ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.19, No.10, October 2008, pp.2739−2745
DOI: 10.3724/SP.J.1001.2008.02739

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

基于ID的门限多重秘密共享方案*

庞辽军[1,2+], 裴庆祺[1], 焦李成[2], 王育民[1]

[1](西安电子科技大学 计算机网络与信息安全教育部重点实验室,陕西 西安 710071)

[2](西安电子科技大学 智能信息处理研究所,陕西 西安 710071)

An Identity (ID)-Based Threshold Multi-Secret Sharing Scheme

PANG Liao-Jun[1,2+], PEI Qing-Qi[1], JIAO Li-Cheng[2], WANG Yu-Min[1]

[1](Key Laboratory of Computer Network and Information Security for the Ministry of Education, Xidian University, Xi'an 710071, China)

[2](Institute of Intelligent Information Processing, Xidian University, Xi'an 710071, China)

+ Corresponding author: E-mail: ljpang@mail.xidian.edu.cn

Pang LJ, Pei QQ, Jiao LC, Wang YM. An identity (ID)-based threshold multi-secret sharing scheme. ***Journal of Software*****, 2008,19(10):2739−2745.** http://www.jos.org.cn/1000-9825/19/2739.htm

Abstract: In order to avoid the flaw of the secret shadow distribution method in the existing secret sharing schemes, a secret shadow distribution method is proposed with the ID-based public key technology integrated, which uses the participant's private key as his master shadow. Firstly, security analyses are made on Zheng's signcryption scheme, which shows his scheme does not offer forward secrecy. Then, an improvement is made on Zheng's signcryption scheme and a new scheme is proposed. Based on the proposed signcryption scheme and the ID-based public key cryptosystem, a new threshold multi-secret sharing scheme is proposed. The problem of the secret shadow distribution is well resolved, and no information exchange is needed between the secret dealer and each participant in advance. The secret shadow distribution can be processed during the secret distribution. At the same time, the proposed scheme offers forward secrecy. That is to say, even if the private key of the secret dealer is exposed, the security of the shared secrets will not be threatened. Therefore, the proposed ID-based secret sharing scheme is more secure and effective than others, and it can be more applicable.

Key words: secret sharing; signcryption; ID-based public key cryptosystem; forward secrecy

摘 要: 为了避免现有秘密共享方案中的秘密份额分发机制的不足,结合基于身份(ID)的公钥密码技术,提出了利用参与者私钥作为其主份额的秘密份额分发方法.首先,对 Zheng 提出的签密方案进行了安全分析,发现其不具备前向保密性,并针对该安全问题,提出了一个改进的签密方案.同时,在所提出的改进方案的基础上,结合基于 ID 的公钥密码系统,提出了一个新的门限多重秘密共享方案.该方案有效地解决了秘密份额的安全分发问题,不需要秘密分发

* Supported by the National Natural Science Foundation of China under Grant Nos.60803151, 60672112 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant No.2008AA01Z411 (国家高技术研究与发展计划(863)); the National Science Foundation for Post-Doctoral Scientists of China under Grant No.20070410376 (中国博士后科学基金); the Natural Science Foundation of Shannxi Province of China under Grant No.2007F37 (陕西省自然科学基金); the 111 Project of China under Grant No.B08038 (高等学校学科创新引智计划)

Received 2007-07-30; Accepted 2008-02-25

者和参与者之间事先进行任何信息交互,能够在分发秘密的同时分发秘密份额.该方案还具有前向保密性,即使秘密分发者的私钥被泄漏,也不会影响之前所共享秘密的安全性.因此,所提出的基于身份的秘密共享方案具有更高的安全性和有效性,能够更好地满足应用需求.

关键词: 秘密共享;签密;基于身份的公钥密码系统;前向保密性

中图法分类号: TP393 **文献标识码:** A

秘密共享是信息安全方向的一个重要分支,是安全协议的设计基础.无论在理论上,还是在实践上,对于计算机及网络的安全保密均具有重要的意义.秘密共享最早是由Shamir[1]和Blakley[2]分别独立提出来的.(t,n)门限秘密共享方案,就是将共享的秘密信息分为n个片段分别分配给n个合法参与者,即一个秘密被n个参与者所共享,当且仅当t个或t个以上的参与者联合可以恢复该秘密;而$(t-1)$个或更少的参与者不能得到该秘密的任何信息.自从秘密共享方案被提出以后,许多研究人员对其进行了大量的研究,取得了不少成果[3−6].

在实际应用中,由于秘密共享系统均为分布式系统,仅仅考虑如何对秘密信息进行共享是不够的,还应考虑在秘密共享方案中如何有效地进行秘密份额的分发,这也是目前在设计和实现秘密共享方案时需要解决的关键问题之一.如果这个问题解决不好,秘密共享方案的应用会受到很大的影响.早期的秘密共享技术并没有考虑这个问题,例如文献[1−4]中提出的方案等,一般都假设事先已经存在了一条安全信道来进行秘密份额的分发.而如何建立这样的安全信道和采用什么样的安全技术都影响着秘密共享方案的安全性和有效性.为此,研究人员提出在设计秘密共享方案时需要同时考虑秘密份额的分发问题[6].在后来的一些方案中,有些采用公钥加密技术来分发秘密份额,例如文献[5]提出的方案等,但这需要付出建立和管理公钥基础设施的代价,同时,还需解决用户存储、管理和传输公钥证书等问题.有些方案采用动态协商来建立秘密份额,例如文献[6]提出的方案等,但该方法需要秘密分发者和各参与者多次进行信息交换,不能离线(off-line)执行,提高了系统的通信复杂度.现有的秘密共享方案一般都采用上述 3 种方式之一来处理秘密份额分发问题.除此之外,秘密共享的一些应用[7]在安全性方面提出了更高的要求,要求秘密分发具备前向保密性[8].而在现有大多数的方案中,秘密分发者的私钥泄漏会影响之前所共享秘密的安全性,这显然达不到安全要求,即不具备前向保密性.

鉴于以上考虑,本文基于身份(ID)的公钥密码系统提出了一个多重秘密共享方案,能够在不增加参与者信息交互的情况下,有效地解决秘密共享技术中的秘密份额分发问题,同时,该方案也具有前向保密性.本文第 1 节分析Zheng提出的签密技术[9],并在分析的基础上进行改进.第 2 节结合基于ID的公钥密码系统和椭圆曲线双线性对,介绍本文所提出的秘密共享方案.第 3 节对该方案进行安全性和性能分析.第 4 节给出本文的结论.

1 Zheng 的签密方案及其改进

1.1 Zheng的签密方案及分析

本节我们将简单地介绍 Zheng 提出的签密方案.为了简单、清晰起见,我们将与安全性无关的时戳等信息略去,具体细节请参考文献[9].

系统参数.令p为一个大素数;令 $q\in Z_p^*$ 为 $p-1$ 的一个大素因子;令$h(\cdot)$是一个单向hash函数;令$h_k(\cdot)$是一个带密钥的钥控单向hash函数;令 (E_k,D_k) 为某安全对称密码算法的加、解密算法;令 $g\in Z_p^*$ 为q阶元素;令 $(x_a,y_a=g^{x_a}\bmod q)$ 为Alice的公、私钥对,其中x_a由Alice随机地从 Z_p^* 中选取;同样地,令 $(x_b,y_b=g^{x_b}\bmod q)$ 为Bob的公、私钥对.

签密过程.假设 Alice 要向 Bob 传递秘密信息 m,Alice 执行过程如下:

Step 1. 随机选取 $x\in Z_p^*$,计算 $k=(k_1,k_2)=h(y_b^x\bmod q)$;

Step 2. 计算 $c=E_{k_1}(m),r=h_{k_2}(m)$ 和 $s=x/(r+x_a)\bmod q$;

Step 3. 发送签密密文(c,r,s)给 Bob.

解密过程.Bob 收到 Alice 发送的签密密文(c,r,s)后,执行如下解密过程以获取信息 m:

Step 1. 计算 $k=(k_1,k_2)=h((y_a g^r)^{sx_b} \bmod p)$;

Step 2. 计算 $m=D_{k_1}(c)$;

Step 3. 计算 $h_k(m)$,并判断 $h_{k_2}(m)\stackrel{?}{=}r$ 是否相等.如果相等,则接受 m,否则拒绝 m.

下面,简单地对该协议是否具备前向保密性进行分析.这里,所谓前向保密性是指,当发送者的私钥泄漏时,攻击者仍然不能从以前发送过的签密密文中恢复出消息[7].很显然,该协议不具备前向保密性.对此,我们通过下面的定理来加以说明.

定理 1. Zheng 的签密方案不具备前向保密性.

证明:假设在Zheng的方案中,当发送者Alice的私钥x_a泄漏之前,Alice向Bob通过该协议传送了秘密信息m.这时,如果x_a被泄漏,攻击者可以由等式 $s=x/(r+x_a) \bmod q$ 变形得到 $x=s(r+x_a) \bmod q$.这里,由于s和r为签密密文的部分信息,而x_a为发送者Alice已经泄露的私钥,因此,攻击者可以正确地计算出x的值.从而,结合接收者 Bob 的公钥很容易计算出 $k=(k_1,k_2)=h(y_b{}^x \bmod p)$.进而,就可以解密得到 $m=D_{k_1}(c)$.故,Zheng 的签密方案不具备前向保密性. □

1.2 改进的签密方案

因为 Zheng 提出的签密方案不具备前向保密性,当发送者的私钥泄漏后,他们之前传送任意秘密信息都可以被计算出来,方案的应用受到了一定影响.这里,我们将对 Zheng 的方案进行改进,提出一个具有前向保密性的新方案.新方案的系统参数与原方案相同.

签密过程.假设 Alice 要向 Bob 传递秘密信息 m,Alice 执行过程如下:

Step 1. 随机选取 $x\in Z_p^*$,计算 $k=(k_1,k_2)=h(y_b{}^x \bmod p)$;

Step 2. 计算 $r=h_{k_2}(m), c=E_{k_1}(m\|r), R=g^r$ 和 $s=x/(r+x_a) \bmod q$;

Step 3. 发送签密密文(c,s,R)给 Bob.

解密过程.Bob 收到 Alice 的签密密文(c, s, R)后,解密过程如下:

Step 1. 计算 $k=(k_1,k_2)=h((y_a R)^{sx_b} \bmod p)$;

Step 2. 计算 $m\|r=D_{k_1}(c)$ 和 $h_{k_2}(m)$;

Step 3. 判断 $h_{k_2}(m)\stackrel{?}{=}r$ 是否相等.如果相等,则接受 m,否则,拒绝 m.

方案分析:这里,主要将新方案与原方案进行比较,从安全性、性能及可用性等方面进行分析.

(1) 安全性.新方案的正确性很容易得到证明,这里主要分析其前向保密性.假设发送者Alice的私钥x_a已经被泄漏.在新方案中,由R计算r面临求解离散对数问题.若不知道r的值,也就无法从 $s=x/(r+x_a) \bmod q$ 中求出x,从而不可能由 $h(y_b{}^x \bmod p)$ 或 $h((y_a R)^{sx_b} \bmod p)$ 计算出密钥k=(k_1,k_2),因此,在发送者私钥泄漏的情况下并不会暴露秘密信息 m,从而证明了新方案具有前向保密性.

(2) 计算性能.新方案比原方案在计算上增加了一个指数运算,计算量有所增加.但该指数运算主要用于保护方案中的信息r,从而使得即使发送方的私钥泄露,攻击者在不知道r的情况下也无法计算出密钥k=(k_1,k_2).因此,新方案具有前向保密性,更安全、更符合应用需求,在安全性和性能方面的折衷是可以接受的.

(3) 可用性.因为 Zheng 的签密方案是非常经典的一个协议,已经得到广泛的应用.如果为了增加系统的前向保密性而对系统的实现作较大的改动往往令人难以接受.为此,在改进的协议中,保持系统参数及参与者双方之间的接口不变,仅对局部实现进行了改进,使得新方案具有较高的可用性,并能够很容易地被用户接受.

2 本文提出的基于 ID 的秘密共享方案

2.1 系统参数

在基于身份ID的公钥密码系统[10]中,用户的公钥就是用户的身份信息ID或由ID产生的信息.系统参数由可

信第三方公钥生成中心PKG选取,包括:两个q阶的循环群$(G_1,+)$和$(G_2,\cdot)$;P为G_1的生成元;令e为G_1和G_2上的双线性变换,即$e:G_1\times G_1\to G_2$;PKG随机选取自己的私钥$S_{PKG}\in Z_p^*$,其对应公钥为$Q_{PKG}=S_{PKG}P\in G_1$;$h_0:\{0,1\}^*\to G_1$和$h_1:\{0,1\}^*\to Z_p^*$为两个单向hash函数;令$h_k(\cdot)$是一个带密钥的钥控单向hash函数;$f(x,y)$为Z_p^*上的一个双变量单向函数[11];(E_k,D_k)为某对称密码算法的加、解密算法;参与者$u_i(i=1,2,\ldots,n)$的公、私钥对为$Q_i=h_0(ID_i)$和$S_i=S_{PKG}Q_i$;秘密分发者d的公、私钥对为$Q_d=h_0(ID_d)$和$S_d=S_{PKG}Q_d$.在本文提出的秘密共享方案中,参与者私钥将作为其主秘密份额来实现对子秘密份额的分发.

2.2 具体设计

(1) 秘密分发.为了在这 n 个参与者中共享秘密信息$m\in Z_p^*$,使得至少 t 个参与者合作才可以重构该秘密,秘密分发者可以执行如下算法:

Step 1. 随机地从Z_p^*中选取n个秘密随机数$m_1,m_2,\ldots,m_n$和公开随机数$m_0\in Z_p^*$,并计算$M_i=f(m_0,m_i)$(i=1,2,…,n).其中,m_i将作为对应参与者u_i(i=1,2,…,n)的子秘密份额,并用于进行秘密恢复;

Step 2. 使用 n+1 个数值对$(h_1(ID_i),M_i)$(i=1,2,…,n)和(0,m)构造 n 次 Lagrange 插值多项式 $F(x)$如下:

$$F(x)=m\times\prod_{i=1}^{n}\frac{x-h_1(ID_j)}{-h_1(ID_j)}+\sum_{i=1}^{n}M_i\frac{x}{h_1(ID_i)}\prod_{j=1,j\neq i}^{n}\frac{x-h_1(ID_j)}{h_1(ID_i)-h_1(ID_j)}\bmod q \tag{1}$$

Step 3. 随机选取$x_i\in Z_p^*$,计算$k_i=(k_{i,1},k_{i,2})=h(e(Q_i,Q_{PGK})^{x_i})$($i$=1,2,…,$n$);

Step 4. 计算$r_i=h_{k_{i,2}}(m_i),c_i=E_{k_{i,1}}(m_i\|r_i),R_i=r_iQ_d$和$s_i=x_iQ_{PKG}-r_iS_d\in G_1$,并将$(c_i,s_i,R_i)$发送给参与者$u_i$($i$=1,2,…,$n$);

Step 5. 从$[1,q-1]-\{h_1(ID_i)\mid i=1,2,...,n\}$中选取$n$–$t$+1 个最小整数$d_i$并计算$F(d_i)$($i$=1,2,…,$n$–$t$+1).最后,将它们通过广播形式进行公开.

(2) 秘密恢复.任意t个参与者可以合作来恢复所共享的秘密m.不失一般性,选取t个参与者的集合$\{u_1,u_2,\ldots,u_t\}$为例来说明秘密重构过程.秘密重构过程如下:

Step 1. 参与秘密重构的每个参与者u_i(i=1,2,…,t)获取信息(c_i,s_i,R_i),计算$k_i=(k_{i,1},k_{i,2})=h(e(Q_i,s_i)e(S_i,R_i))$;

Step 2. 每个参与者u_i(i=1,2,…,t)解密获得$m_i\|r_i=E_{k_{i,1}}(c_i)$.如果等式$r_i\stackrel{?}{=}h_{k_{i,2}}(m_i)$成立,则说明秘密分发成功,否则,秘密分发过程有误,向秘密分发者提供错误报告;

Step 3. 每个参与者u_i(i=1,2,…,t)计算$M_i=f(m_0,m_i)$,并将其提交给指定的秘密计算者DC(designated combiner).其中,m_0为公开信息;

Step 4. 秘密计算者收到这t个信息M_i(i=1,2,…,t)后,利用参与者身份信息可以构造t个数值对$(h_1(ID_i),M_i)$($i=1,2,\ldots,t$),同时,从$[1,q-1]-\{h_1(ID_i)\mid i=1,2,...,n\}$中选取$n-t+1$个最小整数$d_i$构成$n-t+1$个数值对$(d_i,F(d_i))$($i$=1,2,…,$n$–$t$+1);

Step 5. 使用所得到的这n+1 个数值对$(h_1(ID_i),M_i)$(i=1,2,…,t)和$(d_i,F(d_i))$(i=1,2,…,n–t+1)重构n次Lagrange插值多项式$F(x)$如下:

$$F(x)=\sum_{i=1}^{t}M_i\left(\prod_{j=1,j\neq i}^{t}\frac{x-h_1(ID_j)}{h_1(ID_i)-h_1(ID_j)}\prod_{j=1}^{n-t+1}\frac{x-d_j}{h_1(ID_i)-d_j}\right)+\sum_{i=1}^{n-t+1}F(d_i)\left(\prod_{j=1,j\neq i}^{n-t+1}\frac{x-d_j}{d_i-d_j}\prod_{j=1}^{t}\frac{x-h_1(ID_j)}{d_i-h_1(ID_j)}\right) \tag{2}$$

Step 6. 计算所共享的秘密 m=F(0).

(3) 共享多个秘密.本文提出的秘密共享方案具有多重秘密共享方案的特性[4],即只需要每个参与者保存一个秘密份额,该秘密份额可以用于多次秘密共享过程中而无需进行更新.对于本文方案来说,一个秘密分发者在n个参与者中共享第 1 个秘密,秘密分发算法和秘密恢复算法如上文所述;如果还需要进一步共享其他秘密,算法可以进行一些改进以提高系统性能.

为了提高秘密共享系统的性能,在第 1 次秘密分发过程之后,秘密分发者和各参与者保存相应的秘密数据$m_1,m_2,\ldots,m_n$,以便在后续秘密共享过程中使用.后续的秘密分发和秘密恢复过程可以简化如下:在秘密分发过程

中,秘密分发者只需执行Step 1,Step 2 和Step 5 即可.其中,在Step 1 中,秘密分发者不再重新选取秘密数据$m_1,m_2,\ldots,m_n$,仅需要重新选取随机数m_0,并计算$M_i = f(m_0, m_i)$ (i=1,2,…,n);在秘密恢复过程中,合作的参与者只需要执行Step 3~Step 6 即可.其中,在Step 3 中,秘密数据$m_1,m_2,\ldots,m_n$同样取值为上次秘密共享过程中的数值.

重复地使用秘密数据$m_1,m_2,\ldots,m_n$,并不会影响共享秘密的安全性,这是由双变量单向函数的性质所决定的,关于这一点有兴趣的读者可以参阅文献[11].

3 分析和证明

3.1 正确性分析

定理 2. 在第 2 节所述秘密共享方案中,恒有$e(Q_i,s_i)e(S_i,R_i) = e(Q_i,Q_{PGK})^{x_i}$成立.

证明: $e(Q_i,s_i)e(S_i,R_i) = e(Q_i,x_iQ_{PKG} - r_iS_d)e(S_i,r_iQ_d) = e(Q_i,x_iQ_{PKG} - r_iS_d)e(S_i,Q_d)^{r_i}$

$= e(Q_i,x_iQ_{PKG} - r_iS_d)e(Q_i,S_d)^{r_i} = e(Q_i,x_iQ_{PKG} - r_iS_d)e(Q_i,r_iS_d)$

$= e(Q_i,x_iQ_{PKG}) = e(Q_i,Q_{PGK})^{x_i}$.

在上述证明过程中,所使用的等价变换为双线性变换[12]. □

3.2 安全性分析

定理 3. 在秘密分发过程中,只有相应的参与者u_i可以获取秘密分发者发送的秘密数据m_i(i=1,2,…,n),而其他人无法获取该秘密数据.

证明:秘密数据m_i(i=1,2,…,n)的作用是作为参与者u_i的子秘密份额,其安全性是整个秘密共享系统的基础.若攻击者能够得到这些秘密数据,则系统中共享的秘密就很容易被计算出来.由改进的签密方案可知,参与者u_i可以通过对(c_i,s_i,R_i)进行解签密而计算出秘密数据m_i.而其他人想要从(c_i,s_i,R_i)中求取m_i则面临着攻破该签密方案的困难性,这在计算上是不可行的.攻击者若想从密文信息$c_i = E_{k_{i,1}}(m_i \| r_i)$中直接求取秘密数据$m_i$也是不可行的,这将面临攻破对称加密算法的困难性.因此,除了参与者u_i,其他任何人无法获取其秘密份额m_i. □

定理 4. 在共享多个秘密时,秘密数据m_i(i=1,2,…,n)的重用不会影响系统的安全性.

证明:由定理 3 可知,除了秘密分发者以外,只有参与者u_i可以获取子秘密份额m_i,其他人无法获取他人的子秘密份额.在秘密恢复过程中,并没有直接使用这些秘密信息,而是使用双变量单向函数对其计算的结果.双变量单向函数具有很好的安全性质,有兴趣者可参阅文献[11],这里不再赘述.在本方案中,尽管每个参与秘密恢复的参与者u_i(i=1,2,…,t)都提供了一个由其子秘密份额m_i计算的伪份额$M_i = f(m_0, m_i)$,但根据双变量单向函数的安全性质,该伪份额不会披露其真正的秘密份额m_i.同样地,根据双变量单向函数的安全性质,即使在多次秘密共享过程中,参与者u_i披露了一系列伪份额$M_{i,1} = f(m_{0,1}, m_i), M_{i,2} = f(m_{0,2}, m_i), \ldots, M_{i,l} = f(m_{0,l}, m_i)$,攻击者根据这些信息来伪造关于另一个共享秘密$m_{0,l+1}$的伪份额$M_{i,l+1} = f(m_{0,l+1}, m_i)$并使其通过验证也是计算上不可行的. □

定理 5. 本文方案符合门限秘密共享方案的门限规则.

证明:在一个(t,n)门限秘密共享方案中,有两个基本条件必须满足:(1) t或t个以上的参与者合作很容易恢复共享的秘密;(2) (t–1)个或更少的参与者合作却无法恢复共享的秘密.要恢复所共享的秘密,就必须首先重新构造出n次Lagrange插值多项式$F(x)$.由秘密恢复过程可知,t个参与者可以计算出满足多项式$F(x)$的t个数值对$(h_1(ID_i), M_i)$ (i=1,2,…,t),再利用公开信息可以获得满足多项式$F(x)$的另外n–t+1 个数值对$(d_i, F(d_i))$(i=1,2,…,n–t+1),通过这n+1 个数值对,就可以依据等式(2)重构n次多项式$F(x)$,从而计算出所共享的秘密$F(0)$.而对于(t–1)个或更少的参与者来说,即使系统在秘密分发过程的Step 5 已经公开了n–t+1 个关于$F(x)$的数值对,但(t–1)个或更少的参与者只能最多再提供(t–1)个关于$F(x)$的数值对.在这种情况下,要计算出共享的秘密等价于攻破Shamir的门限方案[1],这显然是计算上不可行的.因此,本文方案符合门限秘密共享方案的门限规则. □

定理 6. 本文方案具备前向保密性,即使秘密分发者的私钥泄漏不会影响之前所共享秘密的安全性.

证明:所谓前向保密性,指的是当秘密分发者的私钥不小心或在无意中泄漏后,之前所共享秘密的安全性不会受到任何影响.由对改进的签密方案的安全性分析过程可知,即使秘密分发者的私钥泄漏,秘密分发者通过签密技术发送给各参与者u_i的秘密份额$m_i(i=1,2,\ldots,n)$也不会被任何攻击者所获取.而由定理3~定理5可知,本文方案的安全性主要依赖于参与者秘密份额$m_i(i=1,2,\ldots,n)$的安全性.因此,秘密分发者私钥的泄漏不会对之前所共享的秘密造成安全威胁,即本文方案具备前向保密性. □

3.3 性能分析

本文提出的多重秘密共享方案结合了基于身份ID的公钥密码系统特点,避免了采用传统公钥系统引起的复杂公钥管理难题,如文献[3,5]提出的方案等.这里,用户的公钥就是由身份信息ID经Hash运算生成的信息,或者,有时也可以直接使用其身份信息,用户不需要管理公钥簿.秘密信息的传递使用签密技术,无需进行任何交互,也不再需要像传统公钥系统那样进行证书的传递和验证,只需要知道各参与者的身份信息和一些系统参数即可.同时,由于采用了椭圆曲线上双线性对,能够使方案以较短的密钥得到同等的安全强度.例如,在同等安全前提下,160 bit的椭圆曲线密码相当于1 024 bit的RSA,而签密和解签密速度比RSA快很多.本文采用了签密技术,很好地解决了秘密共享技术中的秘密份额传递问题,不需要进行任何交互过程,也不需要面临传统公钥的公钥管理难题,更符合实际的应用需求.

本文方案能够在不增加通信复杂度的情况下有效地解决秘密份额的分发问题.为了便于与现有方案进行比较,我们根据秘密份额分发机制对现有方案作一分类,然后每一类选取一个方案作为代表来与本文方案进行性能比较.如前文所述,假定实现存在安全信道的秘密共享方案,例如文献[1–4]提出的方案等,以文献[1,4]中提出的方案为代表,后者为一个多重秘密共享方案;采用公钥加密技术来分发秘密份额,以文献[5]提出的方案为代表;采用动态协商来建立秘密份额,以文献[6]提出的方案为代表.下面,我们通过表1将本文方案和这些方案作一简单比较.

Table 1 Performance comparisons between the existing schemes and the proposed scheme

表1 本文方案与现有方案的性能比较

Schemes	Identity authentication	Secure channel	Reuse of secret shadows	Secret shadow distribution method	Forward secrecy
Scheme[1]	No	Required	No	Unspecific method in advance	No
Scheme[4]	No	Required	Yes	Unspecific method in advance	No
Scheme[5]	No	Required	Yes	Encryption method in advance	No
Scheme[6]	No	Not needed	Yes	Negotiation method in advance	Yes
The proposed scheme	Yes	Not needed	Yes	No action in advance	Yes

从表1可以看出,在这些秘密共享方案中:(1) 只有本文方案可以提供参与者的身份验证,而由文献[1,4–6]提出的方案中,必须通过公告牌[11]来公布有效的参与者;(2) 对于安全信道,本文方案使用了改进的签密技术,不需要安全信道,文献[6]提出的方案通过DH交换协商秘密份额,也不需要安全信道,而在文献[1,4,5]提出的方案中,必须维护安全信道;(3) 在秘密份额重用方面,本文方案与文献[4–6]提出的方案一样,每个参与者的秘密份额可以用于多次秘密共享过程而无需更新,仅文献[1]的方案在每次秘密共享过程前都需要重新分发秘密份额,通信量较大;(4) 在秘密份额分发形式方面,文献[1,4–6]提出的方案都需要在秘密分发之前,通过安全信道或消息交换来分发或协商秘密份额,而本文方案可以在秘密分发的同时进行秘密份额的分发,事先无需进行任何处理,因而,效率更高;(5) 在安全性方面,文献[1,4,5]提出的方案通过安全信道进行秘密份额的分发,秘密分发者私钥的泄漏必将影响秘密份额的安全性,从而也影响共享秘密的安全性,而文献[6]提出的方案通过DH交换协商秘密份额,一方私钥的泄漏不会影响方案的安全性,本文方案基于改进的签密方案,因而也继承了其前向保密性.通过分析,相比较而言,本文方案比现有的这些秘密共享方案更有效,也更符合实际应用.

4 结束语

本文分析了Zheng的签密技术,发现其不满足前向保密性.在分析的基础上,对该签密技术进行了改进,改进的签密方案能够满足前向保密性要求.同时,在改进的签密方案的基础上,结合椭圆曲线双线性对,提出了一种

新的基于 ID 的多重秘密共享方案.与现有秘密共享方案相比,本文在不增加参与者之间信息交互的情况下,很好地解决了秘密共享中的秘密分发问题.同时,该方案也具有前向保密性.由于采用了基于身份的公钥密码,不仅节省了建立和管理公钥基础设施的代价,而且,避免了用户存储、管理和传输公钥证书等问题.因此,本文基于 ID 的秘密共享方案具有更高的安全性和有效性,能够更好地满足应用需求.

致谢 在此,我们向对本文提出宝贵建议的审稿专家及参与本文内容讨论的所有老师和同学表示衷心的感谢.

References:

[1] Shamir A. How to share a secret. Communications of the ACM, 1979,22(11):612−613.

[2] Blakley G. Safeguarding cryptographic keys. In: Merwin E, Zanca T, eds. Proc. of the American Federation of Information Processing Societies Conf. (AFIPS'79). New York: AFIPS Press, 1979. 313−317.

[3] Fei RC, Wang LN. Cheat-Proof secret share schemes based on RSA and one-way function. Journal of Software, 2003,14(1): 146−150 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/146.htm

[4] Li HX, Pang LJ, Cai WD. An efficient threshold multi-group-secret sharing scheme. In: Cao BY, ed. Proc. of the 2nd Int'l Conf. of Fuzzy Information and Engineering (ICFIE 2007). Heidelberg: Springer-Verlag, 2007. 911−918.

[5] Pang LJ, Wang YM. (*t*,*n*) threshold secret sharing scheme based on RSA cryptosystem. Journal of Communications, 2005,26(6): 70−73 (in Chinese with English abstract).

[6] Hwang RJ, Chang CC. An on-line secret sharing scheme for multi-secrets. Computer Communications, 1998,21(13):1170−1176.

[7] Zhu Y, Yang YT, Sun ZW, Feng DG. Ownership proofs of digital works based on secure multiparty computation. Journal of Software, 2006,17(1):157−166 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/157.htm

[8] Hwang RJ, Lai CH, Su FF. An efficient signcryption scheme with forward secrecy based on elliptic curve. Applied Mathematics and Computation, 2005,167(1):870−881.

[9] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption)<<cost(signature)+cost(encryption). In: Kaliski B, ed. Proc. of the Advances in Cryptology (CRYPTO'97). LNCS 1294, Heidelberg: Springer-Verlag, 1997. 165−179

[10] Shamir A. Identity-Based cryptosystems and signature schemes. In: Blakley GR, Chaum D eds. Proc. of the Advances in Cryptology (CRYPTO'84). LNCS 196, Heidelberg: Springer-Verlag, 1984. 47−53.

[11] Pang LJ, Wang YM. A new (*t*,*n*) multi-secret sharing scheme based on Shamir's secret sharing. Applied Mathematics and Computation, 2005,167(2):840−848.

[12] Boneh D, Franklin M. Identity-Based encryption from the Weil pairing. In: Kilian J, ed. Proc. of the Advances in Cryptology (CRYPTO 2001). LNCS 2139, Heidelberg: Springer-Verlag, 2001. 213−229.

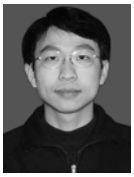
附中文参考文献:

[3] 费如纯,王丽娜.基于 RSA 和单向函数防欺诈的秘密共享体制.软件学报,2003,14(1):146−150. http://www.jos.org.cn/1000-9825/14/146.htm

[5] 庞辽军,王育民.基于 RSA 密码体制(*t*,*n*)门限秘密共享方案.通信学报,2005,26(6):70−73.

庞辽军(1978－),男,陕西渭南人,博士,CCF 学生会员,主要研究领域为密码学,安全协议设计与分析.

焦李成(1959－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为神经网络,机器学习,自然计算,图像感知和认知.



裴庆祺(1975－),男,博士,讲师,CCF 高级会员,主要研究领域为密码学,安全协议设计与分析.

王育民(1936－),男,教授,博士生导师,主要研究领域为信息论,密码,编码.