Journal of Computer Applications
计算机应用,2012,32(3):699-704,728
ISSN 1001-9081
CODEN JYIIDU
2012-03-01
http://www.joca.cn

文章编号:1001-9081(2012)03-0699-06
doi:10.3724/SP.J.1087.2012.00699

具有分布式打开权威的隐藏身份签名方案

柳 欣[1,2*]

(1.山东青年政治学院 信息工程学院,济南 250014; 2.山东大学 计算机科学与技术学院,济南 250101)

(*通信作者电子邮箱 lxonne@163.com)

摘 要:基于双线性映射的隐藏身份签名方案不满足可开脱性和选择密文攻击(CCA)匿名性,而在RSA群上构造的隐藏身份签名方案具有较高的通信和运算耗费。为此,利用块消息签名技术实现了可开脱性,提出一个允许设置分布式打开权威的改进方案。改进方案通过将分布式密钥提取和可同时执行的知识证明技术应用于底层门限加密方案,有效地实现了对打开权威的权利分发。此外,为了克服传统串行注册方式无法抵抗拒绝服务攻击的不足,利用承诺的知识证明技术将注册过程增强为满足并发安全性的协议。在随机预言模型下,改进方案可证满足所要求的所有安全性质。对比实验结果表明:改进方案的签名长度更短,签名与验证算法开销更小,由可信服务器执行的门限解密过程是并发安全的且在自适应攻击者模型下满足可证安全性。

关键词:数字签名;群签名;基于身份的签名;知识证明;门限加密;自适应安全性

中图分类号:TP309.7 **文献标志码**:A

Hidden identity-based signature scheme with distributed open authorities

LIU Xin[1,2*]

(1. *School of Information Engineering, Shandong Youth University of Political Science, Jinan Shandong 250014, China*;
2. *School of Computer Science and Technology, Shandong University, Jinan Shandong 250101, China*)

Abstract: Hidden identity-based signature schemes from bilinear maps do not achieve exculpability and Chosen-Ciphertext Attack (CCA) anonymity, while schemes of this type built on RSA groups suffer from significant communication and computation overheads. Concerning this situation, an improved scheme with distributed open authorities was put forward, which satisfied exculpability by making use of the block messages signature. It achieved efficient distribution of the open authority by applying distributed key extraction and simultaneous proof of knowledge to the underlying threshold encryption scheme. Furthermore, to cope with the shortcomings of traditional serial registration, i.e., being vulnerable to the denial-of-service attack, its registration protocol was enhanced to be concurrent-secure by using the method of committed proof of knowledge. In the random oracle model, the proposed scheme could be proved to fulfill all the required properties. Performance comparison shows that the resultant signature is shorter and the algorithms (i.e., Sign and Verify) are more efficient. Moreover, the process of threshold decryption by trusted servers is proved to be concurrently-secure and it is also immune to adaptive adversaries.

Key words: digital signature; group signature; identity-based signature; knowledge proof; threshold encryption; adaptive security

0 引言

群签名方案[1]1,[2]427,[3]的设计目标是向签名者提供可撤销的匿名性,且签名者有能力代表群体进行签名。在群签名方案中,通常设置两个管理员,其中群管理员(Group Manager, GM)负责加入新的成员,打开权威(Open Authority, OA)负责在发生争议时撤销原始签名者的匿名性。在2007年,Kiayias与Zhou[4]136,[5]3提出了所谓的隐藏身份签名(Hidden identity-Based Signature, Hidden-IBS)方案,并且指出此类方案特别适合于在匿名路由系统中提供可仲裁的匿名性。与普通的群签名方案相比,Hidden-IBS方案具备以下的独特性质,即:OA可以在不借助身份管理员(Identity Manager, IM)的条件下独立地打开争议签名。此外,由于Hidden-IBS方案对用户的IP地址与真实身份进行了绑定,因此一旦用户滥用自己的匿名性,OA可以将其身份(即IP地址)提供给匿名路由系统的运营商,而后者将在此后拒绝来自该IP地址的数据包。

为了具体实现Hidden-IBS方案,Kiayias与Zhou[4]140-142,[5]7-9提出了基于双线性群的方案(简称KZ-Ⅰ方案)。该方案效率较高,且所得签名仅为约570字节。此外,由于注册协议采用了"单一消息以及签名回应"的2轮交互过程,因而直接满足并发加入的理想性质[6]。然而,KZ-Ⅰ方案的缺点是仅实现了较弱的CPA(Chosen-Plaintext Attack)匿名性(即可抵抗选择明文攻击的匿名性,该性质要求在安全性证明中不允许攻击者访问Open预言机),且未能实现可开脱性(即必须假设IM保持诚实),因而严重影响了其实用性。尽管Kiayias与Zhou[5]14-15随后追加了一个声称能实现CCA(Chosen-Ciphertext Attack)匿名性(即可抵抗选择密文攻击的匿名性)和可开脱性的方案(简称KZ-Ⅱ方案),但KZ-Ⅱ方案是在RSA类型的群上实现的,整体效率不高且并未提供

收稿日期:2011-08-23;**修回日期**:2011-11-09。 **基金项目**:山东省高等学校科技计划项目(J11LG29)。

作者简介:柳欣(1978-),男,山东广饶人,讲师,博士研究生,CCF会员,主要研究方向:信息安全、密码学。

安全性证明。此外,Kiayias 与 Zhou 指出,可以在实际的 Hidden-IBS 系统中设置分布式的 OA,但未能提供具体的方案。最近,Zhou 与 Lin[1]13-14 以及 Boyen 与 Waters[2]432-433 分别提出了同样支持 OA 独立地打开争议群签名的方案(以下分别简称 Zhou-Lin 方案和 Boyen-Waters 方案),因此可以将它们归入 Hidden-IBS 的范畴。然而,Zhou-Lin 方案的缺点是不支持并发加入且所得签名太长。Boyen-Waters 方案同样不支持并发加入而且仅实现了较弱的安全性质(即仅满足 CPA 匿名性且未能实现可开脱性)。尽管 Boyen-Waters 方案是在标准模型下构造的,但该方案并不实用,这体现在所得签名的长度以及验证过程要求执行的对运算次数均与群成员数量的对数呈线性关系。

综上,Hidden-IBS 方案[1]13-14,[2]432-433,[4]140-142,[5]7-9,13-14 并不完全令人满意,即尚未提出能同时满足以下性质的方案:1)在双线性群上构造,具有较高的效率且满足 CCA 匿名性与可开脱性;2)允许设置分布式的 OA,即由分布式的可信服务器执行签名的打开算法;3)保持原始方案[4]141 的并发加入性质,从而能有效防止互联网环境下的拒绝服务攻击[7]62。

本文提出一个基于双线性群的改进方案,新方案的设计思路与特点如下:1)在 KZ-Ⅰ方案中,IM 借助 Boneh-Boyen 签名方案[8]为用户颁发成员证书,但 Boneh-Boyen 方案具有难以对涉及消息的操作与涉及签名私钥的操作进行分离的弱点,因此不易于实现可开脱性。本文方案使用块消息签名[7]49-51 技术克服了这个弱点。2)为了实现分布式的 OA,本文方案将 CCA 安全的 Shoup-Gennaro 门限加密方案[9]作为重要的底层模块。最近,Kiayias 等[10]62-68 提出了基于多服务器协议的 Shoup-Gennaro 门限解密方法。然而,该协议的缺点是解密服务器必须以顺序方式执行且要求做出仅存在静态攻击者的较强假设。本文方案利用 Lysyanskaya[11]3-5,10-11 的技术对 Kiayias 等的方法进行了增强,使得解密服务器可以以并发方式执行且允许存在更强的自适应攻击者[12]。3)通过引入承诺的证明技术[11],实现了并发安全的成员注册协议。4)在随机预言模型下改进方案可证满足 Kiayias 等[4]138-140,[5]5-7,13-14 要求的最强安全性质。

1 预备知识

1.1 Pedersen 陷门承诺方案

公共输入 1)(G_q,g,h),其中,G_q 为素数 q 阶循环群,使得该群上的离散对数问题是难解的;g 与 h 为群 G_q 的生成元,使得 g 与 h 相互间的离散对数是未知的。2)抗碰撞的散列函数 $H:\{0,1\}^* \rightarrow \mathbf{Z}_q^*$。

承诺 为了对秘密元素 x 进行承诺,承诺者选取 $r \in_R \mathbf{Z}_q$,向验证者发送 $c = g^{H(x)}h^r$。

打开承诺 承诺者向验证者发送 x 与 r,后者验证是否满足 $c = g^{H(x)}h^r$。

文献[11]指出,若 $\sigma = \log_g h$ 为承诺者所掌握,则上述方案就构成了陷门承诺方案。

1.2 3 轮诚实验证者的公开抛币零知识的知识证明系统

3 轮诚实验证者的公开抛币零知识的知识证明(Three-round Honest-verifier Public-coin Zero-knowledge Proof of knowledge, THPZP)系统[13]是由多项式时间算法对(P,V)定义的,其中 $P = (P_1,P_2)$。THPZP 系统的公共输入为 Pedersen 承诺方案实例(G_q,g,h)以及元素 $x \in_R G_q$。证明者的输入为证据 w,使得$(w,x) \in R$(R 表示多项式时间可计算的关系)以及随机数 $r \in_R \mathbf{Z}_q$。THPZP 系统的具体执行过程如下:

1)证明者计算 $m_1 = P_1(x,w,r)$,并向验证者发送 m_1;

2)验证者产生随机硬币 $\bar{R} \in_R \mathbf{Z}_q$,并返回 $\bar{R}$ 作为挑战;

3)证明者计算 $m_2 = P_2(x,w,\bar{R},r)$,并向验证者发送 m_2;

4)验证者输出 $Ver(x,m_1,\bar{R},m_2)$ = accept/reject。

1.3 承诺的 THPZP 系统

承诺的 THPZP(Committed THPZP, C-THPZP)系统[11]3-5 是由多项式时间算法对(P,V)定义的,其中 $P = (P_1,P_2)$。C-THPZP 系统的公共输入为 Pedersen 承诺方案实例(G_q,g,h)。证明者的输入为证据 w,使得$(w,x) \in R$,元素 $x \in_R G_q$ 以及随机数 $r \in_R \mathbf{Z}_q$。验证者的目标是获得 x 并且判断证明者是否掌握证据 w,使得$(w,x) \in R$。C-THPZP 系统的具体执行过程如下:

1)证明者计算 $m_1 = P_1(x,w,r)$,选取随机数 $r_1 \in_R \mathbf{Z}_q$,并向验证者发送 $M_1 = g^{H(x,m_1)}h^{r_1}$。

2)验证者产生随机硬币 $\bar{R} \in_R \mathbf{Z}_q$,并返回 $\bar{R}$ 作为挑战。

3)证明者计算 $m_2 = P_2(x,w,\bar{R},r)$,选取随机数 $r_2 \in_R \mathbf{Z}_q$,并向验证者发送 $M_2 = g^{H(m_2)}h^{r_2}$,同时删除 w。

4)证明者向验证者发送(x,m_1,m_2,r_1,r_2),验证者输出 accept 仅当以下 3 个条件同时得到满足:$M_1 = g^{H(x,m_1)}h^{r_1}$,$M_2 = g^{H(m_2)}h^{r_2}$,$Ver(x,m_1,\bar{R},m_2)$ = accept。

1.4 同时证明 THPZP 系统

同时证明 THPZP(Simultaneous Proof THPZP, SP-THPZP)系统[13]是由多项式时间算法 $P_1,P_2,\cdots,P_n$ 定义的,其中 $P_i = (P_{i,1},P_{i,2}),i = 1,2,\cdots,n$。SP-THPZP 系统的公共输入为 Pedersen 承诺方案实例(G_q,g,h)以及元素 $x_1,x_2,\cdots,x_n \in_R G_q$。证明者 P_i 的输入为证据 w_i,使得$(w_i,x_i) \in R$,以及随机数 $r_i \in_R \mathbf{Z}_q$。SP-THPZP 系统的具体执行过程如下:

1)对于 $i = 1,2,\cdots,n$,每个证明者 P_i 广播 $m_{i,1} = P_{i,1}(x_i,w_i,r_i)$。

2)$P_1,P_2,\cdots,P_n$ 共同执行分布式抛币协议[11]10-11,从而产生随机硬币 $\bar{R}$。

3)对于 $i = 1,2,\cdots,n$,每个证明者 P_i 广播 $m_{i,2} = P_{i,2}(x_i,w_i,\bar{R},r_i)$,同时验证是否满足 $Ver(x_j,m_{j,1},\bar{R},m_{j,2})$ = accept,$j \in \{1,2,\cdots,n\}, j \neq i$。若存在 $j \in \{1,2,\cdots,n\}, j \neq i$,使得 $Ver(x_j,m_{j,1},\bar{R},m_{j,2})$ = refuse,则将 P_j 从诚实证明者集合 *Qual* 中删除。

1.5 知识签名

知识签名[14](Signatures of Knowledge, SK)协议可视为 THPZP 系统的非交互版本,即利用抗碰撞的散列函数产生随机硬币 $\bar{R}$,从而消除了 THPZP 系统中的交互过程。

1.6 基于离散对数的分布式密钥产生协议

文献[15]提出一个适用于离散对数密码系统的分布式密钥产生协议(Distributed Key Generation in DLog-based protocol, DL-DKG)。DL-DKG 协议是由多项式时间算法 $P_1,P_2,\cdots,P_n$ 定义的。DL-DKG 协议的公共输入为 Pedersen 承诺方案实例(G_q,g,h)。DL-DKG 协议的具体执行过程如下:

1)每个参与方 P_i 选取度数为 t 的秘密多项式 $f_{a_i}(z) = \sum_{k=0}^{t} c_{ik}z^k$,$f_{\hat{a}_i}(z) = \sum_{k=0}^{t} \hat{c}_{ik}z^k$。对于 $k = 0,1,\cdots,t$,P_i 广播 $C_{ik} =$

$g^{c_{ik}}h^{\hat{c}_{ik}}$,从而定义了验证多项式 $F_{a_i}(z)=\prod_{k=0}^{t}(C_{ik})^{z^k}=g^{f_{a_i}(z)}h^{f_{\hat{a}_i}(z)}$。对于 $j=1,2,\cdots,n$,P_i 向 P_j 发送份额 $\alpha_{ij}=f_{a_i}(j)$,$\hat{\alpha}_{ij}=f_{\hat{a}_i}(j)$。

2) 对于 $i=1,2,\cdots,n$,每个参与方 P_j 检查是否满足 $F_{a_i}(j)=g^{\alpha_{ij}}h^{\hat{\alpha}_{ij}}$。若对于任意的 i 验证失败,则 P_j 广播对 P_i 的控诉。

3) 若 P_j 提出对 P_i 的控诉,则 P_i 广播 $\alpha_{ij},\hat{\alpha}_{ij}$,且每个参与方对此进行验证,若 P_i 无法通过这个测试或接收到超过 t 次的控诉,则将 P_i 从诚实参与方集合 $Qual$ 中删除。

4) 最终,参与方 $P_1,P_2,\cdots,P_n$ 实现了对秘密元素 $a=f_a(0)$ 以及随机数 $\hat{a}=f_{\hat{a}}(0)$ 的共享,其中 $f_a(z)=\sum_{P_i\in Qual}f_{a_i}(z)$ 与 $f_{\hat{a}}(z)=\sum_{P_i\in Qual}f_{\hat{a}_i}(z)$ 分别为关于 a 与 $\hat{a}$ 的秘密共享多项式,且满足验证函数 $F_a(z)=g^{f_a(z)}h^{f_{\hat{a}}(z)}$(注意:$F_a(z)$ 是公开可计算的,即 $F_a(z)=\prod_{P_i\in Qual}\prod_{k=0}^{t}(C_{ik})^{z^k}$)。此外,每个参与方 $P_i\in Qual$ 获得了关于 a 的加法份额 $a_i=f_{a_i}(0)$ 和多项式份额 $\alpha_i=\sum_{P_j\in Qual}\alpha_{ji}$,以及关于 $\hat{a}$ 的加法份额 $\hat{a}_i=f_{\hat{a}_i}(0)$ 和多项式份额 $\hat{\alpha}_i=\sum_{P_j\in Qual}\hat{\alpha}_{ji}$。需要指出的是,$P_i$ 的多项式份额 $\alpha_i,\hat{\alpha}_i$ 满足验证关系 $F_a(i)=g^{f_a(i)}h^{f_{\hat{a}}(i)}=g^{\alpha_i}h^{\hat{\alpha}_i}$。

2　本文方案

本文方案涉及以下的参与方:用户 U、IM 以及由解密服务器 $P_1,P_2,\cdots,P_n$ 构成的分布式 OA。

2.1　公共参考字符串

可信功能性 F_{CRS}^{D} 采用如下方式产生公共参考字符串(Common Reference String, CRS):

1) 选取大素数 $\tilde{p},\tilde{q}$,使得 $\tilde{q}\mid(\tilde{p}-1)$。

2) 采用文献[11]中的技术产生 $G_{\tilde{q}}$ 的生成元 $\tilde{g},\tilde{h}$,使得除了安全性证明中的模拟器之外,任何参与方都不掌握陷门 $\sigma=\log_{\tilde{g}}\tilde{h}$。最后,设置 $CRS=(\tilde{p},\tilde{q},\tilde{g},\tilde{h})$。

2.2　系统建立

1) 产生双线性群参数 $(p,g_0,h_0,G_1,G_2,\psi,G_T,\hat{e})$,满足 $G_1=<g_0>,G_2=<h_0>,\hat{e}:G_1\times G_2\to G_T$,$Ord(G_1)=Ord(G_2)=Ord(G_T)=p,\psi(h_0)=g_0$。选取群 G_2 上的随机生成元 h_1,h_2,h_3,满足 $\psi(h_i)=g_i(i=1,2,3)$,且这些生成元相互间的离散对数是未知的。

2) 选取椭圆曲线群 $\bar{G}=<\bar{g}>$,使得 $Ord(\bar{G})=p$,且要求 DDH(Decisional Diffie-Hellman) 问题在群 $\bar{G}$ 上是困难的[10]70,[16]。

3) 选取抗碰撞的散列函数 $H:\{0,1\}^*\to G_{\tilde{q}},H_1:\{0,1\}^*\to\mathbf{Z}_p,H_2,H_3:\{0,1\}^*\to\bar{G}$。

4) IM 选取 $\gamma\in\mathbf{Z}_p^*$,计算 $w=h_0^{\gamma}$。设置 $pk_{\mathrm{IM}}=w,sk_{\mathrm{IM}}=\gamma$。

5) $P_1,\cdots,P_n$ 执行以下的密钥产生过程:

① 设置 $\bar{g}_1=H_2(\tau),\bar{g}_2=H_3(\tau)$,其中 τ 为某个固定的字符串[10]64。

② 利用生成元 $\bar{g}_1,\bar{g}_2$ 以及度数为 t 的秘密多项式 $f_{x_i}(z)=\sum_{k=0}^{t}c_{ik}z^k$,$f_{\hat{x}_i}(z)=\sum_{k=0}^{t}\hat{c}_{ik}z^k$ 执行 DL-DKG 协议,从而产生共享的解密私钥 x 以及相关的随机数 $\hat{x}$,且 $x,\hat{x}$ 满足可公开计算的验证关系 $F_x(z)=\bar{g}_1^{f_x(z)}\bar{g}_2^{f_{\hat{x}}(z)}$。

③ 参与方 $P_i\in Qual$ 执行Lysyanskaya[11]15 的自适应安全的分布式密钥提取协议。在该协议中,$P_i\in Qual$ 公开 $y_i=\bar{g}_1^{f_{x_i}(0)}$。最终,产生元素 $\bar{H}=\prod_{i\in Qual}y_i=\bar{g}_1^{\sum_{i\in Qual}f_{x_i}(0)}=\bar{g}_1^{x}$。

6) 设置 Hidden-IBS 的公开参数为:

$$pub=(p,g_0,h_0,G_1,G_2,\psi,G_T,\hat{e};\bar{g},\bar{h};g_1,g_2,g_3,h_1,h_2,h_3;H,H_1,H_2,H_3;w;\bar{g},\bar{g}_1,\bar{g}_2,\bar{H})$$

2.3　注册

U 与 IM 执行以下过程:

1) U 秘密选取 $y,s'\in_R\mathbf{Z}_p^*$,产生承诺 $C_y=g_2^{s'}g_3^{y}$。然后,U 与 IM 执行证明 $\pi_1=\text{C-THPZP}\{(s',y):C_y=g_2^{s'}g_3^{y}\}$($\pi_1$ 是通过在 C-THPZP 系统框架下对底层的 THPZP 系统进行编译而得到的。限于篇幅,我们省略了具体的编译过程)。最后,U 将 id 发送给 IM,其中 id 为 U 的 32 位 IP 地址。

2) 若 IM 在证明 π_1 中输出 accept,则选取 $s''\in_R\mathbf{Z}_p^*$,计算 $A=(g_0g_1^{id}g_2^{s''}C_y)^{\frac{1}{e+\gamma}}$,并将 (A,e,s'') 返回给 U。

2.4　注册检查

U 设置 $s=s'+s''\bmod p$,并验证是否满足 $\hat{e}(A,wh_0^{e})=\hat{e}(g_0,h_0)\hat{e}(g_1,h_0)^{id}\hat{e}(g_2,h_0)^{s}\hat{e}(g_3,h_0)^{y}$,若是,则保存 $cert=(A,e,s)$ 作为自己的成员证书。

2.5　签名

给定消息 M,U 产生如下的知识签名:

$$\pi_2=SK\{(r,id,r_1,r_2,e,r_1e,r_2e,s,y):T_1=\bar{g}_1^{r}\wedge T_2=\bar{g}_2^{r}\wedge T_3=\bar{g}^{id}\bar{H}^{r}\wedge A_1=g_1^{r_1}g_2^{r_2}\wedge 1=A_1^{-e}g_1^{r_1e}g_2^{r_2e}\wedge\frac{\hat{e}(A_2,w)}{\hat{e}(g_0,h_0)}=\hat{e}(g_1,h_0)^{id}\hat{e}(g_2,h_0)^{s}\hat{e}(g_3,h_0)^{y}\hat{e}(A_2,h_0)^{-e}\hat{e}(g_2,w)^{r_1}\hat{e}(g_2,h_0)^{r_1e}\}(M)$$

π_2 证明了以下事实:1)(T_1,T_2,T_3) 是关于秘密元素 $\bar{g}^{id}$ 的 Shoup-Gennaro 方案密文。2)U 掌握成员证书 (A,e),满足 $\hat{e}(A,wh_0^{e})=\hat{e}(g_0,h_0)\hat{e}(g_1,h_0)^{id}\hat{e}(g_2,h_0)^{s}\hat{e}(g_3,h_0)^{y}$。3)U 利用随机指数 r_1 将证书元素 A 盲化为 A_2 的形式,且 A_1 是对 r_1 的承诺。π_2 是采用标准技术[1]14 构造的,限于篇幅,省略了具体的构造过程。

2.6　验证

给定消息签名对 (M,π_2),验证者验证 π_2 的有效性。

2.7　打开

给定消息签名对 (M,π_2),服务器 $P_1,P_2,\cdots,P_n$ 执行以下过程:

1) $P_i(i=1,2,\cdots,n)$ 验证 π_2 的有效性。

2) $P_i(i=1,2,\cdots,n)$ 利用生成元 $\bar{g}_1,\bar{g}_2$ 和度数为 t 的秘密多项式执行 DL-DKG 协议,从而产生共享的秘密元素 $a=0$ 和相关的随机数 $\hat{a}=0$。为此,可以采用文献[12]中的技术对 DL-DKG 协议做出如下修改,即在该协议的第 1) 步中,设置 $c_{i0}=\hat{c}_{i0}=0$。同时,要求 p_j 在该协议的第 2) 步中验证是否满足 $C_{i0}=1$。

3) $P_i\in Qual$ 计算 $o_i=T_1^{\chi_i}\bar{g}_1^{\alpha_i}$ 并执行以下步骤的同时证明承诺的 THPZP 证明,即:

$$\pi_3=\text{SP-C-TPHZP}\{(\chi_i,\alpha_i,\hat{\chi}_i,\hat{\alpha}_i):o_i=T_1^{\chi_i}\bar{g}_1^{\alpha_i}\wedge F_x(i)=\bar{g}_1^{\chi_i}\bar{g}_2^{\hat{\chi}_i}\wedge F_a(i)=\bar{g}_1^{\alpha_i}\bar{g}_2^{\hat{\alpha}_i}\}$$

π_3 证明了以下事实:① 承诺 o_i 是采用正确方式产生的。

②P_i 掌握关于共享解密私钥 x 以及相关随机数 $\hat{x}$ 的多项式份额 χ_i 与 $\hat{\chi}_i$，且它们满足验证关系 $F_x(i) = \bar{g}_1^{\chi_i}\bar{g}_2^{\hat{\chi}_i}$。③$P_i$ 掌握关于共享秘密元素 a 以及相关随机数 $\hat{a}$ 的多项式份额 α_i 与 $\hat{\alpha}_i$，且它们满足验证关系 $F_a(i) = \bar{g}_1^{\alpha_i}\bar{g}_2^{\hat{\alpha}_i}$（$\pi_3$ 是通过在 SP-THPZP 系统框架下对底层的 C-THPZP 系统进行编译而得到的。限于篇幅，省略了具体的编译过程）。

4）计算：

$$\frac{T_3}{\prod_{i\in Qual} o_i^{\lambda_{0,i}^{Qual}}} = \frac{T_3}{\prod_{i\in Qual}(T_1^{\chi_i}\bar{g}_1^{\alpha_i})^{\lambda_{0,i}^{Qual}}} = \frac{\bar{g}^{id}\bar{H}^r}{T_1^{\sum_{i\in Qual}\lambda_{0,i}^{Qual}\chi_i}\bar{g}_1^{\sum_{i\in Qual}\lambda_{0,i}^{Qual}\alpha_i}} = \frac{\bar{g}^{id}\bar{H}^r}{T_1^x\bar{g}_1^0} = \frac{\bar{g}^{id}(\bar{g}_1^x)^r}{(\bar{g}_1^x)^r} = \bar{g}^{id}$$

其中：$\lambda_{0,i}^{Qual} = \prod_{j'\in Qual/\{i\}}(-j')/\prod_{j'\in Qual/\{i\}}(i-j')$ 为拉格朗日符号[9]。

5）采用 Pollard 的 rho 方法[4]142,[5]10 根据 $\bar{g}^{id}$ 恢复出 id。

3 本文方案的安全性分析

定理 1 协议 π_1 是并发零知识[17] 的知识证明协议。

并发零知识性质 模拟器 $Sim_{\text{C-THPZP}}$（该算法并不掌握 C_y 的离散对数表达式）与可能为恶意的 IM 共同执行以下的交互过程：

1）$Sim_{\text{C-THPZP}}$ 选取 $r_{M_1} \in_R \mathbf{Z}_{\tilde{q}}$，计算 $M_1 = \bar{g}^{r_{M_1}}$，并且向 IM 发送 M_1。

2）IM 返回挑战 $\bar{R} \in_R \mathbf{Z}_{\tilde{q}}$。

3）$Sim_{\text{C-THPZP}}$ 以 $\bar{R}$ 与 C_y 为输入调用底层 THPZP 系统的模拟器 Sim_{THPZP}，从而获得可接受的 THPZP 证明过程副本 $(m_1, \bar{R}, m_2)$。$Sim_{\text{C-THPZP}}$ 选取 $r_2 \in_R \mathbf{Z}_{\tilde{q}}$，计算 $M_2 = \bar{g}^{H(m_2)}\bar{h}^{r_2}$，并且向 IM 发送 M_2。

4）$Sim_{\text{C-THPZP}}$ 利用陷门 $\sigma = \log_{\bar{g}}\bar{h}$ 和 m_1 打开承诺 M_1，方法是计算 $r_1 = (r_{M_1} - H(C_y, m_1))\sigma^{-1} \bmod \tilde{q}$，并且向 IM 发送 $(C_y, m_1, m_2, r_1, r_2)$。

显然，由 $Sim_{\text{C-THPZP}}$ 产生的协议 π_1 的副本与 IM 在与真实用户的证明过程中所获得的副本是不可分辨的。同时，$Sim_{\text{C-THPZP}}$ 在无需对 IM 执行重绕的条件下完成了上述的模拟过程。因此，协议 π_1 满足并发零知识性。

知识证明性质 根据 C-THPZP 系统的知识证明性质[11]6 可知，存在多项式时间提取器 KE，使得若 U 能以不可忽略的概率使得 IM 在证明过程中接受，则 KE 能在多项式时间内以不可忽略的概率从与 U 的交互过程中提取出证据 (s', y)。

定理 2 协议 π_3 是并发零知识[17] 的知识证明协议，而且在自适应攻击者模型下是安全的。

并发零知识性质 在证明过程中，所有的服务器 $P_1, P_2, \cdots, P_n$ 分别属于两个集合，即 $Control$ 与 $\overline{Control}$。其中，$Control$ 表示由模拟器 $Sim_{\text{SP-C-THPZP}}$ 控制的诚实服务器的集合，$\overline{Control}$ 表示由剩余的服务器构成的集合。$Sim_{\text{SP-C-THPZP}}$ 的模拟过程如下：

1）$Sim_{\text{SP-C-THPZP}}$ 选取 $\bar{R} \in_R \mathbf{Z}_{\tilde{q}}$。对于 $P_i \in Control$，$Sim_{\text{SP-C-THPZP}}$ 以诚实方式产生承诺 $m_{i,1}, M_{i,1}$。对于 $P_{i'} \in \overline{Control}$，$Sim_{\text{SP-C-THPZP}}$ 以 $(o_{i'}, F_x(i'), F_a(i'), \bar{R})$ 为输入调用底层 THPZP 系统的模拟器 Sim_{THPZP}，从而获得可接受的 THPZP 证明过程副本 $(m_{i',1}, \bar{R}, m_{i',2})$。同时，$Sim_{\text{SP-C-THPZP}}$ 选取 $r_{M_{i',1}} \in_R \mathbf{Z}_{\tilde{q}}$，计算 $M_{i',1} = \bar{g}^{r_{M_{i',1}}}$。对于所有的 $P_i (i = 1, 2, \cdots, n)$，$Sim_{\text{SP-C-THPZP}}$ 广播 $M_{i,1}$。

2）$Sim_{\text{SP-C-THPZP}}$ 以 $\bar{R}$ 为输入调用分布式抛币协议[11]12 的模拟器 Sim_{TOSS}。

3）对于 $P_i \in Control$，$Sim_{\text{SP-C-THPZP}}$ 以诚实方式产生 $m_{i,2}$，$M_{i,2}$。对于 $P_{i'} \in \overline{Control}$，$Sim_{\text{SP-C-THPZP}}$ 利用陷门 $\sigma = \log_{\bar{g}}\bar{h}$ 和 $m_{i',1}$ 打开承诺 $M_{i',1}$，方法是计算 $r_{i',1} = (r_{M_{i',1}} - H(o_{i'}, F_x(i'), F_a(i'), m_1))\sigma^{-1} \bmod \tilde{q}$。对于所有的 $P_i (i = 1, 2, \cdots, n)$，$Sim_{\text{SP-C-THPZP}}$ 广播 $M_{i,2}$。同时，$Sim_{\text{SP-C-THPZP}}$ 删除 $P_i \in Control$ 的与 a 相关的秘密信息，但验证函数 $F_a()$ 除外。

4）对于所有的 $P_i (i = 1, 2, \cdots, n)$，$Sim_{\text{SP-C-THPZP}}$ 广播 $(o_i, F_x(i), F_a(i), m_{i,1}, m_{i,2}, r_{i,1}, r_{i,2})$。

显然，由 $Sim_{\text{SP-C-THPZP}}$ 产生的协议 π_3 的副本与自适应攻击者 Adv 在执行真实协议 π_3 的过程中所获的副本是不可分辨的。同时，$Sim_{\text{C-THPZP}}$ 在无需对 Adv 执行重绕的条件下完成了上述的模拟过程。因此，协议 π_3 满足并发零知识性。

知识证明性质 协议 π_3 是在 SP-THPZP 系统框架下对底层的 C-THPZP 系统进行编译而得到的。根据 C-THPZP 系统的知识证明性质，可以得出协议 π_3 满足知识证明性质。

抵抗自适应攻击者的安全性 根据底层的 C-THPZP 系统的抵抗自适应攻击者的安全性[11]7 可知，无论 Adv 在任何时刻攻破由自己选取的某台服务器，$Sim_{\text{SP-C-THPZP}}$ 都能为 Adv 提供该服务器的内部状态，且该状态与 Adv 在此前的观察结果相一致。

定理 3 在随机预言模型和公共参考字符串模型下，只要 q-SDH（q-Strong Diffie-Hellman）假设[8]、DDH 假设以及离散对数假设成立，则本文方案满足 Kiayias 等[4]142,[5]5-7,13-14 要求的最强性质，即正确性、不可误验锻造性、CCA 匿名性以及可开脱性。

正确性 容易验证本文方案的注册过程、签名过程以及签名打开过程都是正确的。限于篇幅，我们省略了具体的证明过程。

不可误验锻造性 采用与 Kiayias 等[5]22-24 类似的技术，可以证明，若存在能攻破本文方案不可误验锻造性的攻击者算法 Adv，则能构造可攻破 q-SDH 假设或离散对数假设的算法 B。B 的运行过程如下：

1）B 获得给定的双线性参数 $(p, g_0, h_0, G_1, G_2, \psi, G_T, \hat{e})$ 以及块消息签名方案[7]49-51 的公钥 $(g_1, g_2, g_3, h_1, h_2, h_3, w)$。$B$ 执行系统建立算法产生剩余的参数，并向 Adv 提供 pub。

2）B 与 Adv 共同执行以下的不可误验锻造性游戏，并且在游戏中回答 Adv 提出的预言询问。该游戏的运行过程分为以下两个模式。

模式 1

$H_1(\cdot)$：B 维护表格 H_1。若询问属于 H_1，B 直接返回对应的值；否则，B 选取 Z_p 中的随机元素，将其保存至 H_1 并返回给 Adv。

$H_2(\cdot), H_3(\cdot)$：模拟方法与 $H_1(\cdot)$ 类似。

$CorruptOA(\cdot)$：B 将 $sk_{\text{OA}} = (x_1, x_2, \cdots, x_n)$ 提供给 Adv。

Reg(·):*Adv* 向 *B* 发送($C_{i,y}$,id_i),并与 *B* 执行证明 $\pi_{i,1}$,*B* 利用 $\pi_{i,1}$ 的知识提取器提取出秘密证据(s'_i,y_i)。*B* 将(s'_i,y_i)提交给底层的块消息签名预言机[7]49-51,并获得返回的(A_i,e_i,s''_i)。*B* 向 *Adv* 返回 1,并且保存(id_i,y_i;A_i,e_i,$s_i = s'_i + s''_i$)。

CurruptUser(·):若 *Adv* 提供的 id_i 为注册用户,则 *B* 将(A_i,e_i,s_i)提供给 *Adv*。

Sign(·):若 *Adv* 要求获得身份为 *id* 的用户对消息 *M* 的签名且 *id* 为诚实用户,*B* 采用本文方案签名算法中的方式为 *Adv* 提供签名 π_2。

在概率 ε_1 下,*Adv* 最终输出消息签名对($\bar{M}$,$\bar{\pi}_2$),且 $\bar{\pi}_2$ 在打开后能指向用户身份 $\overline{id} \notin \{id_1, id_2, \cdots, id_q\}$,其中 *q* 表示 *Adv* 的询问次数上界,则根据推广的分叉引理[1]21,*B* 可以通过对 *Adv* 执行重绕而提取出秘密证据($\bar{y}$,$\bar{e}$,$\bar{s}$,$\bar{r}_1$),并计算出 $\bar{A} = A_2 g_2^{-\bar{r}_1}$。现在,*B* 获得了 *Adv* 对元组($\overline{id}$,$\bar{s}$,$\bar{y}$)的伪造块消息签名方案[7]49-51 签名($\bar{A}$,$\bar{e}$)。根据 Au[7]52的结论,此时可以得出与 q-SDH 假设或离散对数假设间的矛盾。此外,在概率 ε_2 下,*B* 在模式 1 下运行失败。此时,*Adv* 输出消息签名对($\bar{M}$,$\bar{\pi}_2$),$\bar{\pi}_2$ 在打开后能指向用户身份 $\overline{id} \notin \{id_1, \cdots, id_q\}$,且 *Adv* 并未提出关于该用户的 *CurruptUser*(·) 询问以及要求获得该用户对消息 $\bar{M}$ 进行签名的 *Sign*(·) 询问。这表明 *B* 无法借助 *Adv* 获得伪造的块消息签名,然而概率 ε_2 是可忽略的。

模式 2

H_1(·),H_2(·),H_3(·),*CorruptOA*(·):同模式 1。

Reg(·): *Adv* 向 *B* 发送($C_{i,y}$,id_i) 并与 *B* 执行证明 $\pi_{i,1}$,*B* 利用 $\pi_{i,1}$ 的知识提取器提取出秘密证据(s'_i,y_i)。*B* 将 1 返回给 *Adv*,同时保存(id_i,y_i; -, -, -),其中"-"表示未知元素。

CurruptUser(·):若 *Adv* 提供的 id_i 为注册用户,*B* 采用模式 1 下 *Reg*(·) 询问中的方式模拟产生用户 id_i 的成员证书(A_i,e_i,s_i),并将其提供给 *Adv*。

Sign(·):若 *Adv* 要求获得身份为 *id* 的用户对消息 *M* 的签名且 *id* 为诚实用户,*B* 在不掌握用户 *id* 成员证书的条件下为 *Adv* 提供模拟产生的签名 π_2。

在概率 ε_3 下,*Adv* 最终能输出消息签名对($\bar{M}$,$\bar{\pi}_2$),且 $\bar{\pi}_2$ 在打开后能指向诚实用户身份 $\overline{id} \in \{id_1, \cdots, id_q\}$,且 *Adv* 并未提出关于该用户的 *CurruptUser*(·) 询问以及要求获得该用户对消息 $\bar{M}$ 进行签名的 *Sign*(·) 询问,则与模式 1 类似,*B* 可以提取出证据($\bar{y}$,$\bar{e}$,$\bar{s}$,$\bar{r}_1$),并计算出 $\bar{A} = A_2 g_2^{-\bar{r}_1}$。现在,*B* 获得了 *Adv* 对元组($\overline{id}$,$\bar{s}$,$\bar{y}$) 的伪造块消息方案签名($\bar{A}$,$\bar{e}$)。采用与模式 1 类似的分析方法,可以得出与 q-SDH 假设或离散对数假设的矛盾。

总之,通过在模式 1 与模式 2 之间做出随机选择,*B* 能以约($\varepsilon_1 + \varepsilon_3$)/2 的概率攻破 q-SDH 假设或离散对数假设。

CCA 匿名性　可以证明,若存在能攻破本文方案 CCA 匿名性的攻击者算法 *Adv*,则能构造可攻破 DDH 假设的算法 *B*。*B* 的运行过程如下:

1)*B* 获得给定的双线性群参数(p,g_0,h_0,G_1,G_2,ψ,G_T,$\hat{e}$)以及 Shoup-Gennaro 方案的公钥($\bar{g}$,$\bar{g}_1$,$\bar{g}_2$,$\bar{H}$)。*B* 执行系统建立算法产生剩余的参数,并向 *Adv* 提供 *pub*。

2)*B* 与 *Adv* 共同执行以下的 CCA 匿名性游戏,并且在游戏中回答 *Adv* 提出的预言询问。

H_1(·),H_2(·),H_3(·):同上。

Open(·):若 *Adv* 提出询问(M,π_2),*B* 首先验证 π_2 的有效性。若是,*B* 从 π_2 中提取出密文部分(T_1,T_2,T_3),并将其提供给底层的 Shoup-Gennaro 方案解密预言机,从而获得返回的 $\bar{g}^{id}$。*B* 为 *Adv* 提供以 $\bar{g}^{id}$ 为输出的分布式解密协议的模拟过程。显然,在该过程结束后,*Adv* 能根据 $\bar{g}^{id}$ 恢复出 *id*。

CorruptIM(·):*B* 将 $sk_{IM} = \gamma$ 提供给 *Adv*。

3) 若 *Adv* 输出(M,id_0,id_1) 并要求获得挑战签名,*B* 将 $\bar{g}^{id_0}$,$\bar{g}^{id_1}$ 提供给 Shoup-Gennaro 方案的挑战者,并获得返回的对 $\bar{g}^{id_b}$(其中 $b \in_R \{0,1\}$) 的加密结果(T_1,T_2,T_3)。然后,*B* 模拟产生 π_2^*,并将 $challenge = \pi_2^*$ 提供给 *Adv*。

4)*B* 继续回答 *Adv* 的预言询问 H_1(·),H_2(·),*Open*(·),但 *Adv* 不允许提出关于挑战签名 *challenge* 的 *Open* 询问。最终,*Adv* 输出对 *b* 的猜测结果 *b'*,*B* 将 *b'* 作为自己对 Shoup-Gennaro 方案挑战者的回答。

显然,若 *Adv* 能做出正确的猜测,则 *B* 能以几乎相同的概率攻破 Shoup-Gennaro 方案的 CCA 安全性,即得出了与 Shoup-Gennaro 方案的底层 DDH 假设间的矛盾。

可开脱性　采用与文献[18]类似的技术,可以证明,若存在能攻破本文方案可开脱性的攻击者算法 *Adv*,则能构造可攻破离散对数假设的算法 *B*。*B* 的运行过程如下:

1)*B* 获得给定的离散对数问题实例(h_3,h_3^*) = (h_3,h_3^μ) $\in G_2$。*B* 选取 $\mu \in_R \mathbf{Z}_p^*$,设置 $h_2 = h_3^{\mu^{-1}}$,并且定义 $g_2 = \psi(h_2)$,$g_3 = \psi(h_3)$。*B* 执行系统建立算法产生剩余参数,并向 *Adv* 提供 *pub*。

2) 设 *q* 为群体中的用户数量上界。*B* 选取 $i^* \in_R \{1,2,\cdots,q\}$。*B* 与 *Adv* 执行以下的可开脱性游戏,并且在游戏中回答 *Adv* 提出的预言询问。

H_1(·),H_2(·),H_3(·):同上。

CorruptIM(·),*CorruptOA*(·):*B* 分别将 $sk_{IM} = \gamma$,$sk_{OA} = (x_1, \cdots, x_n)$ 提供给 *Adv*。

Reg(·):若 $i \neq i^*$,则 *B* 以诚实用户 id_i 的身份与 *Adv* 共同执行注册协议,即 *B* 自行选取成员秘密 $y_i, s'_i \in_R \mathbf{Z}_p^*$,并最终获得 *Adv* 提供的成员证书($A_i$,$e_i$,$s_i$)。若 $i = i^*$,则 *B* 选取 $s'_{i^*} \in_R \mathbf{Z}_p^*$,计算 $C_{y_{i^*}} = g_2^{s'_{i^*}} \psi(h_3^*) = g_2^{s'_{i^*}} g_3^z$,其中 *z* 为未知元素。随后,*B* 在不掌握 *z* 的条件下模拟产生 $\pi_{i^*,1}$,向 *Adv* 发送($\pi_{i^*,1}$,id_{i^*}),并且获得后者提供的成员证书(A_{i^*},e_{i^*},s_{i^*})。

Sign(·):当 *Adv* 要求获得用户 id_i 对消息 *m* 的签名,若满足 $i \neq i^*$,则 *B* 采用本文方案的签名算法为 *Adv* 产生签名 π_2。若满足 $i = i^*$,*B* 在不掌握秘密元素 y_{i^*}(即 *z*) 的条件下为 *Adv* 模拟产生这个签名。

CorruptUser(·):若满足 $i \neq i^*$,则 *B* 为 *Adv* 提供成员秘密(y_i,A_i,e_i,s_i)。若满足 $i = i^*$,*B* 向 *Adv* 提供 ⊥ 并终止运行。

3) 最终,若 *Adv* 能成功地陷害某个诚实用户,则 *Adv* 在 1/*q* 的概率下输出用户 id_{i^*} 对消息 *M* 的有效签名 π_2,根据推广的分叉引理[1]21 可知,*B* 可以通过对 *Adv* 执行重绕而从提取出秘密证据 $\bar{y}, \bar{e}, \bar{s}, \bar{r}_1$,从而求出用户 id_{i^*} 的成员证书($\bar{A} = A_2 g_2^{-\bar{r}_1}, \bar{e}, \bar{s}$)。根据块消息签名方案的强不可伪造性质[7]52,可以得出 $(g_0 g_1^{id_{i^*}} g_2^{\bar{s}} g_3^{\bar{y}})^{\frac{1}{\bar{e}+\gamma}} = (g_0 g_1^{id_{i^*}} g_2^{s_{i^*}} g_3^{y_{i^*}})^{\frac{1}{e_{i^*}+\gamma}}$。由于 $g_3 = g_2^\mu$,进而得出 g_2 指数上的关系 $(\bar{s} + \mu\bar{y})(e_{i^*} + \gamma) = (s_{i^*} + \mu z)(\bar{e} + \gamma) \mod p$。显然,*B* 可以据此求出离散对数 *z*。

4 本文方案的性能分析

表 1 为本文方案与前述方案的主要性质比较。通过比较得出,本文方案在所实现的安全性方面具有优势,而且是唯一允许设置分布式 OA 的方案。表 2 为几种方案的签名长度、签名过程与验证过程的运算耗费的比较,其中参数 k' 表示 Boyen-Waters 方案[2]432-433 中群成员数量的对数。为了对签名长度进行估算,采用了如下的参数选取方式。具体地,KZ-Ⅰ方案[4]140-142,[5]7-9 与本文方案都是在素数 p 阶非对称的双线性群对(G_1,G_2)和目标群 G_T 上实现的。此外,本文方案还使用了群 $\bar{G}$。Boyen-Waters 方案是在合数 $\hat{n}$ 阶对称的双线性群对($\hat{G}$,$\hat{G}$)和目标群 $\hat{G}_T$ 上实现的。根据文献[19]的建议,我们选取 $|p|=171$ 比特,且群 G_1,G_2,G_T 上的元素长度约为 172 比特,1 020 比特,1 020 比特。选取 $|\hat{n}|=1024$ 比特,且群 $\hat{G}$,$\hat{G}_T$ 上的元素长度约为 172,1 020 比特。此外,群 $\bar{G}$ 上的元素长度约为 172 比特[16]。Zhou-Lin 方案[1]14 是在 $\mathbf{Z}_{n2}$ 上实现的,我们采用了 Zhou 与 Lin 提供的参数(即 $\varepsilon=1.1$,$l_n=1024$,$\mu_z=1623$,$\mu_x=598$,$l_x=939$,$\mu_e=1965$,$l_e=2339$,$k=160$)。KZ-Ⅱ方案[5]14-15 是在 QR_n,Z_{N^2} 上实现的,我们选取了如下的参数,即 $l_n=l_N=1024$,$\lambda_0=\lambda_1=160$,$u'=1024$,$u''=512$,$l_d=1024$,$l_e=162$,$l_s=1346$(具体含义可以参考 Kiayias 等[5]14-15 的描述)。此外,为了对签名产生与验证过程的运算耗费进行估算,用符号 EXP_G 表示执行 1 次群 G 上的指数(多指数)运算的耗费,用符号 $Pair$ 表示执行 1 次对运算的耗费。此外,在分析对运算次数的过程中,假设采用了预先存储技术[5]10。通过表 2 可看出:在签名长度以及签名产生与验证过程的运算耗费方面,本文方案显著优于 KZ-Ⅰ方案和 Boyen-Waters 方案。尽管 KZ-Ⅱ方案和 Zhou-Lin 方案无需执行代价较高的对运算,但本文方案的签名过程同样具有优势,因为椭圆曲线上的短指数运算在运算速度上明显优于 RSA 类型群上的长指数运算[20]。

表 1 本文方案与其他方案的主要性质比较

方 案	是否支持并发注册	匿名性等级	是否满足可开脱性	OA 的类型
KZ-Ⅰ方案[4-5]	是	CPA	否	集中式
KZ-Ⅱ方案[5]	是	CCA	是	集中式
Zhou-Lin 方案[1]	否	CCA	是	集中式
Boyen-Waters 方案[2]	否	CPA	否	集中式
本文方案	是	CCA	是	分布式

表 2 本文方案与已有方案的性能比较

方 案	签名长度/b	签名产生	签名验证
KZ-Ⅰ方案[4-5]	4 605	$7EXP_{G_1}+6EXP_{G_2}+EXP_{G_T}+2Pair$	$5EXP_{G_1}+4EXP_{G_2}+EXP_{G_T}+2Pair$
KZ-Ⅱ方案[5]	22 270	$7EXP_{QR_n}+6EXP_{Z_{N^2}}$	$4EXP_{QR_n}+3EXP_{Z_{N^2}}$
Zhou-Lin 方案[1]	19 669	$9EXP_{Z_{n2}}$	$5EXP_{Z_{n2}}$
Boyen-Waters 方案[2]	$(2k'+3)\times 172$	$(2k'+3)EXP_{\hat{G}}$	$(2k'+3)Pair$
本文方案	2 570	$4EXP_{G_1}+6EXP_{\bar{G}}+EXP_{G_T}$	$2EXP_{G_1}+EXP_{G_2}+3EXP_{\bar{G}}+EXP_{G_T}+Pair$

此外,与上述方案相比,由于将块消息签名方案[7]49-51 作为底层模块,因此本文方案更易于与短签名的批验证技术[21-22]相结合。具体地,在匿名路由系统中,充当出口点的服务器[4]137 或许在短时间内需要对来自 η 个用户的签名 $\pi_{1,2},\cdots,\pi_{\eta,2}$ 进行验证。此时,即使采用预先存储技术,也需要执行 η 次在线对运算。在应用批验证技术之后,可以将对运算次数降至 2 次。这样不仅减轻了服务器的运算负担,而且降低了系统的数据包丢失率[22]。

5 结语

本文基于门限加密、陷门承诺以及承诺的知识证明等技术提出一个允许设置分布式 OA 的 Hidden-IBS 方案。性能比较表明,新方案在签名长度和运算耗费方面明显优于 Kiayias 等的方案以及 Boyen-Waters 方案。新方案不仅实现了最强的安全性质,而且特别适合于在互联网环境下进行部署,这体现在:1)支持"成员并发加入"的注册协议,克服了传统的串行注册方式无法抵抗拒绝服务攻击的弱点。2)由可信服务器执行的门限解密过程是并发安全的,且在自适应攻击者模型下满足可证安全。此外,通过引入短签名的批验证技术,可以有效地降低验证算法的复杂度。

参考文献:

[1] ZHOU S, LIN D. An interesting member ID-based group signature [EB/OL]. [2011-08-01]. http://eprint.iacr.org/2007/126.

[2] BOYEN X, WATERS B. Compact group signatures without random oracles [C]// EUROCRYPT 2006: Proceedings of the 25th Annual International Cryptology Conference, LNCS 4004. Berlin: Springer-Verlag, 2006: 427-444.

[3] 袁艳,蔡光兴. 新的无随机预言的短群签名方案[J]. 计算机应用,2011,31(3): 790-792.

[4] KIAYIAS A, ZHOU H S. Hidden identity-based signatures [C]// FC 2007: Proceedings of the 11th International Conference on Financial Cryptography and Data Security, LNCS 4886. Berlin: Springer-Verlag, 2007: 134-147.

[5] KIAYIAS A, ZHOU H S. Hidden identity-based signatures [EB/OL]. [2011-08-01]. http://eprint.iacr.org/2007/140.

[6] HAZAY C, KATZ J, KOO C Y, *et al*. Concurrently-secure blind signatures without random oracles or setup assumptions [C]// TCC 2007: Proceedings of the 4th IACR Theory of Cryptography Conference, LNCS 4392. Berlin: Springer-Verlag, 2007: 323-341.

[7] AU M H. Contribution to privacy-preserving cryptographic techniques [D]. Wollongong, Australia: University of Wollongong, 2009.

[8] BONEH D, BOYEN X. Short signatures without random oracles and the SDH assumption in bilinear groups [J]. Journal of Cryptology, 2008, 21(2): 149-177.

[9] SHOUP V, GENNARO R. Securing threshold cryptosystems against chosen ciphertext attack [J]. Journal of Cryptology, 2002, 15(2): 75-96.

(下转第 728 页)

分块效应;变分模型的引入对放大后的图像强加了几何正则性的要求,这就保证了用本文算法放大的图像边缘的光滑性,因而能够重构出高质量的图像。由实验结果可知,本文算法适合处理自然图像及含丰富细节的图像,并且在视觉上可以达到比样条插值更好的放大效果。但是,由于本文算法考虑了图像的全局信息,所以算法复杂度比较高,提高算法速度将是今后需要研究的主要内容。

参考文献:

[1] 朱宁,吴静,王忠谦.图像放大的偏微分方程方法[J].计算机辅助设计与图形学学报,2005,17(9):1941-1945.

[2] 谢美华,王正明.基于边缘定向扩散的图像增强方法[J].光子学报,2005,34(9):1420-1424.

[3] GUICHARD F, MALGOUYRES F. Edge direction preserving image zooming: a mathematical and numerical analysis[J]. SIAM Journal of Numerical Analysis, 2001, 39(1): 1-37.

[4] CHAMBOLLE A. An algorithm for total variation minimization and applications[J]. Journal of Mathematical Imaging and Vision, 2004, 20(1/2): 89-97.

[5] 石澄贤,吴建成,夏德深.各向异性扩散方程和一种图像放大方法[J].南京大学学报:数学半年刊,2005,22(1):153-160.

[6] 郝彬彬,冯象初.一种基于小波和矩阵型扩散的图像放大[J].光子学报,2008,37(11):2365-2368.

[7] 冯象初,姜东焕,徐光宝.基于变分和小波变换的图像放大算法[J].计算机学报,2008,31(2):340-345.

[8] JIANG DONG-HUAN, XU GUANG-BAO. Image zooming based on cartoon and texture decomposition [C]// International Conference on Information Systems and Computational Intelligence. Washington, DC: IEEE Computer Society, 2011:119-122.

[9] BAUDES A, COLL B, MOREL J M. A non-local algorithm for image denoising[C]// IEEE Computer Society Conference on Computer Vision and Pattern Recognition. Washington, DC: IEEE Computer Society, 2005: 60-65.

[10] BAUDES A, COLL B, MOREL J M. On image denoising method [J]. SIAM Multiscale Modeling and Simulation, 2005, 4(2):490-530.

[11] SINGER A, SHKOLNISKY Y, NADLER B. Diffusion interpretation of non-local neighborhood filters for signal denoising[J]. SIAM Journal on Imaging Sciences, 2009, 2(1):118-139.

[12] GILBOA G, OSHER S. Nonlocal linear image regularization and supervised segmentation[J]. SIAM Multiscale Modeling and Simulation, 2007, 6(2): 595-630.

[13] GILBOA G, OSHER S. Nonlocal operators with applications to image processing[J]. SIAM Multiscale Modeling and Simulation, 2008, 7(3):1005-1028.

[14] 孙伟峰,彭玉华.一种改进的非局部平均去噪方法[J].电子学报,2010,38(4):923-928.

[15] 徐大宏,王润生.基于非局部正则化的图像去噪[J].计算机应用研究,2009,26(12):4830-4832.

[16] 王卫卫,韩雨,冯象初.基于非局部扩散的图像去噪[J].光学学报,2010,30(2):373-375.

[17] 吴晓明,陈斌,阮波,等.基于非局部算法的序列图像超分辨率重构[J].计算机应用,2009,29(1):95-96.

[18] GILBOA G, OSHER S. Nonlocal operators with applications to image processing[J]. SIAM Multiscale Modeling and Simulation, 2008, 7(3):1005-1028.

[19] GILBOA G, DARBON J, OSHER S, *et al.* Nonlocal convex functionals for image regularization[R]. [S.l.]: UCLA, 2006.

(上接第 704 页)

[10] KIAYIAS A, XU S, YUNG M. Privacy preserving data mining within anonymous credential systems [C]// SCN 2008: Proceedings of the 6th Conference on Security and Cryptography for Networks, LNCS 5229. Berlin: Springer-Verlag, 2008: 57-76.

[11] LYSYANSKAYA A. Threshold cryptography secure against the adaptive adversary, concurrently [EB/OL]. [2011-08-01]. http://eprint.iacr.org/2000/019.

[12] CANETTI R, GENNARO R, JARECHI S, *et al.* Adaptive security for threshold cryptosystems [C]// CRYPTO 1999: Proceedings of the 19th Annual International Cryptology Conference, LNCS 1666. Berlin: Springer-Verlag, 1999: 98-116.

[13] JARECHI S. Efficient threshold cryptosystems [D]. Cambridge, USA: Massachusetts Institute of Technology, 2001.

[14] FISCHLIN M, ONETE C. Relaxed security notions for signatures of knowledge [C]// ACNS 2011: Proceedings of the 9th International Conference on Applied Cryptography and Network Security, LNCS 6715. Berlin: Springer-Verlag, 2011: 309-326.

[15] GENNARO R, JARECHI S, KRAWCZYK H, *et al.* Secure distributed key generation for discrete-log based cryptosystems [J]. Journal of Cryptology, 2007, 20(1): 51-83.

[16] AU M H, SUSILO W, MU Y. Constant-size dynamic *k*-TAA [EB/OL]. [2011-08-01]. http://eprint.iacr.org/2008/136.

[17] ROSEN A, SHELAT A. Optimistic concurrent zero knowledge [C]// ASIACRYPT 2010: Proceedings of the 16th Annual International Conference on the Theory and Application of Cryptology and Information Security, LNCS 6477. Berlin: Springer-Verlag, 2010: 359-376.

[18] NGUYEN L, SAFAVI-NAINI R. Efficient and provably secure trapdoor-free group signature schemes from bilinear pairings [C]// ASIACRYPT 2004: Proceedings of the 10th Annual International Conference on the Theory and Application of Cryptology and Information Security, LNCS 3329. Berlin: Springer-Verlag, 2004: 372-386.

[19] OHTAKE G, FUJII A, HANAOKA G, *et al.* On the theoretical gap between group signatures with and without unlinkability [C]// AFRICACRYPT 2009: Proceedings of the 2nd African International Conference on Cryptology, LNCS 5580. Berlin: Springer-Verlag, 2009: 149-166.

[20] FISCHLIN M. Communication-efficient non-interactive proofs of knowledge with online extractor [C]// CRYPTO 2005: Proceedings of the 25th Annual International Cryptology Conference, LNCS 3621. Berlin: Springer-Verlag, 2005: 152-168.

[21] FERRARA A L, GREEN M, HOHENBERGER S, *et al.* Practical short signature batch verification [C]// CT-RSA 2009: Proceedings of the Cryptographers' Track at the RSA Conference 2009, LNCS 5473. Berlin: Springer-Verlag, 2009: 309-324.

[22] WASEF A, SHEN X. Efficient group signature scheme supporting batch verification for securing vehicular networks [C]// IEEE ICC 2010: Proceedings of the 2010 IEEE International Conference on Communications. Piscataway, NJ: IEEE Press, 2010: 1-5.