doi:10.3969/j.issn.1000-436x.2013.z1.013

基于可信平台模（TPCM）的盲签名方案

黄文廷，佟玲玲，王永建
（国家计算机网络应急技术处理协调中心，北京 100029）

摘 要：针对基于身份的盲签名过程中 PKG 密钥泄露问题，提出了基于可信平台控制模块的盲签名方案，该方案中签名信息对签名者不可见，无法追踪签名信息。盲签名方案采用可信的秘密共享分配中心(SDC, share distribution center)和 TPCM 合作生成用户的签名密钥，不单独产生用户私有密钥，解决了用户的密钥托管问题，可以有效地防止用户的密钥泄露，保护了用户的匿名性和签名的不可追踪。最后在随机语言机模型下证明了该方案的安全性，与传统的盲签名方案对比，本方案计算效率较高。

关键词：盲签名；双线性映射；SDC；随机预言机
中图分类号：TP309.7 **文献标识码**：A **文章编号**：1000-436X(2013)Z1-0101-05

Blind signature scheme based on trusted platform computation module

HUANG Wen-ting, TONG Ling-ling, WANG Yong-jian
(National Computer Network Emergency Response Technical Team Coordination Centre, Beijing 100029, China)

Abstract: For the key leak problem in identity-based blind signature, a blind signature scheme based on the trusted platform control module (TPCM) was presented. The message which will be signed is unknown to the signer, and the information of the signature cannot be tracked. In the blind signature scheme, the secret share distribution center and the TPCM cooperate to generate the user's signature key, and the user's private key is not alone to be produced. So it solves the key escrow problem, and can also be effective to prevent disclosure of the user's key and protect the user's anonymity and the no track of the signature. Finally random oracle was used to prove the security of the scheme. Compared with the traditional scheme, the proposed scheme has better computational efficiency.

Key words: blind signature; bilinear map; SDC; random oracle

1 引言

基于身份密码学的概念和模型最早由 SHAMIR 在 1984 年提出[1]，该模型大大简化了 PKI 繁琐的工作。同时在该模型中，公钥可以由用户的任何身份信息生成；用户私有密钥由可信第三方给用户产生，该可信第三方被称为 PKG (private key generator)。相比基于证书的密码机制，基于身份密码体制更加方便和有效，因而得到了更为广泛的应用[2]。

文献[3]论述的方案是最早基于身份加密的方案，该方案使用双线对完成了基于身份的加密。文献[4]论述了一种新的门限签名方案，该方案基于用户身份生成签名密钥，具有较高的效率。但是基于身份的密码体制存在密钥托管问题，在基于身份的密码体制中，用户的密钥都是由可信第三方管理，可信第三方知道所有用户的私钥，如果可信第三方被攻陷，那么它可以冒充任何用户进行签名和加密操作，为解决这一安全问题，文献[5,6]提出了分布式密钥管理中心方案，用户的私有密钥由多个 PKG 共同创建，然而这一方案并不抵抗合谋攻击，足够多的 PKG 依然能够伪造用户的签名和冒充用户进行加密。文献[7~9]提出了一种新的基于身份的签名

收稿日期：2013-08-08
基金项目：国家高技术研究发展计划（“863”计划）基金资助项目（2013AA011102）；国家自然科学基金资助项目（61001091,61271118）
Foundation Items: The National High Technology Research and Development Program of China (863 Program) (2013AA011102); The National Natural Science Foundation of China(61001091, 61271118)

方案，该方案能够防止 PKG 伪造签名，可以对用户的密钥进行有效的管理，随后在这一方案的基础上在提出了基于身份的门限环签名方案。

CHAUM 在 1982 年提出了一种新的签名方案——盲签名[9]。盲签名方案具有盲性，签名人不知道签名的内容。盲签名可以有效保护所签署消息的具体内容，因此盲签名广泛应用到电子商务和电子选举中。盲签名和一般的签名相比有 2 点不同：第一，签名者不知道其签名信息的具体内容；第二，无法追踪到签名信息，即使签名信息被公开，签名者也无法判断改签名的具体信息。自从盲签名诞生之后，国内外产生了许多盲签名方案。文献[10]论述了基于 RSA 的盲签名方案，该方案安全性较高，但是计算效率较低。为了提高盲签名的计算效率，文献[11]等提出了一个基于双线性对的盲签名方案。文献[12]提出了标准模型下的基于双线性对的盲签名方案，该方案计算效率较高但是不能抵抗选择密文攻击。为了进一步提高盲签名的安全性，文献[13]提出了基于身份的盲签名方案，该方案可以抵抗选择密文攻击，但是计算效率较低。为了提高盲签名的计算效率，文献[14]首次构造了标准模型下的基于身份的限制性部分盲签名方案，但是该方案仅能抵挡选择密文攻击的 I 型攻击。文献[15]提出了第一个基于身份的部分盲签名方案，并使用随机预言机证明该方案的安全性，但是该签名方案没有解决身份信息泄露的问题。

当前盲签名的私钥生成中心(PKG)可以使用系统的主密钥计算出任意一个签名者地私钥，因此 PKG 可以伪造系统内合法用户有效地签名，而且验证方无法判断 PKG 是否有欺骗行为，因此为了解决这一问题，本文提出了基于可信平台控制模块(TPCM, trusted platform control module)的盲签名方案，TPCM 是由国内著名信息安全专家沈昌祥院士提出，与 TCG 提出的可信平台模块(TPM)不同，TPCM 里面加入了主动度量模块以及访问控制模块，可以主动对交互对象进行度量且可作为密码运算引擎对外提供加解密的密码运服务。其内部拥有受保护的安全存储单元、可存储密钥等敏感数据。通过 TPCM 功能支持、可信计算平台能够提供各种安全服务，可以实现用户等级的区分。本文的盲签名方案采用秘密共享分配中心(SDC, share distribution center)和 TPCM 合作生成用户的身份密钥，用户私有密钥不单独产生，阻止了用户的密钥泄露，实现了用户的匿名性以及签名信息的不可追踪。

2 预备知识

定义 1 双线性群

群 $G_1=<g_1>$ 和群 $G_2=<g_2>$ 是 2 个 p 加法群和群， p 是一个大素数，群 G_2 和 G_1 上的离散对数是难解的，ϕ 是群 G_2 到 G_1 可计算重构，群 G_1、G_2 为一对双线性群当且仅当满足以下性质：

1) 可计算的双线性：存在可计算的映射 $e:G_1\times G_2\to G_3$ (G_3 也是一个阶为 q 的循环群)使得任意的 $\eta\in G_1$， $\gamma\in G_2$，都存在 $e(\eta^a,\gamma^b)=e(\eta,\gamma)^{ab}$；

2) 非退化性：对于群上的生成元 g_1、g_2，$e(g_1,g_2)\neq 1$。

定义 2 计算性 Diffie-Hellman 问题（CDHP）

给定 $(g,g^a,g^b)\in G$，$a,b\in Z_p$，P 是一个大素数，计算 g^{ab}，假设存在一个敌手 A 在 t 时间内进行 q 次提问后，计算出 g^{ab} 的概率为 $Pr[A(g^a,g^b,g^{ab}]\leqslant\varepsilon$，而 ε 是可忽略的。

3 签名方案

系统参数建立：设 (G_1,G_2) 为一对双线性群，系统参数的生成，给定一个大素数 P 以及 P 阶的循环群 $(G_1,+)$，$(G_2,\cdot)$，设双线性映射为 $e:G_1\times G_1\to G_2$，给定 $H_1:\{0,1\}^*\to G_1$， $H_1:\{0,1\}^*\to Z_p^*$ 为无碰撞的 Hash 函数，选择双线性映射 $e:G_1\times G_1\to G_2$，其中 g_1、g_2 分别为群 G_1、G_2 的生成元，$I=e(g_1,g_1)$，选择无碰撞的散列函数 $H_1\{0,1\}^*\to Z_p^*$， $H_2:\{0,1\}^l\to G_1$ 选择 $s\in Z_p^*$ 为系统的私有密钥，$k_s=g_1^s$ 为系统的公开密钥，则系统的公开参数为 $(G_1,G_2,g_1,g_2,p,Pk_s,H_1,H_2,I)$。

3.1 用户密钥生成

每一个用户的 TPCM 随机选择 $x\in Z_p^*$，令 $K_u=g_1^x$ 作为用户的公开密钥，系统根据私有密钥 s、g_1、g_2 以及用户的 $ID\in\{0,1\}^*$，计算 $M=H_1(ID)$，从而得出客户端的部分私有密钥 $d=g_2^{sM}$，然后 SDC 选择 $r\in Z_p^*$，计算 $\sigma=(g_2^M)^{\frac{1}{x+g_1^d+sr}}$，将 (d,r,σ) 通过安全的信道发送到用户，用户收到 (d,r,σ) 之后计算等式 $e(\sigma,Ku\cdot g_1^{g_1^d}\cdot K_s^r)=e(g_2^M,g_1)$ 是否成立，如果成立，就接受私有密钥 $d=g_1^{sM}$。最后得出用户公开密钥为 $k_u=g_1^x$，私有密钥为 (d,x)。

3.2 签名过程

用户计算$U=I^d$，随后选择$\gamma_1,\gamma_2,\gamma_3,\gamma_4\in {}_RZ_P$，随后计算$B_1=g_1^{\gamma_1},B_2=g_2^{\gamma_2},B_3=g_3^{\gamma_1+\gamma_2},B_4=\Gamma_i T_1^{\gamma_1}T_2^{\gamma_2}$，用户选择$\delta_1,\delta_2,\delta_3,\delta_4,\delta_5\in {}_RZ_P$，计算$U_1=g_1^{\delta_1}$，$U_4=e(B_4,g)^{\delta_3}e(h_1,g)^{-\delta_4}e(h_1,\beta)^{-\delta_1}e(h_2,g)^{-\delta_5}e(h_2,\beta)^{-\delta_2}$；用户选择$\gamma_1,\gamma_2,\gamma_3\in {}_RZ_P$。然后用户对其要证明的摘要值$h(i)$计算$T=(B_1\|B_2\|B_3\|B_4\|U_1\|U_2\|U_3\|U_4\|h(i))$，$d_1=\delta_1+T\gamma_1,d_2=\delta_2+T\gamma_2,d_3=\delta_3+T\gamma_3$，$d_4=\delta_4+T\gamma_4$，最后计算$\varepsilon=dg-hxT$，于是群成员$i$生成了签名$\Delta=(U,\varepsilon,B_1,B_2,B_3,B_4,T,d_1,d_2,d_3,d_4,)$。

3.3 验证签名

对于$\Delta=(U,\varepsilon,B_1,B_2,B_3,B_4,T,d_1,d_2,d_3,d_4,)$，签名者身份 ID，验证者按照以下步骤验证签名的正确性：

1) 验证者将会计算$\bar{U}_1=g_1^{d_3}/B_1^T,\bar{U}_2=g_2^{d_2}/B_2^T,\bar{U}_3=g_3^{d_1+d_2}/B_3^T,\bar{U}_4=e(B_4,g)^{d_3}e(h_1,g)^{-d_4}e(h_1,\beta)^{-d_1}e(h_2,g)^{-d_5}e(h_2,\beta)^{-d_2}(e(g,g)/e(B_4,g))^{-T}$；

2) 验证$T=(B_1\|B_2\|B_3\|B_4\|\bar{U}_1\|\bar{U}_2\|\bar{U}_3\|\bar{U}_4\|h(i))$是否成立；

3) 验证$U=e(\varepsilon,g)e(k_u,T)^h$是否成立，如果成立则接受签名，如果不成立则拒绝签名。

4 安全性分析

4.1 正确性分析

1) 密钥生成阶段正确性分析。

根据双线性映射的性质，可以得到如下的推导过程：

$$e(\sigma,ku\cdot g_1^{g1^d}\cdot K_s^{\,r})=e((g_2^{\,M})^{\frac{1}{x+g1^d+sr}},g_1^{\,x+g1^d+sr})$$

$$=e((g_2^{\,M})^{\frac{x+g1^d+sr}{x+g1^d+sr}},g_1)=e(g_2^{\,M},g_1)$$

所以密钥生成阶段的验证过程是正确的。

2) 签名过程的正确性分析。根据双线性映射的性质，签名过程的推导如下所示：

$$U=e(\varepsilon,g_1)e(k_u,eT)^h=e(yg_1-hxT,g_1)e(g_1^{\,x},T)^h$$

$$=e(dg_1-hxT,g_1)e(g_1,xTh)=e(dg_1,g_1)=I^d$$

所以签名过程是正确的。

4.2 安全性阶段分析

首先构造一个敌手 A，假设 A 可以解决计算性 Diffie-Hellman 假设，然后构造一个多项式复杂度的算法 F，F 把敌手 A 作为子程序，A 想通过与 F 交互后冒充某个诚实的客户端，F 已知一个 CDHP 三元组g,g^a,g^b，记为$(g,g^a,g^b)\in G_1$，F 的目的是求g^{ab}，即解决 CDH 问题。F 与敌手 A 之间的两阶段交互过程描述如下：F 运行系统参数建立算法，令$A=g_2^s$(F 不知系统私钥)，将系统参数给 A，然后开始交互过程。

4.2.1 密钥分发阶段

1) F 拥有一个列表 H 可以供敌手查询，A 将进行基于$(ID_1,ID_2,\cdots,ID_i,\cdots,ID_n)$公钥提取查询。F 根据 A 提供的$ID_i$首先会查询查列表 H，若列表中没有$ID_i$，则 F 将随机选择$a_i,b_i\in {}_RZ_p^*$，计算$R_i=g_1^{a_i}$，然后 F 将进行掷硬币操作，把掷硬币的结果记做$D$，设$Pr(D=0)=\varepsilon$，则$Pr(D=1)=1-\varepsilon$，如果$D=0$，则计算$g_2^{b_i}$，定义$Pk_u=g_2^{b_i}$，然后将其返回给 A；如果$D=1$，则返回$\perp$，最后 F 将$(ID_i,R_i,D,a_i,b_i,k_{ui})$添加到列表 H 中去。如果$ID_i$已经在列表 H 中，那么查找 H 中对应的$M_i$返回给 A。

2) A 将进行基于$(ID_1,ID_2,\cdots,ID_i,\cdots,ID_n)$私钥提取查询。F 根据 A 提供的$ID_j$首先会查询查列表 H，若列表上没有$ID_j$，将回到第一阶段 1）中。否则 F 查找列表中$ID_j$对应的$D$的值，如果$D=0$，选择$c\in {}_RZ_p^*$，计算$d=A^c$，然后将$(b_i,d)$返回给$A$，并且将$b_i$、$d$添加到列表 H 中；如果$D=1$，则因 F 无法生成满足验证等式的部分私钥，则输出$\perp$表示放弃。

4.2.2 签名阶段

敌手 A 首先选择一个在私钥提取查询中没有查询过的身份ID，而这个ID是敌手 A 想要冒充的客用户，然后 A 通过和 F 进行交互，成功地冒充了身份为ID的证明者。敌手 A 首先提取记录(ID,PK,D,a,b,c,R,y)，由于敌手 A 冒充成功，那么公式$U=e(\varepsilon,g)e(PK,T)^h$成立。接下来 F 查询$D$的值，如果$D=0$，F 输出$\perp$放弃；如果$D=1$，则敌手 A 计算$e(\varepsilon,g)e(k_u,T)^h$，而根据双线性映射的性质可以得出$U=e(\varepsilon,g)e(k_u,T)^h$，如果$g^c=g^d$说明伪造成功，那么说明 A 成功的找到了计算性离散对数复杂问题的解，这在多项式计算能力内是不可能的，计算$g^c=g^d$等同于暴力猜解，综上所述敌手 A 伪造证明者的身份的概率是可忽略的，因此本文提出的方案是安全的。

4.3 计算效率仿真

下面将使用 Matlab 对本文方案和文献[12,13]

进行试验仿真，从计算复杂性方面进行比较，结果总结如图 1 所示。本文的实验参数如表 1 所示。

设在一个区域网络内有 10 000 个实体，证明者每隔 100 min 要像这 10 000 个实体中随机的 100 个实体进行签名，通过本文方案和文献[12,13]的方案对不同长度消息进行签名所花费的时间，对比方案的计算复杂性，图 1 表明在面对短消息签名时本文方案和文献[12,13]方案的对比，短消息指的是签名信息小于 1 Mbit。

表 1　　仿真参数

参数	初始值		参数解释
网络环境	N	10 000	网络总的实体数量
参数	M	100	每次签名者的数量
算法参数	*time*	1 000 min	系统运行时间

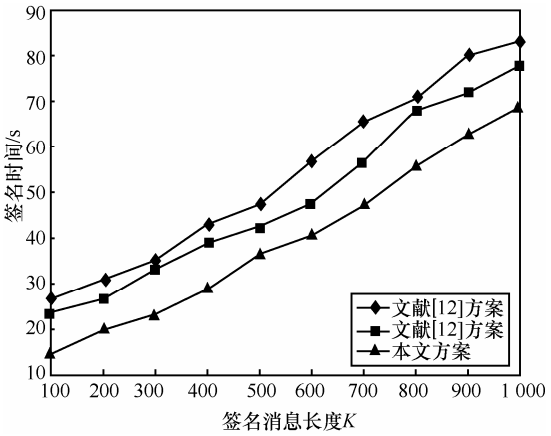

图 1　短消息签名时间对比

图 2 表明在面对较长消息签名时，本文方案和文献[12,13]方案的对比，长消息指的是签名信息大于 1 Mbit 的消息。

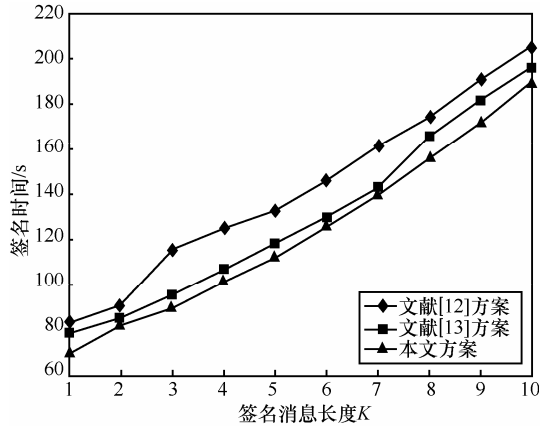

图 2　长消息签名时间对比

从图 1 和图 2 可以看出，根据时间比率可以看出本文提出的方案在计算时间上明显优于文献[12,13]中的方案，而且对长消息签名和短消息签名，本文方案都有较高的计算效率。

5　结束语

本文提出了一种基于 TPCM 的盲签名方案，该方案采用 SDC 和 TPCM 合作生成用户的身份密钥，该方案使盲签名更加容易生成，该方案采用无证书公钥密码体制生成私钥，避免了公钥证书的撤销以及密钥托管问题，保证了实现匿名证明和防止用户的密钥泄露，具有较高的安全性，而且本文方案具有较高的计算效率。

参考文献：

[1] HAMIR A. Identity-based cryptosystems and signature schemes[A]. Blakely Proc Of Crypto'84，LNCS 196[C]. Berlin: Springer-Verlag, Germany, 1984.47-53.

[2] BE M, FUJISAKI E. How to date blind signatures[A]. Proc of ASIACRYPT[C]. London: Spring-Verlag, UK, 1996.244-251.

[3] RIYARNI S, PATERSOA K. Certificate less public key cryptograph[A]. Proc of Asia CRYPT[C]. Berlin: Springer Verlag, Germany, 2003. 452-473.

[4] HEN X F, ZHANG F G, KONIDALA D M, *et al*. New ID-based threshold signature scheme from Weil pairing[A]. INDO_CRYPT2004. LNCS 3348[C]. Berlin: Springer-Verlag, Germany ,2004.371-383.

[5] BESSIE C H, WONG D S, ZHANG Z F, *et al*. Certifieateless signature: a new security model and an improved generic construction[J]. Designs, Codes and Cryptography, 2007, 42(2): 109-126.

[6] HOI K Y, PARK J H, HWANQ J Y, *et al*. Efficient cerificateless signature schemes[A]. Proc of the 5th International Conference on Applied Cryptography and Network Security[C]. Berlin: Springer-Verlag, Germany, 2007. 443-458.

[7] 陆洪文, 郑卓. 基于双线性对的门限部分盲签名方案[J]. 计算机应用, 2005, 25(9):2057-2059.
LU H W, ZHENG Z. Threshold bilinear pairings partially blind signature scheme[J]. Computer Applications, 2005, 25(9):2057-2059.

[8] IOVANNI D C, GONZALO A, RENWEI G. Threshold cryptography in mobile ad hoc networks[A]. SCN 2004[C]. Berlin, Heidelberg, NewYork: Springer-Verlag, 2005. 91-104.

[9] ABE M, FUJISAKI E. How to date blind signatures[A]. Advances inCryptology-AisaCrypt'96[C]. Heidelberg: Springer-Verlag, Germany, 1996.244-251.

[10] ZHANG F, SAFAVI N R, SUSILO W. Efficient verifiably encrypted

signature and partially blind signature from bilinear pairings[A]. Cryptology-Indocrypt 2003, 4th International Conference on Cryptology[C]. Heidelberg: Springer-Verlag, Germany, 2003. 71-84.

[11] OKAMOTO T. Efficient blind and partially blind signatures without-random oracles[A]. Third Theory of Cryptography Conference, TCC 2006[C]. Heidelberg: Springer-Verlag, Germany, 2006. 80-99.

[12] ZHANG F, KIM K. Efficient ID-based blind signature and proxy signature from bilinear pairings[A]. 8th Australasian Conference on Information Security and Privacy[C]. Wollongong, Australia, 2003. 312-323.

[13] CHEN X, ZHANG F, LIU S. ID-based restrictive partially blind signaturesand applications[J]. Journal of System and Software, 2007, 80(2):164-171.

[14] CHOW S, HUI L, YIU S, *et al*. Two improved partially blind signature schemes from bilinear pairings[A]. 10th Australian Conference on Information Security and Privacy[C]. Heidelberg: Springer-Verlag, 2005. 316-328.

[15] HU X, HUANG S. An efficient id-based partially blind signature scheme[A]. IEEE Eighth International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing[C]. Qingdao, China, 2007. 291-296.

作者简介：

黄文廷（1981），男，江苏徐州人，国家计算机网络应急技术处理协调中心工程师，主要研究方向为网络安全、计算机通信等。

佟玲玲（1985-），女，辽宁阜新人，博士，国家计算机网络应急技术处理协调中心工程师，主要研究方向为多媒体内容分析与安全及视频编解码等。

王永建[通信作者]（1977-），男，河南郸城人，博士，国家计算机网络应急技术处理协调中心副研究员，主要研究方向为物联网技术及安全、通信网技术及安全等。E-mail: wyj@cert.org.cn。