数 q 的循环群.g_1 是群 G_1 的生成元,g_2 是群 G_2 的生成元;ψ 是 G_2 到 G_1 的可计算的同构,$\psi(g_2)=g_1$;e 是双线性对映射:$e:G_1\times G_2\to G_T$,满足如下的性质,则称群(G_1,G_2)是一对双线性群:

(1) 映射 e 是双线性的:给定元素 $u\in G_1,v\in G_2,e(u^a,v^b)=e(u,v)^{ab}$.

(2) 映射 e 是非退化的:$e(g_1,g_2)\neq 1$.

(3) 映射 e 对任何可能的输入对都能有效地进行计算,

***q*-SDH 假设**.G_1,G_2 是阶为素数 p 的循环群.q-SDH 假设在(G_1,G_2)中成立指的是对所有的概率多项式时间算法 A,概率 $\Pr[A((g_1,g_2,g_2^{\gamma},g_2^{\gamma^2},\ldots,g_2^{\gamma^q})\in(G_1\times(G_2)^{q+1}))=(g_1^{1/(\gamma+x)},x)\wedge x\in Z_p^*]$ 是可忽略的.其中,$x,\gamma\in Z_p^*$,ψ是从群 G_2 到 G_1 的同构.$\psi(g_2)=g_1$.

Pedersen 承诺方案(commitment scheme)[13].给定阶为素数 q 的群 G,生成元为 g 和 h,对秘密消息 $x\in\mathbb{Z}_q$ 的承诺为随机选择 $r\leftarrow\mathbb{Z}_q$,计算承诺值 $C=g^xh^r$.该承诺方案是完备隐藏(information-theoretically hiding)的,并且在离散对数假设下是计算绑定(binding)的.

知识签名.在构造直接匿名证明方案时用到了知识签名这一工具.它允许一方在不泄露任何有用信息的情况下证明他知道一个秘密值.这种工具本质上是知识的零知识证明或最小泄露证明.

为了描述这些证明协议和签名,本文将采用 Camenisch 和 Stadler 给出的标记法[14]来描述零知识证明协议,例如, $PK\{\alpha,\beta,\delta: y=g^{\alpha}h^{\beta}\wedge\tilde{y}=\tilde{g}^{\alpha}=\tilde{h}^{\delta}\wedge(u\leqslant\alpha\leqslant v)\}$ 表示"关于整数α,β,δ的零知识证明,并且$y=g^{\alpha}h^{\beta}$, $\tilde{y}=\tilde{g}^{\alpha}\tilde{h}^{\delta}$成立,同时$(u\leqslant\alpha\leqslant v)$",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.同时,可以利用 Fiat-Shamir 启发式[15]将零知识证明转化为对消息 m 的知识签名,如可记作 $SPK\{(\alpha):y=g^{\alpha}\}(m)$.

2 基于双线性映射的直接匿名证明方案

2.1 密钥生成算法

给定安全参数 1^k,颁发者选择群 $G_1=\langle g_1\rangle,G_2=\langle g_2\rangle,G_T=\langle g_T\rangle,G_3=\langle g_3\rangle$,存在 $e:G_1\times G_2\to G_T,\psi(g_2)=g_1$,群的阶为长度为 k 的素数 p,并且随机选择$\gamma\in_R\mathbb{Z}/p\mathbb{Z}$和$(g,h)\in_R(G_1)^2$,计算 $Y=g_2^{\gamma}$,生成颁发者的公私钥对为

$$(pk,sk)=((p,g_1,g_2,g_3,g_T,Y,g,h),\gamma).$$

2.2 加入过程(join协议)

1. 首先执行 Pedersen 信息隐藏承诺方案.TPM 选择秘密信息 $f\in_R\mathbb{Z}/p\mathbb{Z}$,选择随机数 $t'\in_R\mathbb{Z}/p\mathbb{Z}$,计算 $C=g^fh^t$(f是承诺的秘密值),发送给颁发者,然后运行零知识证明协议,证明TPM拥有秘密知识f,t'.具体协议过程如下:
   a) TPM 随机选择 $r_f,r_{t'}\in_R(\mathbb{Z}/p\mathbb{Z})^2$,计算 $C'=g^{r_f}h^{r_{t'}}$,发送给颁发者.
   b) 颁发者随机选择 $c\in_R\mathbb{Z}/p\mathbb{Z}$,发送给 TPM.
   c) TPM 计算 $s_f=r_f+cf,s_{t'}=r_{t'}+ct'$,发送 $s_f,s_{t'}$给颁发者.
   d) 颁发者验证 $C'\stackrel{?}{=}C^{-c}g^{s_f}h^{s_{t'}}$.
2. 颁发者选择 $x\in_R\mathbb{Z}/p\mathbb{Z},t''\in_R\mathbb{Z}/p\mathbb{Z}$,计算 $A=(g_1Ch^{t''})^{1/(\gamma+x)}$,发送 A,x,t''给主机.
3. 主机存储 A,x,发送 t''给 TPM.
4. TPM 计算 $t=t'+t''$,存储 f,t,主机验证等式(1)是否成立.在主机验证过程中,$e(g^f,g_2)$和 $e(h^t,g_2)$的值可以向TPM请求而获得

$$e(A,Yg_2^x)=e(g_1,g_2)\cdot e(g^f,g_2)\cdot e(h^t,g_2) \tag{1}$$

讨论:通过 Join 协议过程,可信计算平台得到成员证书(A,x,t)以及秘密信息f,其中,主机存储(A,x),TPM 存储(f,t).从该协议可以看出,TPM 可以在保持匿名性的同时,使用同一个秘密信息 f 多次申请成员证书.

2.3 签名过程(sign)

1. 主机随机选取 $w\in_R\mathbb{Z}/p\mathbb{Z}$,计算 $T_1=(Ah^w),T_2=g^wh^{-x},T_1,T_2$ 是对 A,x 的承诺,证明等式(2)、等式(3)成立:

$$e(T_1,Y)/e(g_1,g_2)=e(h,Y)^we(h,g_2)^{wx+t}e(g,g_2)^f/e(T_1,g_2)^x \tag{2}$$

$$T_2=g^wh^{-x},\ T_2^{-x}g^{wx}h^{-xx}=1 \tag{3}$$

2. 证明可信计算平台拥有知识f,x,w,t,使得等式(2)、等式(3)成立.利用 Fiat-Shamir 启发式[15],将对知识f,x,w,t 的零知识证明转换为知识签名,计算辅助值$\delta_1=wx,\delta_2=-xx$,其中,$H:\{0,1\}^*\to\mathbb{Z}_p$:
   a) 首先,TPM 随机选取 $r_f\in\mathbb{Z}/p\mathbb{Z},r_t\in\mathbb{Z}/p\mathbb{Z}$,计算 $\tilde{R}_1$,将 $\tilde{R}_1$ 发送给主机:

$$\tilde{R}_1=e(g,g_2)^{r_f}e(h,g_2)^{r_t}.$$

   b) 主机选取 $r_x,r_w,r_{\delta_1},r_{\delta_2}\in\mathbb{Z}/p\mathbb{Z}$, 计算

$$R_1=\tilde{R}_1e(h,Y)^{r_w}e(T_1,g_2)^{r_x}e(h,g_2)^{r_{\delta_1}},\ R_2=g^{r_w}h^{r_x},\ R_3=T_2^{r_x}g^{r_{\delta_1}}h^{r_{\delta_2}}.$$

   c) 主机计算 $c_h=H(g\|h\|g_1\|g_2\|g_T\|Y\|T_1\|T_2\|R_1\|R_2\|R_3\|)$,发送 c_h 给 TPM.
   d) TPM 选择 $n_t\in_R\mathbb{Z}/p\mathbb{Z}$,计算 $c=H(H(c_h\|n_t)\|m)$.

e) 主机计算 $s_x=r_x+c(-x), s_{\delta_1}=r_{\delta_1}+c\delta_1, s_w=r_w+cw, s_{\delta_2}=r_{\delta_2}+c\delta_2$,TPM 计算 $s_f=r_f+cf, s_t=r_t+c(-t)$.

3. 最后,主机输出签名是 $\sigma=(T_1,T_2,c,n_t,s_f,s_x,s_t,s_w,s_{\delta_1},s_{\delta_2})$.

2.4 验证过程(verify)

1. 给定消息 m 的签名 $\sigma=(T_1,T_2,c,n_t,s_f,s_t,s_x,s_w,s_{\delta_1},s_{\delta_2})$ 和公钥(p,g_1,g_2,g_T,Y,g,h);

2. 计算

$$R_1'=e(g,g_2)^{s_f}e(h,Y)^{s_w}e(h,g_2)^{s_{\delta_1}+s_t}e(T_1,g_2)^{s_x}(e(T_1,Y)/e(g_1,g_2))^{-c},\ R_2'=T_2^{-c}g^{s_w}h^{s_x},\ R_3'=T_2^{s_x}g^{s_{\delta_1}}h^{s_{\delta_2}}.$$

3. 验证以下等式是否成立:

$$c\overset{?}{=}H(H(H(g\|h\|g_1\|g_2\|g_T\|Y\|T_1\|T_2\|R_1'\|R_2'\|R_3')\|n_t)\|m).$$

2.5 可变匿名性机制

第 2.3 节中给出的签名对验证方来说是完全匿名的,为了达到可变匿名性,可信计算平台在产生签名时使用 TPM 的秘密 f 计算一个承诺值 T_3;同时,计算时将选择一个签名唯一标示符(solely signature identifier,简称 SSID).如果可信计算平台在签名时选择的 SSID 是相同的,那么由该可信计算平台生成的签名是可关联(linkability)的;如果可信计算平台在生成签名时随机选择 SSID,那么生成的签名是完全匿名的.SSID 在选择时可以由 TPM 和验证者共同协商确定.

为了提供可变的匿名性机制,在执行签名操作时,同时执行下面的运算(这里是在群 G_3 中计算):

$$\eta=H_1(SSID), T_3=\eta^f, R_4=\eta^{r_f}, R_4'=T_3^{-c}\eta^{s_f}, c=H(H(H(\eta\|g\|h\|g_1\|g_2\|g_3\|g_T\|Y\|T_1\|T_2\|T_3\|R_1\|R_2\|R_3\|R_4)\|n_t)m),$$

其中,$H_1:\{0,1\}^*\to G_3$.加入匿名性机制之后输出的签名是 $\sigma=(\eta,T_1,T_2,T_3,c,n_t,s_f,s_t,s_x,s_w,s_{\delta_1},s_{\delta_2})$.

验证签名是否成立的等式为

$$c\overset{?}{=}H(H(H(\eta\|g\|h\|g_1\|g_2\|g_3\|g_T\|Y\|T_1\|T_2\|T_3\|R_1'\|R_2'\|R_3'\|R_4')\|n_t)\|m).$$

2.6 假冒TPM检测(rogue tagging)

如果 TPM 内部的秘密 f 泄露,那么验证者在签名验证时必须对 TPM 进行检测,以确定签名是否来自于被攻陷的 TPM.检测的方法是:将已经泄露的 TPM 秘密信息 f 加入到撤销列表(其中保存了所有假冒 TPM 的秘密 f)中,对于在撤销列表中的 f,验证者计算:

$$T_3\overset{?}{=}\eta^f.$$

如果存在某个 f 使得等式成立,那么该签名来自假冒的或者已经撤销的 TPM.

3 性能和效率分析

签名长度.本文的直接匿名证明方案,如果考虑匿名性保护机制,最后得到的签名 σ 包括了 4 个群 G_1 中的元素和 8 个 $\mathbb{Z}_p$ 中的元素.假设 $G_1\neq G_2$,利用文献[16]中定义的椭圆曲线族,当 $|p|=170$ 时,G_T 和 G_1 中的元素长度分别为 1 020 比特和 171 比特,则本文提出的 BM-DAA 方案的签名长度为 2 044 比特.

计算效率.由于指数运算/多指数运算和双线性对运算是最耗时的运算,本文将根据方案中用到的指数运算(多指数运算)和双线性对运算来估算计算开销.下面分别计算方案中加入过程、签名操作和验证操作的可信计算平台的计算开销(考虑匿名性机制).其中,双线性运算 $e(g,g_2),e(h,Y),e(h,g_2),e(T_1,g_2)=e(A,g_2)\cdot e(h,g_2)^w$ 都是可以预先计算的:

a) 加入过程:TPM 做 2 次指数运算.

b) 签名操作:主机做 5 次指数运算,TPM 做 4 次指数运算.

c) 验证操作:4 次多指数运算和 1 次双线性运算.

4 方案比较

性能比较.本节将 HS 方案[10]、BCC 方案[1]和我们提出的方案进行比较,具体的性能指标在表 1 中列出.其中,BM 表示双线性运算,ME 表示指数运算(多指数运算),SC 表示模平方运算,MC 表示乘法运算.由于在计算过程中 TPM 的计算量是一个非常重要的性能指标,因此我们将比较在签名过程中 TPM 的计算量.对于指数运算,我们将参照文献[17]给出的方法估算计算开销.对于某个指数运算,设 m_1 是指数的二进制表示的比特长度,m_2 是指数的二进制表示中 1 的个数,则该指数运算的计算开销可以估算为 m_1 次模平方运算和 m_2 次乘法运算.

Table 1 Performance comparison of direct anonymous attestation

表 1 直接匿名证明方案的性能比较

Schemes	Signature length (bit)	Total computational cost of sign process (TPM computation cost)	Computational cost of join process	Computational cost of sign process	Assumpations
BCC	20 555	8ME+0BM (16186SC+8093MC)	4ME+0BM	4ME+0BM	Strong-RSA, DDH
HS	7 614	3ME+0BM (2352SC+958MC)	5ME+0BM	3ME+0BM	Strong-RSA, DDH
This paper	2 044	9ME+0BM (855SC+425MC)	4ME+0BM	4ME+1BM	q-SDH, DDH

在 HS 方案中,安全参数的一般取值为

$$l_n=2048,\ \alpha=9/8,\ X=2^{792},\ Y=2^{520},\ l_s=540,\ l_b=300,\ l_c=160,$$

其长度至少为 7 614 比特.

而在 BCC 方案中,安全参数的一般取值如下:

$$l_n=2048,\ l_f=104,\ l_e=368,\ l'_e=120,\ l_v=2536,\ l_\phi=80,\ l_H=160,\ l_r=80,\ l_\Gamma=1632,\ l_\rho=208,$$

其长度至少为 20 555 比特.

从表 1 中可以看出,本文的方案与其他直接匿名证明方案相比,签名长度大为缩短,能够有效地节省传输带宽.更重要的是,由于该方案可以采用椭圆曲线来实现,因此指数运算的效率要比其他方案高;同时,最耗时的双线性对运算可以在主机上执行,为新一代基于 ECC 算法的 TPM 提供了一种隐私性保护解决方案.

安全级别比较.(1) 安全模型比较.本文与 BCC 方案、HS 方案采用了同一个安全模型,安全性定义是一致的,同样实现了不可伪造性、可变匿名性和不可关联性.(2) 安全假设比较.BCC 方案与 HS 方案都是基于强 RSA 假设和 DDH(decision Diffie-Hellman)假设,而本文的方案基于 q-SDH 假设和 DDH 假设.3 种方案都基于零知识证明技术来构建签名方案,安全证明中都使用了回绕(rewind)技术,因此,安全归约方法都有一定的局限性.(3) 安全参数的选择.不同的参数选择将决定不同的安全等级,根据椭圆曲线和 RSA 算法强度的比较(http://www.nsa.gov/ia/industry/crypto_elliptic_curve.cfm),如果采用“性能比较”中给出的安全参数,这 3 种方案能够提供相同的安全级别.

5 安全证明

定理 2. 在 q-SDH 假设和群 G_3 的 DDH 假设下,本文给出的 BM-DAA 方案安全地实现了一个直接匿名证明系统.

与文献[1]中的安全证明类似,本文将采用理想系统/现实系统(ideal-system/real-system)模型[18,19]来证明 BM-DAA 的安全性.理想系统/现实系统模型的基本思想是,在现实系统中存在一些参与方 P_i,并且有一个攻击方 A 以及环境 ε,攻击方 A 控制了一些参与方.ε 给参与方 P_i 提供输入,在运行完安全协议之后,参与方将输出提交给 ε,并且 ε 能够与 A 任意交互.在理想系统中,与现实系统有相同的参与方,但是参与方之间并不执行安全协议,而是将输入发送给可信方 T,并从可信方 T 处得到输出.该可信方 T 执行的理想函数性(ideal functionality)是所设计的安全协议预期要达到的功能.

安全性的定义是:如果对于任意的攻击方 A 和任意的环境 ε,在理想系统中存在一个模拟器 S,其中,S 控制的参与方与现实系统中 A 控制的参与方相同,使得 ε 不能区分自己是运行在现实系统中还是理想系统中,那么就认为该安全协议是安全的.因此,证明系统的安全性主要有如下 3 步:

(1) 给出理想系统的可信方 T;

(2) 在理想系统中构建一个模拟器 S;

(3) 证明模拟器能够成功地模拟 A,使得环境ε不能区分.

5.1 理想系统可信方T

下面首先给出 BM-DAA 方案理想系统的可信方 T.该可信方与文献[1]中给出的可信方基本上是一致的.在理想系统中有如下的参与方:一个颁发者 I,一个身份为 id_i 可信平台模块 TPM,一个带 TPM 的可信计算平台 H_i,一个验证者 V_j.下面将给出 BM-DAA 方案的理想系统中的可信方 T.可信方 T 支持如下的操作:

初始化操作(setup).每个参与方与 T 交互,表明该参与方是否已经被攻击方攻陷(corrupted).

加入操作(join).可信计算平台 H_i 向 T 发出请求,希望成为群成员,T 询问 M_i 是否希望成为群的一员,如果 M_i 同意,T 向颁发者 I 发送消息表明身份为 id_i 的可信计算平台希望加入;如果 M_i 是假冒的,那么 T 将向颁发者 I 表明这一点.如果 I 批准,那么 T 向 H_i 通知其已经成功地加入.

签名/验证操作(sign/verify).H_i 拟对消息 m 做签名,用的签名唯一标识符为 $SSID\in\{0,1\}^*\cup\{\perp\}$.$H_i$ 将 m,$SSID$ 发送给 T.首先,T 验证 H_i/M_i 是否群的成员,如果不是,T 将拒绝 H_i/M_i 的请求;否则,T 将 m 交给相应的 M_i,询问是否同意签名.如果 M_i 同意,那么 T 询问 H_i 是否需要签名.如果 H_i 没有退出,那么 T 执行如下步骤:

(1) 如果 M_i 是假冒的,那么 T 通知 V_j:假冒 TPM 对 m 进行了签名.

(2) 如果 $SSID=\perp$,那么 T 通知 V_j:H_i/M_i 已经对 m 进行了签名.

(3) 如果 $SSID\neq\perp$,那么 T 检查 H_i/M_i 是否已经用参数 $SSID$ 对消息进行了签名.如果是,T 就在其假名数据库中查找对应的假名 P;如果不是,就随机生成一个假名 $P\in_R G_3$,T 通知 V_j 假名为 P 的平台对消息 m 签名.

该理想系统具有如下的安全特性:

(1) 不可伪造性(unforgeability):不是群成员的用户或者已经被撤销的群成员不能成功地做签名操作.

(2) 可变匿名性(variable anonymity):验证者不能标识出签名者的身份,如果 $SSID=\perp$,那么签名是完全匿名的;如果 $SSID\neq\perp$,那么签名具有部分的匿名性,验证者通过假名 P 标识签名者.

(3) 不可关联性(unlinkability):如果 $SSID=\perp$,那么验证者无法区分两个不同的签名是否由同一个可信计算平台签发.

5.2 模拟器S

本节将在理想系统中构造模拟器 S.在下面的讨论中,沿用了文献[1]提出的标记,大写字母表示该参与方没有被攻陷(corrupted),小写字母表示已经被攻陷.如,(Ihm)表示颁发者 I 是诚实的参与方,主机和 TPM 已经被攻陷.

5.2.1 系统初始化的模拟

系统初始化的模拟是针对颁发者进行的,分为两种情况,分别是(i)和(I).

(i) 如果颁发者被攻陷,那么模拟器 S 从攻击方处接收到颁发者的公钥$(p,g_1,g_2,g_3,g_T,Y,g,h)$;

(I) 如果颁发者是诚实的,那么模拟器 S 运行密钥生成算法得到公钥$(p,g_1,g_2,g_3,g_T,Y,g,h)$和私钥$\gamma$.

5.2.2 Join 的模拟

在 Join 的模拟过程中,根据颁发者 I、主机 H_i 和 TPM M_i 是否被攻陷,可以分为 6 种情况,分别为(IHM),(Ihm),(IhM),(iHM),(ihm),(ihM),下面将分别加以讨论:

(IHM),(ihm):在这两种情况下,所有的操作都是在参与方之间进行的,不需要触发模拟器.

(Ihm):在这种情况下,颁发者 I 没有被攻陷,可信计算平台(h 和 m)被攻陷.模拟器 S 从攻击方 A 处得到加入请求,S 与 A 交互,运行 Join 协议.在这个过程中,A 同时将 T_3 发送给 S 用于假冒 TPM 检测,如果 S 第 1 次接收到 T_3,那么 S 存储 T_3,同时通知可信方 T 可信计算平台 H_i 请求加入,模拟器 S 在与可信方通信的过程中将扮演理想系统中的 M_i 的角色.如果可信方 T 同意 H_i 加入,那么模拟器 S 与攻击方 A 将交互完成 Join 协议;如果 T 不同意,那么模拟器 S 将中止协议.

(IhM):这种情况与(Ihm)类似,但不同的是,模拟器将执行 Join 过程中 TPM M_i 执行的动作.

(iHM):在这种情况下,模拟器 S 从可信方 T 处得到平台 id_i 的加入请求.在理想系统中,S 将扮演颁发者的角色,在与攻击方交互的过程中模拟现实系统中的 H_i/M_i,如果 Join 协议能够成功地完成,那么 S 将从攻击方 A 处得到证书(A,x,t),S 存储证书和秘密信息 f 并通知 T 允许平台加入;如果 S 没有成功地完成 Join 协议,那么 S 将通知 T 不允许平台加入.

(ihM):模拟器 S 从攻击方 A 从得到 H_i 的请求,要求 M_i 加入群,模拟器 S 向可信方 T 发送信息表明 H_i 希望加入群.之后,S 从可信方 T 处得到请求消息,表明具有身份 id_i 能否加入.接下来,模拟器 S 以 TPM M_i 运行 Join 协议.如果 Join 协议能够成功地完成,S 从攻击方处得到 t'',存储 t'',通知可信方 T 该平台允许加入;否则,S 通知 T 平台不允许加入.

5.2.3 Verify 的模拟

在 Verify 的模拟过程中,主要探讨 3 种情况:分别为(HV),(hv),(hV).下面分别加以讨论:

(hv),(HV):在这两种情况下,所有的操作都在参与方之间进行,不需要触发模拟器.

(hV):模拟器 S 从攻击方处得到对消息 m 的签名$\sigma=(\eta,T_1,T_2,T_3,c,n_t,s_f,s_t,s_x,s_w,s_{\delta_1},s_{\delta_2})$,首先验证签名$\sigma$的正确性.若签名$\sigma$不合法,则 S 忽略消息请求;若σ合法,则需要做假冒 TPM 检测,根据撤销列表中的 f 验证 $T_3\overset{?}{=}\eta^f$.

(a) 如果找到对应的 f 使得 $T_3=\eta^f$,那么模拟器 S 检查是否存在与 f 对应的 id_i,如果存在这样的 id_i,那么 S 作为主机 H_i 请求可信方 T 对消息 m 签名;如果不存在对应的 id_i,那么 S 检查签名中的消息对$\langle\eta,T_3\rangle$是否是第一次出现,S 选择一个已经被攻陷的 M_i(该 M_i 还没有成为群成员),以 M_i 的身份请求可信方 T 加入,并且将该 M_i 标记为假冒的,最后以 H_i 的身份对消息 m 签名.

(b) 如果找不到对应的 f,则表明对 m 进行签名的平台是假冒的,但还没有放入撤销列表.模拟器 S 必须找出签名来自于哪个平台,模拟器检查签名中的$\langle\eta,T_3\rangle$以前是否出现过.

- 如果$\langle\eta,T_3\rangle$不是第一次出现,那么 S 做如下的操作:
  - 如果 S 在 Sign 的模拟过程中使用了$\langle\eta,T_3\rangle$,但是 S 已经在 Sign 的模拟过程中回答了可信方,那么 S 输出“模拟失败”.S 模拟失败的原因在于,攻击方伪造了签名,并且签名中 T_3 是模拟器选择的.因为该签名本质上是对 T_3 的离散对数的零知识证明,因此,如果存在这样的攻击方 A,就存在另一个攻击方 A',A'调用攻击方 A,利用回绕(rewinding)技术能够解决群 G_3 上的 DDH 问题.
  - 否则,找到与$\langle\eta,T_3\rangle$对应的主机 H_i,TPM M_i,作为主机 H_i 与可信方 T 交互,完成对 m 的签名.
- 如果$\langle\eta,T_3\rangle$是第一次出现,模拟器 S 为$\langle\eta,T_3\rangle$找到对应的 TPM M_i.TPM 已经被攻陷.
  - 如果 $SSID=\perp$,那么 S 任选一个没有标记为假冒 TPM 的 M_i,S 与 T 交互完成对消息 m 的签名.
  - 如果 $SSID\neq\perp$,那么 S 选择一个没有标记为假冒 TPM 的 M_i,如果能够找到这样的 M_i,那么 S 与 T 交互完成对消息 m 的签名;如果找不到,则表明攻击方可以成功地伪造签名,S 将模拟失败.但是,由附录的引理 2 可知,如果攻击方能够成功地伪造签名,那么必定存在一种算法可以攻破 q-SDH 难题.

5.3 模拟器的正确性

最后,证明环境ε不能区分自己是运行在现实系统中还是理想系统中,也就是说,证明现实系统和理想系统中的输出参数是计算不可区分的.在模拟的过程中,S 扮演了现实系统中的不同角色.模拟器 S 在模拟过程中选择的参数(输出)有一些 s_*以及 T_*,这些参数都是随机选定的,而在现实系统中,这些参数是由秘密信息经过计算得到的.由于这些参数是统计不可区分的,因此在$\mathbb{Z}_p$中也是计算不可区分的.

另外,c 由模拟器随机选择,在现实系统中是 Hash 函数的计算结果.由于是在随机预言机模型下,所以这两者是计算不可区分的.

6 结 论

本文基于双线性映射提出了一种直接匿名证明方案,并对其性能和效率进行了分析.与 HS 方案和 BCC 方案相比,本文提出的方案的签名长度更短,在签名过程中,TPM 的计算量更少.该方案为基于椭圆曲线的 TPM 提

供了一种隐私性保护解决方案.本文的直接匿名证明方案满足不可伪造性、可变匿名性和不可关联性.

References:

[1] Brickell EF, Camenisch J, Chen LQ. Direct anonymous attestation. In: Brickell E, Camenisch J, Chen LQ, eds. Proc. of the ACM Conf. on Computer and Communications Security. New York: ACM Press, 2004. 132−145.

[2] Chaum D, van Heyst E. Group signature. In: Davies DW, ed. Advances in Cryptology—Eurocrypt'91. Berlin: Springer-Verlag, 1992. 257−265.

[3] He YF, Zhang JZ. An efficient and secure dynamic group signature scheme. Journal of Software, 2005,16(4):609−615 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/16/609.htm [doi: 10.1360/jos160609]

[4] Camenisch J. Better privacy for trusted computing platforms. In: Molva D, ed. Proc. of the ESORICS. Berlin: Springer-Verlag, 2004. 73−88.

[5] Brickell E, Li JT. Enhanced privacy ID: A direct anonymous attestation scheme with Enhanced revocation capabilities. Technical Report, 2007/194, 2007.

[6] Smyth B, Ryan M, Chen LQ, Ryan M. Direct anonymous attestation (DAA): Ensuring privacy with corrupt administrators. In: Stajano F, ed. Proc. of the 4th European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS 2007). LNCS 4572, Berlin: Springer-Verlag, 2007. 218−231.

[7] Backes M, Maffei M, Unruh D. Zero-Knowledge in the applied pi-calculus and automated verification of the direct anonymous attestaion protocol. Technical Report, 2007/289, 2007.

[8] Camenisch J. Protecting (anonymous) credentials with the trusted computing group's TPM V1.2. In: Proc. of the SEC 2006. Berlin: Springer-Verlag, 2006. 135−147.

[9] Leung A, Mitchell CJ. Ninja: Non identity based, privacy preserving authentication for ubiquitous environments. In: Krumm P, ed. Proc. of the 9th Int'l Conf. on Ubiquitous Computing. LNCS 4717, Berlin: Springer-Verlag, 2007. 73−90.

[10] He G, Tate SR. A direct anonymous attestation scheme for embedded devices. In: Proc. of the Public Key Cryptography 2007. Berlin: Springer-Verlag, 2007. 16−30.

[11] Boneh D, Shacham H. Group signatures with verifier-local revocation. In: Atluri V, Pfitzmann B, McDaniel PD, eds. Proc. of the ACM Conf. on Computer and Communications Security. New York: ACM Press, 2004. 168−177.

[12] Furukawa J, Imai H. An efficient group signature scheme from bilinear maps. IEICE Trans. on Fundamentals, 2006,89-A(5): 1328−1338.

[13] Pedersen TP. Non-Interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum J, ed. Advances in Cryptology—CRYPTO'91. LNCS 576, Berlin: Springer-Verlag, 1992. 129−140.

[14] Camenisch J, Stadler M. Efficient group signature schemes for large groups. In: Kaliski B, ed. Advances in Cryptology—CRYPTO'97. LNCS 1296, Berlin: Springer-Verlag, 1997. 410−424.

[15] Fiat A, Shamir A. How to prove yourself: Practical solutions to identification and signature problems. In: Proc. of the CRYPTO'86. LNCS 263, Berlin: Springer-Verlag, 1986. 186−194.

[16] Miyaji A, Nakabayashi M, Takano S. New explicit conditions of elliptic curve traces for FR-reduction. IEICE Trans. on Fundamentals, 2002,E85-A(2):481−484.

[17] Menezes A, van Oorschot P, Vanstone S. Handbook of Applied Cryptography. CRC Press, Inc., 1997. 613−619.

[18] Canetti R. Studies in secure multiparty computation and applications [Ph.D. Thesis]. Rehovot: Weizmann Institute of Science, 1995.

[19] Pfitzmann B, Waidner M. Composition and integrity preservation of secure reactive systems. In: Gritzalis D, Jajodia S, eds. Proc. of the 7th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2000. 245−254.

[20] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures. Journal of Cryptology, 2000,13(3):361−396. [doi: 10.1007/s001450010003]

附中文参考文献:

[3] 何业锋,张建中.一种有效且安全的动态群签名方案.软件学报,2005,16(4):609−615. http://www.jos.org.cn/1000-9825/16/609.htm [doi: 10.1360/jos160609]

附录

引理 1. 给定 m 的两个签名:

$\{\eta,T_1,T_2,T_3,c_1,n_t,R_1',R_2',R_3',R_4',s_f',s_t',s_x',s_w',s_{\delta_1}',s_{\delta_2}',H_1\}$, $\{\eta,T_1,T_2,T_3,c_2,n_t,R_1',R_2',R_3',R_4',s_f'',s_x'',s_t'',s_w'',s_{\delta_1}'',s_{\delta_2}'',H_2\}$,

使得 $$(s'_f,s'_x,s'_t,s'_w,s'_{\delta_1},s'_{\delta_2})\neq(s''_f,s''_x,s''_t,s''_w,s''_{\delta_1},s''_{\delta_2}),$$

$$c_1=H_1(H_1(H_1(\eta\|g\|h\|g_1\|g_2\|g_3\|g_T\|Y\|T_1\|T_2\|T_3\|R'_1\|R'_2\|R'_3\|R'_4)\|n_t)\|m)\neq$$

$$c_2=H_2(H_2(H_2(\eta\|g\|h\|g_1\|g_2\|g_3\|g_T\|Y\|T_1\|T_2\|T_3\|R'_1\|R'_2\|R'_3\|R'_4)\|n_t)\|m),$$

$$R'_1=e(g,g_2)^{s'_f}e(h,Y)^{s'_w}e(h,g_2)^{s'_{\delta_1}+s'_t}e(T_1,g_2)^{s'_x}(e(T_1,Y)/e(g_1,g_2))^{-c_1},$$

$$R'_1=e(g,g_2)^{s''_f}e(h,Y)^{s''_w}e(h,g_2)^{s''_{\delta_1}+s''_t}e(T_1,g_2)^{s''_x}(e(T_1,Y)/e(g_1,g_2))^{-c_2},$$

$$R'_2=T_2^{-c_1}g^{s'_w}h^{s'_x},\ R'_2=T_2^{-c_2}g^{s''_w}h^{s''_x},\ R'_3=T_2^{s'_x}g^{s'_{\delta_1}}h^{s'_{\delta_2}},\ R'_3=T_2^{s''_x}g^{s''_{\delta_1}}h^{s''_{\delta_2}},\ R'_4=T_3^{-c_1}\eta^{s'_f},\ R'_4=T_3^{-c_2}\eta^{s''_f},$$

那么可以计算出(A,x,t,w,f)满足方程(1).

证明:下面的(A,x,t,w,f)满足引理 1:

$$A=\frac{T_1}{h^{\left(\frac{s'_w-s''_w}{c_1-c_2}\right)}},\ x=\frac{s''_x-s'_x}{c_1-c_2},\ f=\frac{s'_f-s''_f}{c_1-c_2},\ w=\frac{s'_w-s''_w}{c_1-c_2},\ t=\frac{s'_t-s''_t}{c_1-c_2}.$$ □

引理 2. 在颁发者没有被攻陷的情况下,如果存在攻击方 $\bar{A}$ 运行 Join 协议少于 $q-1$ 次,能够伪造出合法签名 $(m,\sigma=(\eta,T_1,T_2,T_3,c,n_t,s_f,s_t,s_x,s_w,s_{\delta_1},s_{\delta_2}))$,就存在一个攻击方 $\bar{A}'$ 能够解决 q-SDH 问题.

证明:假设算法 $\bar{A}'$ 的输入为 $q+2$ 元组 $(g_1,g_2,g_2^{\gamma},g_2^{\gamma^2},...,g_2^{\gamma^q})$,$\psi(g_2)=g_1$,$\bar{A}'$ 与 $\bar{A}$ 做如下的游戏(game):

1. $\bar{A}'$ 选择 $\alpha\in_R\mathbb{Z}/p\mathbb{Z},\{(a_i,b_i)\in_R(\mathbb{Z}/p\mathbb{Z})^2\}_{i\in[q-1],m\in_R[q-1]}$.

2. 令 $\omega=\gamma-a_m$. $\bar{A}'$ 选择 $\theta\in_R\mathbb{Z}/p\mathbb{Z}$,生成颁发者公钥信息如下:

$$G_2=g_2^{\left[b_m\prod_{i=1,i\neq m}^{q-1}(\gamma+a_i-a_m)\right]}g_2^{\left[\alpha\prod_{i=1}^{q-1}(\gamma+a_i-a_m)\right]},\ G_1=\psi(G_2),\ g=\psi(g_2)^{\left[\prod_{i=1,i\neq m}^{q-1}(\gamma+a_i-a_m)\right]},\ h=g^{\theta},\ Y=G_2^{\omega}.$$

3. $\bar{A}'$ 输出公钥 $pk=(p,G_1,G_2,Y,g,h)$,将 pk 发送给 $\bar{A}$.

4. $\bar{A}'$ 调用 $\bar{A}$(作为需要加入群的可信计算平台)运行 Join 协议:

a) $\bar{A}'$ 回绕(rewind)调用 $\bar{A}$ 得到 f,t'.

b) $\bar{A}'$ 产生 A,x,t''

$$t''=(b_i-f)/\theta-t',\ x=a_i,\ A=(G_1g^fh^{t'+t''})^{1/(\omega+x)}=(G_1g^{b_i})^{1/(\omega+a_i)}=\psi(g_2)^{\left[(b_m+b_i)\prod_{j=1,j\neq m,i}^{q-1}(\gamma+a_j-a_m)\right]}\psi(g_2)^{\left[\alpha\prod_{j=1,j\neq i}^{q-1}(\gamma+a_j-a_m)\right]}.$$

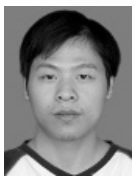
$\bar{A}'$ 发送 (A,x,t'') 给 $\bar{A}$.

5. $\bar{A}$ 输出签名对 (m,σ),使得验证算法能够通过.根据 Forking 引理[20]和引理 1,$\bar{A}'$ 计算得出 $(A,x,t,f)\in G_1\times(\mathbb{Z}_p)^5$ 满足等式(1).其中,

$$A=(G_1g^fh^{t'+t''})^{1/(\omega+x)}=(G_1g^{\theta t+f})^{1/(\omega+x)}=\psi(g_2)^{\left[\frac{\alpha\gamma+(\theta t+f)+b_m}{\gamma-a_m+x}\prod_{j=1,j\neq m}^{q-1}(\gamma+a_j-a_m)\right]}.$$

将等式进行化简,得到 $A=\psi(g_2)^{\sum_{i=0}^{q-1}c_i\gamma^i+(c_q/(\gamma-a_m+x))}$.

从以上分析可以得出,对给定的 q-SDH 元组,其解为 $\left(\left(A\Big/\left(\psi(g_2)^{\sum_{i=0}^{q-1}c_i\gamma^i}\right)\right)^{(1/c_q)},x-a_m\right)$. □



陈小峰(1980－),男,浙江金华人,博士,主要研究领域为网络与信息安全,可信计算.

冯登国(1965－),男,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为网络与信息安全.