基于身份自证实的秘密共享方案

裴庆祺[1),2)] 马建峰[1)] 庞辽军[1)] 张红斌[3)]

[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 西安 710071)

[2)](中国电子设备系统工程公司研究所 北京 100141)

[3)](河北科技大学信息科学与工程学院 石家庄 050018)

摘 要 为了解决现有秘密共享方案中秘密份额的安全分发问题,基于 Girault 密钥交换协议,结合基于身份(ID)的公钥密码技术提出了一个新的秘密共享方案,并对其进行了安全性和性能分析.该方案中,用户的私钥作为其秘密份额,无须秘密分发者为每个用户分发秘密份额.用户的私钥可以由用户自己选取,可信第三方无法获取其私钥.同时,任何人都可以以离线方式验证每一个参与者公钥的合法性.分析表明,文中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,能更好地满足应用需求.

关键词 密钥交换;基于身份的公钥密码技术;秘密共享

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2010.00152

An Identity (ID)-Based and Self-Certified Secret Sharing Scheme

PEI Qing-Qi[1),2)] MA Jian-Feng[1)] PANG Liao-Jun[1)] ZHANG Hong-Bin[3)]

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

[2)](*Institute of China Electronic System Engineering Corporation, Beijing* 100141)

[3)](*Institute of Information Science and Engineering, Hebei University of Science and Technology, Shijiazhuang* 050018)

Abstract In order to resolve the secure distribution problem in the existing secret sharing schemes, based on Girault's key exchange protocol, a new secret sharing scheme is proposed, which adopts the ID-based public key cryptography technology. And then, security and performance analysis is made on this scheme. Each participant's private key is used as his secret shadow, which are not selected and redistributed by the secret dealer any longer. The private key of each participant is chosen by the participant himself, and even the trusted third party cannot gain his private key. At the same time, anyone can verify every participant's public key, and judge whether it is valid in the form of off-line. Analysis shows that the proposed ID-based secret sharing scheme is more secure and effective than others, and it can be more applicable.

Keywords key exchange; ID-based public key cryptography technology; secret sharing

1 引 言

秘密共享是现代密码学领域中一个非常重要的分支,也是信息安全方向一个重要的研究内容.第一个秘密共享方案是 (t,n) 门限秘密共享方案,该方案是 Shamir[1] 和 Blakley[2] 在 1979 年分别基于 Lagrange 插值法和多维空间点的性质提出的.自从

收稿日期:2008-05-20;最终修改稿收到日期:2009-05-15.本课题得到国家自然科学基金(60803150,60803151)、国家"八六三"高技术研究发展计划项目基金(2008AA01Z411)、国家自然科学基金委员会-广东联合基金重点项目(U0835004)、中国博士后科学基金(20090451495)和陕西省自然科学基础研究计划项目(2007F37)资助.**裴庆祺**,男,1975 年生,博士,副教授,主要研究方向为无线网络及其安全、数字版权管理.E-mail: qqpei@mail.xidian.edu.cn.**马建峰**,男,1963 年生,博士,教授,主要研究领域为网络与信息安全、密码学.**庞辽军**,男,1978 年生,博士,副教授,主要研究方向为网络与信息安全.**张红斌**,男,1976 年生,博士,研究方向为计算机网络安全与管理.

秘密共享概念被提出后，许多研究人员对其做了大量的研究，并取得了不少成果[3-7].

现有大多数秘密共享方案具有一些共同点：(1)各参与者的秘密份额都是由秘密分发者产生，秘密分发者掌握着所有参与者的秘密份额，如文献[1-2]等.这使得秘密分发者需要保存大量的秘密信息，而且会成为攻击者所攻击的目标；(2)在秘密分发者和各参与者之间需要一条安全信道，利用该信道进行秘密份额的分发，但是维护一条安全信道会提高系统的代价和复杂度.而且在许多秘密共享方案中，为了能够检验在秘密重构过程中合作的参与者是否进行欺骗，秘密分发者需要专门构造一个验证算法和一些验证信息.这必然会增加系统的复杂度，并影响秘密分发的效率.这些特点或多或少会影响秘密共享方案的实际应用，比如，当参与者和秘密分发者不可能存在安全信道时，这些方案也将不再有用.

本文利用 Girault 设计的基于身份的密钥交换协议[10-11]，提出了一个(t,n)门限秘密共享方案.它使用参与者的身份作为他们的秘密份额对应的公开信息，秘密分发者和各参与者之间无须进行任何通信和信息交换，因此，他们之间不需要维护安全信道.在秘密重构过程中，每个合作的参与者只需提交一个由秘密份额计算的伪份额，而且不需要暴露其真实的秘密份额值.由于在秘密重构过程中，每个参与者只需提交一个由秘密份额计算的伪份额，而不必暴露他的秘密份额，因此，该方案可以用来共享任意多个秘密，而不必修改参与者的秘密份额.方案的安全性是基于所使用的 Girault 基于身份的密钥交换协议、所采用对称加密算法和 Shamir 的(t,n)门限方案的安全性.

2　Girault 基于身份的密钥交换协议

Girault 方案需要一个可信赖的机构 TA(假设它是 Trent)，TA 建立系统参数，并帮助秘密分发者和各参与者建立他们的密钥.

2.1　系统密钥建立过程

Trent 生成 RSA 密钥数据如下：

(1) 一个公开模数 $N=pq$，其中 p,q 是长度相等大素数，例如$|p|=|q|=512$；

(2)一个公开指数 e 且与 $\phi(N)$互素，其中$\phi(N)=(p-1)(q-1)$；

(3)一个秘密指数 d 且满足 $ed\equiv 1(\phi(N))$；

(4)一个公开元素 $g\in Z_n^*$ 具有最大的乘法阶，为了计算 g，Trent 找 g_p作为模 p 的生成元和 g_q作为模 q 的生成元，然后 Trent 可以运用中国剩余定理来构造.

Trent 公开系统参数(N,e,g)，并秘密保存系统私钥 d.

2.2　用户的密钥数据

秘密分发者和各参与者可以通过以下过程与 Trent 一起生成自己的密钥.假设 Alice 要建立自己的密钥系统，可以执行以下过程：

(1) Alice 随机选择一个长度为 160bit 的整数 s_A作为私钥，计算

$$v\leftarrow g^{-s_A}(\mathrm{mod}N) \tag{1}$$

并把 v 发送给 Trent.

然后，她运用任何一个零知识证明协议向 Trent 证明她知道 s_A且不泄漏 s_A，Alice 也发送她的身份 I_A给 Trent.

Trent 创建 Alice 的公钥为$v-I_A$的 *RSA* 签名：

$$P_A\leftarrow (v-I_A)^d(\mathrm{mod}N) \tag{2}$$

Trent 发送 P_A给 Alice 作为 Alice 公钥的一部分.因此，下面的等式成立.

$$I_A\equiv P_A^e-v(\mathrm{mod}N) \tag{3}$$

表面看来，在密钥的建立过程中，由于 P_A和 v 是 Z_N^* 两个随机数，因此看起来构造(3)似乎并不困难.例如，Alice 随机选取 P_A并根据式(3)用 P_A^e和 I_A 计算 v.然而，如果按这种方式来计算 v，Alice 就不能知道它以 g 为底模 N 的离散对数.

Alice 能够证明她知道以 g 为底模 N 的离散对数，即值$-s_A$，这就保证了 P_A是由 Trent 发行的.完成这个证明的最简单方法是运用 Diffie-Hellman 密钥交换协议的一个变形.

2.3　密钥交换协议

假设(s_A,P_A,I_A)是 Alice 的公钥数据，(s_B,P_B,I_B)是 Bob 的公钥数据.他们可以通过协商简单地交换一个认证的密钥：

$$K_{AB}\equiv(P_A^e+I_A)^{s_B}\equiv(P_B^e+I_B)^{s_A}\equiv g^{-s_As_B}(\mathrm{mod}N) \tag{4}$$

在这个密钥协商中，Alice 计算$(P_B^e+I_B)^{s_A}(\mathrm{mod}N)$，Bob 计算$(P_A^e+I_A)^{s_B}$.因此，这的确是一个 Diffie-Hellman 密钥协商协议.如果双方能够协商相同的密钥，那么他们就知道另一方已经证明了她/他的身份.

3　本文提出的新方案

3.1　系统成员及主要参数

系统成员.包括可信的秘密分发者 d(dealer)和 n 个参与者(participant) $P_1,P_2,\cdots,P_n$.

系统参数. 首先,可信第三方 Trent 生成Girault方案的公开系统参数(N,e,g),并秘密保存系统私钥d,该过程与第 2.1 节内容相似;假设秘密分发者的公钥数据为(s_d,P_d,I_d),各参与者P_i的公钥数据为(s_i,P_i,I_i);令Q是一个随机选取的且大于N的素数;一个公告牌(Noticeboard),只有秘密分发者可以修改、更新公告牌上的内容,其他人只能阅读或下载;以每个参与者的私钥作为其秘密份额;令(E_k,D_k)为某安全的对称密码算法的加、解密算法,其中k为对称密钥;令$h(\cdot)$是一个单向 hash 函数.

3.2 秘密分发算法

为了在n个参与者$P_1,P_2,\cdots,P_n$中共享秘密$s\in Z_Q$,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.

D1. 从$[N^{1/2},N-1]$中随机选取一个整数r;

D2. 对于每一个参与者$P_i(i=1,2,\cdots,n)$,秘密分发者执行以下过程:

D2.1. 计算$K_{d,i}=(P_i^e+I_i)^{s_d}=g^{-s_d s_i}(\mathrm{mod}N)$;

D2.2. 利用自己计算的$K_{d,i}$作为对称加密密钥对r进行加密,即计算$E_{K_{d,i}}(r)$;

D2.3. 计算$H_{d,i}=h(E_{K_{d,i}}(r))$.

D3. 利用$(n+1)$个点$(0,s)$,$(x_1,E_{K_{d,1}}(r))$,$(x_2,E_{K_{d,2}}(r))$,$\cdots$,$(x_n,E_{K_{d,n}}(r))$和 Lagrange 插值方法构造n阶多项式$f(x)$:

$$f(x)=s\times\prod_{k=1}^{n}(x-x_k)/(-x_k)+\sum_{l=1}^{n}[E_{K_{d,l}}(r)\times(x/x_l)\times\prod_{k=1,k\neq l}^{n}(x-x_k)/(x_l-x_k)]\mathrm{mod}Q \tag{5}$$

D4. 分别计算$f(1),f(2),\cdots,f(n-t+1)$;

D5. 在公告牌上公开关于秘密s的信息:

$$\mathrm{Msg}(s)=(r,f(1),f(2),\cdots,f(n-t+1),H_{d,1},\cdots,H_{d,n}).$$

3.3 秘密重构算法

为了重构秘密s,需要至少t个参与者合作. 不失一般性,假设t个参与者$P_1,P_2,\cdots,P_t$准备重构秘密s. 注意每一个参与者不需要提供他的秘密份额,即他的私钥,而仅仅需要提供一个由秘密份额计算的伪份额. 而且,在这个过程中,任何人都可以立即检验各参与秘密重构的合作者是否诚实地提供自己正确的份额. 下面,给出参与者$P_1,P_2,\cdots,P_t$如何重构秘密s:

R1. 每个合作的参与者P_i从公告牌上读取关于共享秘密s的公开信息 Msg(s).

R2. 每个合作的参与者P_i利用自己的私钥计算

$$K_{i,d}=(P_d^e+I_d)^{s_i}=g^{-s_d s_i}(\mathrm{mod}N) \tag{6}$$

R3. 每个合作的参与者P_i利用自己计算的$K_{i,d}$作为对称加密密钥对r进行加密,即计算$E_{K_{i,d}}(r)$,并将其提交给指定的秘密计算者.

R4. 由 Girault 方案的性质可知,$K_{i,d}=K_{d,i}$,因此有$E_{K_{i,d}}(r)=E_{K_{d,i}}(r)$. 这样就可以得到$t$个点$(x_1,E_{K_{1,d}}(r))$,$(x_2,E_{K_{2,d}}(r))$,$\cdots$,$(x_t,E_{K_{n,d}}(r))$,再利用公开的信息 Msg$(s)$可以得到另外的$(n-t+1)$个点$(1,f(1))$,$(2,f(2))$,$\cdots$,$(n-t+1,f(n-t+1))$. 通过汇集这$(n+1)$个秘密点,采用 Lagrange 内插多项式[1]即可重构多项式$f(x)$. 为简单起见,如果用(X_i,Y_i) $i=1,2,\cdots,n+1$来表示所得到的$(n+1)$个数值对,就可以如下方法重构n次 Lagrange 插值多项式$f(x)$:

$$f(x)=\sum_{i=1}^{n+1}Y_i\prod_{j=1,j\neq i}^{n+1}\frac{x-X_j}{X_i-X_j}\ \mathrm{mod}\ Q \tag{7}$$

R5. 恢复所共享的秘密$s=f(0)$.

4 分析与讨论

定理 1. 本文方案能够预防参与者之间的相互欺骗.

证明. 在任何基于群的密码协议中,均需要考虑预防内部参与者之间的相互欺骗问题,本文方案在设计时已经考虑到预防参与者之间相互欺骗的内部攻击. 如果某个参与者P_i想进行欺骗,他可以在秘密恢复过程的第 R3 步计算$E_{K_{i,d}}(r)$时进行欺骗. 但是,任何参与者均可以通过验证等式$H_{d,i}=h(E_{K_{i,d}}(r))$是否成立来验证其提交的份额$E_{K_{i,d}}(r)$的有效性. 因为信息$H_{d,i}$是公开的,因此,任何参与者都可以利用该等式对$E_{K_{i,d}}(r)$进行验证,发现这种欺骗,从而防止内部参与者之间的相互欺骗. 证毕.

定理 2. 本文方案能够预防外部攻击者的主动攻击.

证明. 系统外的攻击者可以通过设法推导出秘密分发者在第 D2.1 步计算的密钥$K_{d,i}$,或各参与者P_i在第 R2 步计算的密钥$K_{i,d}$来对本方案进行攻击. 如果他能够设法计算出这些信息,那么,整个秘密共享系统将会被攻破. 但是,由于 Girault 密钥交换协议的安全性,攻击者的这种攻击无法奏效,除非他能够获取秘密分发者或各参与者的私钥. 而要获取他们的私钥,攻击者面临着求解离散对数问题的困难性,因此,这种攻击在 Girault 方案安全假设前提下无法奏效. 证毕.

定理 3. 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能够很容易恢复出所共享的秘密;(2)$(t-1)$个或更少的参与者合作却无法恢复出所共享的秘密,

甚至不能得到与该秘密相关的任何信息. 在本文方案中，要恢复出所共享的秘密，就必须首先重新构造出 n 次 Lagrange 插值多项式 $f(x)$. 由 Lagrange 内插多项式的性质可知，只有 t 个或 t 个以上的参与者合作才可以重构多项式 $f(x)$，从而恢复秘密 s；而不超过 $(t-1)$ 个参与者的合作无法重构多项式 $f(x)$，从而无法获得秘密 s 的任何信息. 因此，本文所提的方案体现了 (t,n) 门限秘密共享方案的原则. 攻击者即使与 $(t-1)$ 个参与者串通，由他们所计算的关于秘密 s 的 $(t-1)$ 个伪份额及公开信息也无法得到其他任何一个参与者的份额. 由 $(t-1)$ 个份额恢复秘密 s 相当于在 Z_Q 中随机猜测 s 获得成功，其概率仅为 $1/Q$. 因为方案中 Q 是足够大的数，因此，这种攻击成功的概率几乎为 0. $(t-1)$ 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.　　证毕.

定理 4.　在共享多个秘密时，参与者私钥的重用不会影响系统的安全性.

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
文献[1]的方案	No	Required	No	Unspecific method in advance	No
文献[4]的方案	No	Required	Yes	Unspecific method in advance	No
文献[5]的方案	No	Required	Yes	Encryption method in advance	No
文献[6]的方案	No	Not needed	Yes	Negotiation method in advance	Yes
本文方案	Yes	Not needed	Yes	No action in advance	Yes

证明.　本文方案也是一个多秘密共享方案，可使一群参与者利用他们各自的私钥共享任意多个秘密而不必更新他们的私钥. 为了共享多个秘密 $s_1, s_2, \cdots, s_k \in Z_Q$，秘密分发者在进行秘密分发时，只需在秘密分发过程的第 D1 步为每个秘密 s_i $(i=1,2,\cdots,k)$ 随机选取一个唯一的整数 r_i. 由于对称加密算法的安全性可知，在秘密的分发和重构过程中，每个参与者 P_i 的私钥不会被其它参与者或系统外的任何人计算出来. 而且，根据 Girault 密钥交换协议的安全性可知，只有秘密分发者和相应的参与者可以计算出某个特定的对称加密算法的加密密钥. 另外，即使知道某个参与者 P_i 关于若干个秘密的伪份额，也不可能计算出他的关于其它秘密的伪份额，这也是由对称加密算法的安全性决定的. 可以共享任意多个秘密而不必更新参与者的私钥是本文方案的一个优点，即秘密分发者可以动态地在 n 个参与者中共享任意秘密.　　证毕.

5　性能分析

本小节通过与现有方案进行比较来简单分析本文方案的性能. 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做一分类，然后每一类选取一个方案作为代表和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]的方案等，选取文献[1,4]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]的方案为代表；采用动态协商来建立秘密份额，以文献[6]的方案为代表. 下面，我们通过表 1 将本文方案和这些方案做一简单比较.

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身份验证，而在文献[1,4-6]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]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]的方案中，必须维护安全信道；(3) 在秘密份额重用方面，本文方案和文献[4-6]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须更新，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]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，事先无须进行任何处理，因而，效率更高；(5) 在安全性方面，文献[1,4-5]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]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 Girault 密钥交换协议，具有 DH 密钥交互的安全性，因而也继承了其前向保密性[8]. 通过分析，相比较而言，本文方案比现有这些秘密共享方案更有效、更符合实际应用.

6 结 论

本文基于 Girault 密钥交换协议提出了一个基于身份的(t,n)门限秘密共享方案. 在提出的新方案中,参与者的秘密份额不是由秘密分发者决定,而是使用他们的私钥作为秘密份额,即使秘密分发者也不能获得每个参与者的秘密份额;秘密分发者和各参与者间不需要进行任何交互,不需要在他们之间维护一条安全信道,这对于秘密分发者与参与者之间不存在安全通信信道甚至不存在任何通信信道的场合尤为有用;秘密重构过程中,任何人可以立即检验每个合作的参与者是否进行了欺骗. 利用该方案可以共享任意多个秘密,而不必修改参与者的秘密份额. 方案的安全性是基于 Girault 密钥交换协议、所采用对称加密算法和 Shamir 的(t,n)门限方案的安全性.

参 考 文 献

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

[2] Blakley G. Safeguarding cryptographic keys//Proceedings of the AFIPS 1979 National Computer Conference. New York, 1979: 313-317

[3] Fei R C, Wang L N. Cheat-proof secret share schemes based on RSA and one-way function. Journal of Software, 2003, 14(1): 146-150(in Chinese)
(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)

[4] Li H X, Pang L J, Cai W D. An efficient threshold multi-group-secret sharing scheme//Proceedings of the Advances in Soft Computing (ICFIE'07). Springer-Verlag. ASC 40, 2007: 911-918

[5] Pang L J, Wang Y M. A new (t,n) multi-secret sharing scheme based on Shamir's secret sharing. Applied Mathematics and Computation, 2005, 167(2): 840-848

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

[7] Hwang R J, Lai C H, Su F F. An efficient signcryption scheme with forward secrecy based on elliptic curve. Applied Mathematics and Computation, 2005, 167(1): 870-881

[8] Pang L J, Wang Y M. A new (t,n) multi-secret sharing scheme based on shamir's secret sharing. Applied Mathematics and Computation, 2005, 167(2): 840-848

[9] Girault. An identity-based identification scheme based on discrete logarithms modulo a composite number//Proceedings of the EUROCRYPT'90, 1991: 481-486

[10] Girault. Self-certified public keys//Proceedings of the EUROCRYPT'91, 1991: 490-497

PEI Qing-Qi, born in 1975, Ph.D., associate professor. His research interests include digital contents protection, information and network security.

MA Jian-Feng, born in 1964, Ph. D., professor. His research interests include distributed systems, wireless and mobile computing systems, computer networks, and information and network security.

PANG Liao-Jun, born in 1978, associate professor. His research interests include information and network security, sensor network.

ZHANG Hong-Bin, born in 1976, Ph. D.. His research interests include security and management of computer network.

Background

The research is supported by National Natural Science Foundation of China under grant Nos. 60803150, 60803151 and the National High Technology Research and Development Program (863 Program) of China under grant No. 2008AA01Z411, the Key Program of NSFC-Guangdong Union Foundation under grant No. U0835004 and China Postdoctoral Science Foundation No. 20090451495, the Natural Science Foundation of Shannxi Province, China under grant No. 2007F37.

A majority of existing secret sharing schemes have the following common characteristics: first, each participant's secret shadow is generated by secret dealer, who manages all participants' secret shadow. Thus enable secret dealer to need to conserve a mass of secret information, with being an attack goal of attackers; second, a secure channel is needed for secret dealer and participants. The channel is used to disseminate secret shadow, but its maintenance increases system cost and complexity.

The paper proposes a (t,n) threshold secret sharing scheme by using Girault's ID-based key exchange protocol. Our scheme uses participants' identity as the open information of their secret shadows, and secret dealer and participants do not need to communicate and exchange information, so a secure channel is not indispensable. In the process of secret reconstruction, each participant only need to submit a pseudo-shadow computed by secret shadow, and do not need discover the actual value.