基于密钥分割的多移动代理系统安全性研究

王海艳[①] 王汝传[①②]
[①](南京邮电大学计算机科学与技术系 南京 210003)
[②](中国科学院研究生院 信息安全国家重点实验室 北京 100039)

摘 要 自移动代理提出以来，安全性问题一直是制约其广泛应用的一个最主要的因素。作为分布式C/S计算模式的延伸，目前备受关注的“多移动代理”协作为提高整个移动代理系统安全性提供了一个新的思路。该文通过分析基于拉格朗日插值的密钥分割和多重签名方案应用于多移动代理系统中出现的问题，给出了一个改进的、更有实际应用价值的算法。最后，给出了一个基于此算法的电子交易的案例。

关键词 多移动代理系统，密钥分割，多重签名，安全性
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1009-5896(2006)03-0546-05

The Security Research of Multiple Mobile AgentSystem Based on Secret Splitting

Wang Hai-yan[①] Wang Ru-chuan[①②]
[①](*Dept. of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*)
[②](*State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing* 100039, *China*)

Abstract Since the introduction of Mobile Agent (MA), security is always an important issue for its restriction to the MA's wide-application. As the extension of distributed Client/Server computing, the present idea of “multiple mobile agents” gives a new way for increasing the security of the whole mobile agent system. In this paper, problems are firstly discussed in detail when applying the secret splitting scheme based on Lagrange interpolation and the subsequent multiple-signature scheme into Multiple Mobile Agent System (MMAS). Secondly, an improved and more practical scheme for the MMAS is proposed. An e-business case based on this scheme is presented at the end of this paper.

Key words Multiple Mobile Agent System (MMAS)，Secret splitting，Multi-signature，Security

1 引言

移动代理作为一种分布式计算方式，以任务为导向，允许协作程序在支持平台间具有完全的自主移动性，很容易以此构成一个大规模、松耦合的系统，被认为是软件和网络未来发展的方向，在信息检索、电子商务、网络管理等领域有着广泛的发展前景。但是正由于移动代理的自由迁移和可完全自主的在宿主机器上执行这一特性，使它无法避免网络中各种攻击和威胁。而且移动代理本身的自治性、移动性、灵活性等特点又加剧了各种安全隐患，使得安全问题成为移动代理发展的一个巨大障碍，并成为其推向商业应用的瓶颈。

一般而言，移动代理系统面临着3类安全威胁[1]：对宿主的攻击，对传输中移动代理的攻击和恶意主机对移动代理的攻击。前两类安全问题与传统的C/S(Client/Server)模式下的安全问题类似，已有各种成熟的解决方案，比如自带检验代码(Proof carrying code)技术及广泛使用的“沙盒”类似的访问控制机制, SocketSSL等方法[2]；但是，对于“恶意主机攻击移动代理”安全策略的研究仍差强人意。原因是多方面的，移动代理与执行主机之间的安全要求应当是对称的，但它们对各自的资源、数据和服务的控制却是不对称的——主机能对代理完全控制且易于掌握代理所携带的内容与信息。因此，迫切需要在移动代理系统中引入安全机制，以保证移动代码的正确性、代理所携带数据的机密性及控制流的完整性。为此，我们提出了基于多移动代理的密钥分割方案，以保护执行中的移动代理。

2 多移动代理系统

多移动代理系统(Multiple Mobile Agent System)的产生大大地提高了移动代理的安全性和执行效率。源主机根据某

2004-07-09 收到, 2005-08-17 改回
国家自然科学基金(60173037 和 70271050)，江苏省自然科学基金(BK2005146)和江苏省自然科学基金预研项目(BK2004218)，江苏省高技术研究计划(BG2004004、BG2005037、BG2005038)，国家863计划(2005AA775050)，江苏省计算机信息处理技术重点实验室基金(kjs050001) 和江苏省高校自然科学研究计划(05KJB520092)资助课题

一任务的目的与性质，创建并派遣多个移动代理，并按一定的等级和任务分配法则，使其在某一或多个主机上交互执行。通过任务分割，多移动代理系统能灵活地控制系统的效率与安全等级[3]，这就给移动代理走向应用提供了更大的可能性。

2.1　多移动代理的组织结构

多移动代理系统是由多个移动代理组成的相互协同、相互作用为完成某项特定任务或目标的系统[4]。根据系统中主代理的有无，多移动代理系统可分为两种结构：对等结构，主从结构。

(1) 多移动代理协作的对等模式(Peer to Peer Pattern)

各个移动代理之间的地位是平等的，主要表现在协作关系的对等、所携带重要信息的机密程度类似、所分派任务的繁简程度类似。这种模式易于扩展，便于组成大规模系统；但同时，系统中各子代理的通信协作完全靠自己进行，每个代理都需要有强大的通信与协调机制，当系统规模不大时效率反而不高。

(2) 多移动代理协作的主从模式(Master-Slave Pattern)

源主机创建主代理，而主代理创建从代理并把任务委派给从代理，从代理移动到指定目的地完成委派任务后将结果返回给主代理，它们之间的地位是不平等的主从关系，主要表现在主代理具有创建和调度从代理的功能，二者所携带机密信息及关键数据的不对等。这种模式便于管理，执行效率高，适用于中小规模的系统。

此外，对于主从式多移动代理系统，主代理又可分为强定义与弱定义两种。前者具有创建从代理的功能，并能依据任务性质和执行环境自主地将数据与任务分配给由它创建的从代理，一般情况下，它携带着源主机的机密信息或关键数据驻留于可信任的节点，本身并不参与具体任务的执行；而后者不具备创建从代理的功能，也不予从代理分派任务，它充当了指挥调度的角色，自身也参与任务的执行；强主代理比弱主代理具有更高的构件要求和开发难度。

2.2　多移动代理系统的任务分割

无论是主从式还是对等式多移动代理系统，任务分割都是一个及其重要的环节，区别仅仅在于进行分割的是源主机还是主代理(强定义)。当接到用户的任务请求后，源主机会根据知识领域决定是直接执行该任务、委托其它代理执行此任务还是将任务分解后再由多个移动代理合作完成。这个任务分配过程的目的就是要使系统在完成某个任务时的执行和通信开销尽量小，在保证多个移动代理之间不发生冲突的前提下，同时达到局部和全局目标。下面我们对目前已有的几种任务分配机制进行介绍。

(1)启发式任务分配算法　把任务的分解与子任务的分配过程合并为一个线性规划问题，为复杂任务的分配提供了一个可行的方法。其主体思想是把任务分配过程中应满足的条件形式化为一组约束条件，再将系统执行和通信开销定义为一个系统开销函数，最后用线性规划方法求系统开销函数在一组约束条件下的最小值，在这个最小值之下得到的任务执行计划就是最终的任务分配结果。

(2) 基于排队论的调度算法　在多移动代理系统中，如果用户提交的任务请求经常只需一个移动代理就可以完成，不需要先进行任务的分解，就可以用排队论的方法进行任务分配。这样既可以有效地选择任务的执行者，也可以使系统复杂度降低、易于实现。

排队论调度算法适合于集中模式，其主要思想是:每个移动代理都允许任务排队，称之为服务队列，移动代理根据先来先服务(FCFS)的原则依次执行自己队列中的任务。系统根据与移动代理服务队列相关的参数，在提供同种服务的多个 Agent 间选择一个队列参数最优的移动代理作为某个任务的执行者，并将该任务放到被选定移动代理的服务队列末尾。

多移动代理系统可分为对等模式与主从模式两种，其区别不仅仅在于主代理的有无，任务分割与协作及通信机制也有巨大的差异。现有的移动代理平台还未能很好地实现对等模式多移动代理系统，这就必然导致任务分割不能由移动代理间通过协议协商完成、且代理间也未能实现完全的分布式通信。所以，就目前而言，对多移动代理系统的研究主要集中于主从模式上，这就必然导致对主代理所携带的源主机秘密数据的保护，而主密钥就是这其中最重要的数据之一。

3　密钥分割与多重签名

如前所述，密钥分割与多重签名对加强多移动代理系统的安全性有着至关重要的作用。多重签名能够实现多个子签名体对同一个消息进行数字签名，而各种多重签名方式无论在复杂度、适用范围、灵活性、安全性以及实用性等方面都有着巨大的差异。一般而言，算法简单、计算容易且安全性高的算法才能有广泛的应用价值。

当然，多重签名和密钥分割是两个不同的概念，多重签名不一定要使用密钥分割，比如各子签名体可独立选择公钥及私钥，并通过广播的方式相互交换；但密钥分割的最直接的应用就是多重签名。就多移动代理系统而言，各子代理有着共同的任务，共享资源，那么必然存在一个共享的主密钥，对集中模式的多代理系统尤为如此，所以我们所讨论的多重签名是以密钥分割为基础的多重签名。在多移动代理系统中，多重签名的原理大体相似，各种算法的区别主要就在密钥分割上。总的来说，多重签名算法大致可分为两类，基于(t, n)门限的多重签名方案和一般的非门限的多重签名方案。前者有基于拉格朗日插值的(t, n)门限方案、基于RSA的门限签名方案以及ElGamal型门限方案等，而后者有ElGamal密码系统等[5]。一般而言，非门限方案在每次交易需所有子代理同时签名，虽安全性较高，但它无法根据需要灵活调整系统的安全级别，对安全级别要求低、任务复杂度高的应用反而效率低下；反观$(t，n)$门限方案，它有着许多不可比拟的优

点：t值的变化可使安全级别灵活改变，多个移动代理共享密钥，可以在没有认证中心的情况下，利用各自的子密钥进行计算，子密钥可以是一次性的，也可以被重复地使用等等，所以成为理论研究的热点。我们对基于拉格朗日插值的(t, n)门限方案进行了深入研究，在发现该方案的一个实践上的漏洞的同时，提出了一种在理论和实践都完全正确的新的门限方案。

3.1 基于拉格朗日插值的密钥分割与多重签名方案

基于拉格朗日插值[6]的密钥分割与多重签名方案有多种变形，比如LZ门限，XU门限方案等；这些方案大同小异，现举出一种典型的基于拉格朗日插值的密钥分割与多重签名方案如下：

3.1.1 *源主机的初始化阶段* (a) 源主机创建一个主代理，并根据任务的安全级别确定门限值 t； (b) 源主机选择大素数 p 与 q，满足 $2^{511}<p<2^{512}$，$2^{159}<q<2^{160}$，且 q 可将$(p-1)$整除；

(c) 依据门限值 t，源主机选择$\{a_i, i=0, 1, 2, \cdots, t-1\}$，且有 $f(x)=a_0+a_1x+\cdots+a_{t-1}x_{t-1} \pmod q$，其中 $a_i \in [1, q-1]$； (d) 源主机随机选择某整数 h，计算 $\alpha=h^{(p-1)/q} \pmod p>1$，其中，生成的 α 为在 GF(p)中阶为 q 的生成元； (e) 源主机选定 $y=\alpha^{f(0)} \pmod p$为公开密钥，并公开$\{p, q, \alpha\}$而保密$\{a_i\}$； (*f*) 源主机将密钥、相关函数、数据信息和任务信息加载至主代理。

3.1.2 *主代理创建从代理并进行密钥分割* (a) 主代理可根据任务的复杂度创建一定数量的从代理，假定为 n，其中 $n \geq t$；(b) 它任选 x_i 为公开值，为每一从代理指定其子密钥 $f(x_i)$和相应的公开子密钥 $y_i=\alpha^{f(x_i)} \pmod p$(将公钥也进行了分割)；(c) 需要数字签名时，主代理将任选 t 个从代理代表源主机到目标主机上签发文件； (d) 对于这 t 个从代理，主代理将为其随机选择一整数 $k_j \in [1, q-1]\ (1 \leq j \leq t)$，计算 $r_j=\alpha^{k_j} \pmod p$及 $r=\prod_{j=1}^{t} r_j \pmod p$，并将相应的$\{k_j, r_j, r\}$分配给对应的从代理。

3.1.3 *多个从代理协作生成(t, n)数字签名* (a) 当 t 个从代理代表源主机依次到目标主机上签发文件 m 时，每一从代理会利用自己的子密钥 $f(x_j)$和 k_j 来产生对文件 m 的签名：

$$s_j=f(x_j)m'\left(\prod_{l=1,l\neq j}^{t}\frac{-x_l}{x_j-x_l}\right)-k_jr \pmod q$$

其中$\{r_j, s_j\}$为各个从代理的数字签名，且 $m'=f(m)$；

对每一个子代理签名，可由下式进行验证：

$$y_j^{m'\left(\prod_{l=1,l\neq j}^{t}\frac{-x_l}{x_j-x_l}\right)}=r_j^{r}\alpha^{s_j} \pmod p$$

，如相等，则子签名通过，否则丢弃此签名； (b) 最后一个从代理签名之后，会将所有的子签名合并成 $S=s_1+s_2+\cdots+s_t \pmod q$；

3.1.4 *对多移动代理协作数字签名的认证* 执行主机可根据源主机公开的公钥 $y=\alpha^{f(0)} \pmod p$，来验证对文件 m 的数字签名$\{r, S\}$：$y^{m'}=r^r\alpha^s \pmod p$，若相等，则接受该签名；若不相等，则抛弃该签名。

现证明如下：已知参与数字签名的每一从代理的签名$\{r_j, s_j\}$满足 $y_j^{m'\left(\prod_{l=1,l\neq j}^{t}\frac{-x_l}{x_j-x_l}\right)}=r_j^{r}\alpha^{s_j} \pmod p$，若将上式重复对 $j=1, 2, \cdots, t$ 相乘，可以得到：

$$\prod_{j=1}^{t} y_j^{m'\left(\prod_{l=1,l\neq j}^{t}\frac{-x_l}{x_j-x_l}\right)}=\prod_{j=1}^{t} r_j^{r}\alpha^{s_j} \pmod p \Rightarrow \alpha^{m'\sum_{j=1}^{t} f(x_j)\prod_{j-1,l\neq j}^{t}\frac{-x_l}{x_j-x_l} \pmod q}$$

$$=\left(\prod_{j=1}^{t} r_j\right)^{r}\alpha^{\sum_{j=1}^{t} s_j} \pmod p \Rightarrow \alpha^{m'f(0)}=r^r\alpha^s \pmod p \Rightarrow y^{m'}$$

$$=r^r\alpha^s \pmod p。$$

3.2 小数问题

在理论上基于拉格朗日的密钥分割与多重签名方案完全正确，但密码学是基于数论的，此方案也是基于有限域理论，而在实际中，在 3.1.3 节的签名过程中应用拉格朗日插值时运用了除法运算，则不可避免的产生小数签名，则子验证无法通过。证明如下：

对任一子签名 s_j 的子验证：

设 $s_j+k_ir+uq=f(x_j)m'\prod_{l=1,l\neq j}^{t}\frac{-x_l}{x_j-x_l}$，其中 u 为整数，则

$$y_j^{m'\left(\prod_{l=1,l\neq j}^{t}\frac{-x_l}{x_j-x_l}\right)}=\alpha^{f(x_j)m'\prod_{l=1,l\neq j}^{t}\frac{-x_l}{x_j-x_l}}=\alpha^{s_j+k_jr+uq}=\alpha^{uq}\alpha^{s_j+k_jr}$$
$$=h^{(p-1)u}\alpha^{s_j+k_jr}$$

由费尔马定理，$h^{(p-1)u}=1 \pmod p$，即 $h^{(p-1)u}=vp+1$，v 为整数。

如 s_j 为整数，则 $y_j^{m'\left(\prod_{l=1,l\neq j}^{t}\frac{-x_l}{x_j-x_l}\right)}=(vp+1)\alpha^{s_j+k_jr}=\alpha^{s_j+k_jr} \cdot \pmod p$，故验证成立；

如 s_j 为小数，则 $y_j^{m'\left(\prod_{l=1,l\neq j}^{t}\frac{-x_l}{x_j-x_l}\right)}=(vp+1)\alpha^{s_j+k_jr}\neq\alpha^{s_j+k_jr} \cdot \pmod p$，则验证不成立。

而在实际中，x_i为任意值，则小数签名是不可避免的，所以此算法在实践中不可行。

3.3 基于向量相关的密钥分割与多重签名方案

由上面的分析可知，基于拉格朗日插值的算法由于在签

名过程中产生小数而在实践中不可行。为了解决这一问题，方案[7]，设计以下基于向量相关的多重签名算法。

3.3.1 源主机初始化　(a)源主机创建一个主代理，并根据任务的安全级别确定门限值t，假定 $k=t$；　(b)源主机选择一个k维非零向量$\boldsymbol{\beta}=(b_1,b_2,\cdots,b_k)^{\mathrm{T}}$；　(c)源主机选择一个$k\times n$矩阵$\boldsymbol{G}$，要求此矩阵任意$k\times k$阶子矩阵行列式不为 0，且任意$k-1$维列向量和$\boldsymbol{\beta}$线性无关；　(d) 源主机选择大素数$p$与$q$，满足 $2^{511}<p<2^{512}$，$2^{159}<q<2^{160}$，且q可将$(p-1)$整除，源主机随机选择某整数 h，计算 $\alpha=h^{(p-1)/q} \pmod p>1$，其中，生成的 α 为在GF(p)中阶为q的生成元；　(e) 源主机选择一个k维非零向量$S=(s_1,s_2,\cdots,s_k)^{\mathrm{T}}$；　(f) 主密钥：Sm= S β，主公钥为 $y=\alpha^{\mathrm{sm}} \pmod p$。

3.3.2 主代理创建从代理并进行密钥分割　(a) 主代理创建n个从代理；(b) 对各从代理，其子密钥为$(\mathbf{Ss1},\mathbf{Ss2},\cdots,\mathbf{Ssn})=(\boldsymbol{s}_1,\boldsymbol{s}_2,\cdots,\boldsymbol{s}_k)\boldsymbol{G}$；(c) 对各从代理，其子公钥为 $y_i=\alpha^{Ssi} \bmod p$；(d) 需要数字签名时，主代理将任选t个从代理代表源主机到目标主机上签发文件，并为这t个从代理计算辅助子密钥Ci；辅助子密钥和子密钥同时使用，其值公开，且它的值不会为破译子密钥提供任何信息；　(e)对于这t个从代理，主代理将为其随机选择一整数 $k_j\in[1,\ q-1]$ $(1\le j\le t)$，计算 $r_j=\alpha^{k_j} \pmod p$及 $r=\prod_{j=1}^{t} r_j \pmod p$，并将相应的$\{k_j, r_j, r\}$分配给对应的从代理。

3.3.3 多个从代理协作生成$(t,\ n)$数字签名　(a) t 个从代理代表源主机依次到目标主机上签发文件 m 时，每一从代理会利用自己的子密钥 Ssi 和辅助子密钥 Ci 来产生对文件 m 的签名：

Sgn(i)=CiSsi $m'-k_j r \pmod q$，其中 $m'=f(m)$。

对此签名可做如下验证：　$y_i^{\mathrm{Ci}\,m'}=r_i^{r}\alpha^{\mathrm{Sgn}(i)} \pmod p$，如相等则验证通过，否则丢弃此子签名；(b) 最后一个从代理签名之后，会将所有的子签名合并成 Sgn=Sgn(1)+Sgn(2) +⋯ +Sgn(t) (mod q)。

3.3.4 对多移动代理协作数字签名的认证　执行主机可根据源主机公开的公钥 y，来验证对文件 m 的数字签名$\{r$，Sgn $\}$：$y^{m'}=r^{r}\alpha^{\mathrm{Sgn}} \pmod p$，若相等，则接受该签名；若不相等，则抛弃该签名。

现对此算法做如下讨论：

(a)辅助子密钥的求法与唯一性　辅助子密钥在本算法中有着至关重要的作用。因为如果辅助子密钥不唯一，那么密钥分割就失去了意义，那么本算法也就是失败的。其求法与唯一性证明如下：

我们参考杨波、马文平和王育民所提出的一种新的密钥分割

对矩阵$\boldsymbol{G}$可知，其任意t阶子矩阵行列式不为零，那么其任意t个列向量$\boldsymbol{G}_{i1},\boldsymbol{G}_{i2},\cdots,\boldsymbol{G}_{it}$线性相关，又在$t$维向量空间中，任意$t+1$ 个向量线性相关，则$\boldsymbol{G}_{i1},\boldsymbol{G}_{i2},\cdots,\boldsymbol{G}_{it},\boldsymbol{\beta}$ 线性相关，所以方程 $\boldsymbol{x}_1\boldsymbol{G}_{i1}+x_2\boldsymbol{G}_{i2}+\cdots+x_t\boldsymbol{G}_{it}=\boldsymbol{\beta}$ 有唯一解，记为$\boldsymbol{C}=(\boldsymbol{C}1,\boldsymbol{C}2,\cdots,\boldsymbol{C}t)$，即$\boldsymbol{C}1\boldsymbol{G}_{i1}+\boldsymbol{C}2\,\boldsymbol{G}_{i2}+\cdots+\boldsymbol{C}t\,\boldsymbol{G}_{it}=\boldsymbol{\beta}$，所以辅助子密钥Ci唯一。

又因为Sm=$\boldsymbol{S}\,\boldsymbol{\beta}=(\boldsymbol{s}_1,\boldsymbol{s}_2,\cdots,\boldsymbol{s}_k)(\boldsymbol{C}1\boldsymbol{G}_{i1}+\boldsymbol{C}2\boldsymbol{G}_{i2}+\cdots+\boldsymbol{C}t\boldsymbol{G}_{it})=\boldsymbol{C}1\mathbf{S}1+\boldsymbol{C}2\mathbf{S}2+\cdots+\boldsymbol{C}t\mathbf{S}st$，且子验证 $y_i^{\mathrm{Ci}\,m'}=r_i^{r}\alpha^{\mathrm{Sgn}(i)} \pmod p$，两边相乘有：

$$\prod_{i=1}^{t} y_i^{Ci\ m'}=\prod_{i=1}^{t} r_i^{r}\alpha^{\mathrm{Sgn}(i)} \pmod p$$

$$\Rightarrow \alpha^{(\mathrm{Ss1}C1+\mathrm{Ss}2C2+\cdots+\mathrm{Sst}Ct)m'}=r^{r}\alpha^{\mathrm{Sgn}} \pmod p \Rightarrow \alpha^{m'\mathrm{Sm}}$$

$$=r^{r}\alpha^{\mathrm{Sgn}} \pmod p \Rightarrow y^{m'}=r^{r}\alpha^{\mathrm{Sgn}} \pmod p$$

所以验证成立。

(b)小数问题　令$\boldsymbol{G}t=(\boldsymbol{G}_{i1},\boldsymbol{G}_{i2},\cdots,\boldsymbol{G}_{it})$,则$\boldsymbol{C}\boldsymbol{G}t=\boldsymbol{\beta}\ \Rightarrow$ $\boldsymbol{C}=\boldsymbol{\beta}\boldsymbol{G}t^{-1}=\dfrac{\boldsymbol{\beta}\boldsymbol{G}t^{*}}{|\boldsymbol{G}t|}$。在这里，我们可以取 $\boldsymbol{G}=\begin{pmatrix}1 & 1 & \cdots & 1\\ 1 & 2 & \cdots & n\\ \vdots & \vdots & \ddots & \vdots\\ 1 & 2^{t-1} & \cdots & n^{t-1}\end{pmatrix}$，则由 Vandermonde 行列式的性质，$\boldsymbol{\beta}$ 的每个分量取 n 阶 Vandermonde 行列式值的整数倍，则可保证 C 的每个分量都为整数。

我们可以通过一个简单的实例来说明改进算法能避免小数问题：取 p=3671, q=367, t=3, n=5, 则利用基于拉格朗日插值的密钥分割和多重签名方案与改进算法的密钥分割与多重签名方案得出的签名值如表 1 所示。其中各子签名正确的值与表 1 中改进算法所对应的各子签名值相同，均为整数。

3.4 两种算法的对比研究

由上面的分析可看出，这两种算法各有千秋。基于拉格朗日插值的密钥分割和多重签名方案存在小数问题，此问题几乎不可能解决，但如若解决这一问题，它也有很多优点。首先，它的计算较后一种算法简单，没有大量费时的矩阵运算；其次，门限值 t 和子代理数 n 分别由源主机和主代理确定，即确定任务安全级别时不需要知道任务的复杂度，主代理可根据实际灵活确定，而后一种方案则需要源主机同时确定 t，n 的值，降低了主代理的功能。但如果不能解决小数问题，基于向量相关的算法似乎是更切实际的选择。

表 1　两种算法比较的一个简单实例

Table 1　A simple example of the comparison of two algorithms

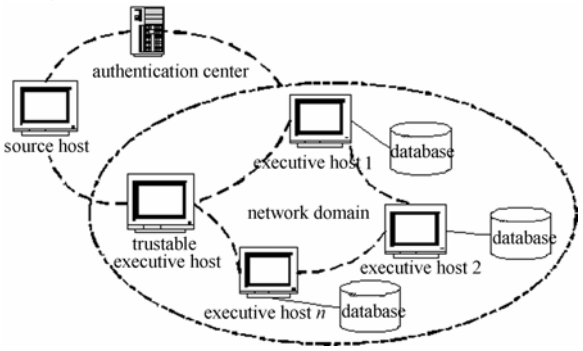
	子签名 1	子签名 2	子签名 3
基于拉格朗日插值算法	213548.19607843139	241999.62848297216	148283.26315789472

改进的算法	213282	241893	148257

4 基于多重签名的多移动代理系统的案例分析

我们可以通过一个具体的商务交易案例来分析这一过程：假定源主机(购物主机)欲在某网域内的若干执行主机上寻求“南京—北京”的最优航空票价，寻求完毕之后再与拥有最优票价的目标主机签订预定票协议，产生源主机的预定签名。源主机将创建主代理并设定密钥分割的门限值 t，并将相关函数、数据信息和任务信息加载至主代理。主代理漫游至该网域，驻留于可信任主机或服务器，根据网域内执行主机的数目创建相应数量的从代理，并将寻求“南京—北京”航空票价的数据信息与任务信息加载至从代理，派遣其到不同主机上并行执行任务。各从代理执行完任务之后，将执行结果返回给主代理，主代理对各从代理返回的结果进行合并选择，挑选出具有最优报价的执行主机作为其预定航空票的目标主机。此时进行 3.3.2，3.3.3，3.3.4 3 个步骤，任务完毕后，主代理可注销从代理返回源主机。具体的网络拓扑结构模型如图 1 所示。

在系统设计与实现时，CA 认证中心等价于 Grasshopper 平台实现的 Region Register(注册域)，源主机为移动代理的发起者(即购物主机)，执行主机 1，2，…，n 为具有电子商务信息的执行主机，它们连同可信任的主机节点，均是在 Region Register 登记注册的 Agency(Grasshopper 中的代理执行平台)。



认证中心－authentication center

源主机－source host

执行主机－executive host

可信任执行主机－trustable executive host

数据库服务器－database

网域－network domain

图 1 电子交易与认证的拓扑结构模型

Fig.1 Topologic model of the e-commerce and its authentication

5 结束语

本文着重讨论了应用多移动代理进行密钥分割并利用密码学理论的多重签名方法进行签名认证，从而提高移动代理系统的安全性问题。通过对已有的密钥分割方案分析，给出了一个实用的密钥分割的方案，构建了一个安全的可进行数字认证的多移动代理系统。同时，将多移动代理协作及多重签名机制引入到电子商务中，给出了一个具体案例。有关文中提及的小数问题及多移动代理协作问题将是今后研究工作的重点。

参 考 文 献

[1] 张云勇. 移动 agent 及其应用. 北京: 清华大学出版社, 2002: 12－14.

[2] 王汝传, 赵新宁. 基于网络的移动代理系统安全模型研究和分析. 计算机学报, 2002, 26(4): 477－483.

[3] Roth V. Mutual Protection of Co-operating Agents. Secure Internet Programming, Security Issues for Mobile and Distributed Objects, Lecture Notes in Computer Science, 1999, 1603: 275－285.

[4] Ye Y M, Yi X. Coalition Signature Scheme in Multi-agent Systems. 11th International World Wide Web Conference, Honolulu, Hawaii, USA May, 2002: 7－11.

[5] 赖溪松, 韩亮, 张真诚著, 张玉清, 肖国镇改编. 计算机密码学及其应用. 北京: 国防工业出版社, 2001: 131－138.

[6] Harn L, Lin H Y, Yang S. Threshold cryptosystem with multiple secret sharing policies. *IEE Proceedings of Computer Digital Technology*, 1994, 141(2): 142－144.

[7] 杨波, 马文平, 王育民. 一种新的密钥分割门限方案及密钥托管体制. 电子学报, 1998, 26(10): 1－3.

王海艳： 女，1974 年生，博士生，研究方向为计算机软件、计算机网络、信息安全、移动代理等.

王汝传： 男，1943 年生，教授，博士生导师，主要研究方向为计算机软件、计算机网络、信息安全、移动代理和虚拟现实技术等.