基于新型秘密共享方法的高效 RSA 门限签名方案

张文芳[*,**] 何大可[*,**] 王小敏[*] 郑 宇[**,***]
*(西南交通大学计算机与通信工程学院 成都 610031)
**(西南交通大学信息安全与国家计算网格省重点实验室 成都 610031)

摘 要：针对传统的门限RSA签名体制中需对剩余环$Z_{\varphi(N)}$中元素求逆(而环中元素未必有逆)的问题，该文首先提出一种改进的Shamir秘密共享方法。 该方法通过在整数矩阵中的一系列运算来恢复共享密钥。由于其中涉及的参数均为整数，因此避免了传统方案中由Lagrange插值公式产生的分数而引起的环$Z_{\varphi(N)}$中的求逆运算。然后基于该改进的秘密共享方法给出了一个新型的门限RSA Rivest Shanair Atleman签名方案。由于该方案无须在任何代数结构(比如$Z_{\varphi(N)}$)中对任何元素求逆，也无须进行代数扩张，因此在实际应用中更为方便、有效。

关键词：秘密共享，门限群签名，RSA，子密钥(密钥影子)，可信任中心
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5869(2005)11-1745-05

A New RSA Threshold Group Signature Scheme Based on Modified Shamir's Secret Sharing Solution

Zhang Wen-fang[*,**] He Da-ke[*,**] Wang Xiao-min[*] Zheng Yu[*,**]
*(*School of Computer and Communications Engineering, Southwest Jiaotong University, Chengdu* 610031, *China*)
**(*Laboratory of Information Security and National Computing Grid, Southwest Jiaotong University, Chengdu* 610031, *China*)

Abstract In order to avoid computing elements' inverses in the ring $Z_{\varphi(N)}$ since they may not exit, a new RSA threshold group signature scheme based on modified Shamir's secret sharing solution is proposed. Differing from the old schemes based on Lagrange interpolation solution in which fraction arithmetic operations leading to the computation of elements' inverses in $Z_{\varphi(N)}$ should be handled, this new scheme reconstructs its group secret key through series of integer arithmetic operations in integral matrixes, by which it can efficiently avoid the computation of any element's inverse in any algebraic structure (such as $Z_{\varphi(N)}$), and can further avoid algebraic extensions. Therefore, this new scheme is more efficient and convenient than the old ones.

Key words Secret sharing, Threshold group signature, RSA, Sub-key (shadow), Trusted party

1 引言

门限签名是一种由秘密共享与数字签名相结合产生的签名体制。在(t,n)门限签名方案中，群体的签名密钥被所有 n 个成员共享，使得群体中任意不少于 t 个成员的子集可以代表群体签名，而任意少于 t 个成员的子集不能代表群体产生签名，同时签名的验证者只需要知道群体的唯一公开密钥，就可以方便而简单地验证签名是否有效。

门限签名是门限密码中主要组成部分之一。门限密码最初是由以下几位学者引进的：Desmedt[1]，Boyd[2]，Croft和Harris[3]，以及Desmedt和Frankel[4]。其中文献[4]在门限密码技术方面取得了具有开创意义的成果，该文给出了一个高效的(t,n)门限ElGamal型公钥密码体制，并指出了门限RSA所面临的困难：首先，$Z_{\varphi(N)}$不是域，于是不能利用一般的秘密共享方法(比如Shamir方案)共享签名密钥d；其次，为了保护RSA (Rivest Shamir Adleman)模数N的因子分解，不能让参与签名的成员知道$\varphi(N)$。在此基础上，Desmedt和Frankel在文献[5]中对文献[4]所提出的上述困难进行了讨论。但是，文献[5]提出的方法为了克服由于RSA密钥结构引起的问题，采用了复杂、笨拙的数学结构(比如代数扩张)。文献[6,7]对门限RSA方案做了进一步研究，但是仍然没能给出更为有效的解决方法。本文所提出的方案其实是对文献[8]中方案的扩展，它不仅能够通过矩阵计算的方法高效而巧妙的解决上述问题，而且由于将秘密信息分散到$t-1$阶多项式的各个系数中，从而使其具有比文献[8]中方案更高的安全性。

本文首先构造了一个改进的 Shamir 秘密共享方法，与传

2004-05-31 收到，2004-11-19 改回

统的基于 Lagrange 插值公式的 Shamir 方法不同的是：首先，该方法将共享的秘密信息分散到$t-1$ 阶多项式的各个系数中，而不仅仅分布在常数项中，因此具有更高的安全性；其次，该方法通过在整数矩阵基础上的一系列运算来恢复共享密钥，其中涉及到的参数均为整数，从而避免了由于Lagrange插值公式产生的分数而引起的在环$Z_{\varphi(N)}$中的求逆运算。然后，基于该改进的秘密共享方法构造出一个不需要在任何代数结构(比如$Z_{\varphi(N)}$)中对任何元素求逆，进而也无须对$Z_{\varphi(N)}$进行代数扩张的门限RSA签名方案，因此更为有效，且为实现带来了方便。

2 改进的 Shamir 秘密共享方法

2.1 基于 Lagrange 插值公式的 Shamir 门限方案简介

Shamir门限方案[9]基于下面简单的数学原理：一个$t-1$次多项式，如果已知它在t个不同点的值，则可求出这个多项式(的所有系数)。

方案描述如下：设将被分割的(秘密)密钥是k，$p(p>t)$是素数，密钥分发者构造Z_p中的一个$t-1$次多项式：$f(x)=a_0+a_1x+a_2x^2+,\cdots,+a_{t-1}x^{t-1}$，并令$a_0=k, a_i\in Z_p\ (i=0,\cdots,t-1)$。设有$n\ (n>t)$个参与者，则分发者计算出该多项式在$n$个不同点$x_i$处的值$y_i=f(x_i)$，并将$(x_i,y_i)\ (i=1,\cdots,n)$分发给这$n$个参与者。多项式$f(x)$保密，$x_i$可以公开也可以不公开。$(x_i,y_i)\ (i=1,\cdots,n)$就是分割出的子密钥，也称为密钥$k$的$n$个影子(密钥)。

如果有t个参与者会合，要计算密钥k，不妨设他们的子密钥是$(x_i,y_i)\ (i=1,\cdots,t)$。假设秘密多项式为：$f(x)=a_0+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}$，将$(x_i,y_i)\ (i=1,\cdots,n)$代入，得到$t$个方程组成的方程组：

$$\begin{cases}1\cdot a_0+x_1^1a_1+x_1^2a_2+\cdots+x_1^{t-1}a_{t-1}=y_1\\1\cdot a_0+x_2^1a_1+x_2^2a_2+\cdots+x_2^{t-1}a_{t-1}=y_2\\\quad\vdots\\1\cdot a_0+x_t^1a_1+x_t^2a_2+\cdots+x_t^{t-1}a_{t-1}=y_t\end{cases}$$

由 Lagrange 插值公式得 $f(x)=\sum_{j=1}^{t}\left(\prod_{1\le l\le t,l\ne j}\frac{x-x_l}{x_j-x_l}\right)y_j$，

所以，常数项为 $k=f(0)=\sum_{j=1}^{t}\left(\prod_{1\le l\le t,l\ne j}\frac{x_l}{x_l-x_j}\right)y_j$。

令 $b_j=\prod_{1\le l\le t,l\ne j}\frac{x_l}{x_l-x_j}\bmod p$，则有 $k=\sum_{j=1}^{t}b_jy_j$。

在基于Lagrange插值公式的Shamir门限方案中需要计算 $b_j=\prod_{1\le l\le t,l\ne j}\frac{x_l}{x_l-x_j}\bmod p$ 的值，即需要在域Z_p中求(x_l-x_j)(其中$l\ne j$)在Z_p中的乘法逆元——$(x_l-x_j)^{-1}\bmod p$。

然而在RSA签名体制中，按照通常习惯，用$N=pq$表示RSA模数，其中p,q为大素数，$\varphi(N)=(p-1)(q-1)$为Euler函数，e和d分别表示公开钥和秘密钥。因此要想实现门限RSA签名体制，就要实现秘密钥(签名密钥)d的共享，同时由于$d\in Z_{\varphi(N)}$，在$Z_{\varphi(N)}$中考虑秘密共享方案是自然的，但是这有两点困难[4]：(1)由于$\varphi(N)$不是素数，因此$Z_{\varphi(N)}$是环不是域，其中的元素不一定存在乘法逆，所以难以直接在该结构上建立基于普通Shamir秘密共享方法的门限体制；(2)$\varphi(N)$必须保密，不允许签名参与者知道，因而他们无法进行模$\varphi(N)$算术。为解决这两点困难，对传统的基于Lagrange插值公式的Shamir门限方案，不得不采取以下两种方法[5]：(1)选取安全素数$p=2p'+1$，$q=2q'+1$及特殊插值点$(x_i, f(x_i))$使$(x_l-x_j)\ (l\ne j)$均在$Z_{\varphi(N)}$中可逆，并预先求出所需的逆元素；(2)对$Z_{\varphi(N)}$进行代数扩张。但这两种方法都是非常繁琐且不实用的。

因此，为克服上述困难，我们提出了一种改进的Shamir秘密共享方法，该方法通过在整数矩阵基础上的一系列运算来恢复共享密钥d，其中涉及到的参数均为整数，从而避免了由于Lagrange插值公式产生的分数而引起的在剩余环$Z_{\varphi(N)}$中的求逆运算，为建立高效实用的门限RSA签名方案提供了条件。

2.2 改进的 Shamir 秘密共享方法

设被分割的(秘密)密钥是k，选择t个数$a_0,a_1,\cdots,a_{t-1}\in Z_p$，使其满足$k=(a_0+a_1+\cdots+a_{t-1})\bmod p$，其中$p(p>t)$不一定是素数(在门限RSA签名方案中$p=\varphi(N)$)，于是在环$Z_p$上构造$t$-1 次多项式：$f(x)=a_0+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}\ (a_i\in Z_p,\ i=0,\cdots,t-1)$。其余假设同 2.1 节。

如果有t个参与者会合，要计算密钥k，不妨设他们的子密钥是$(x_i,y_i)\ (i=1,\cdots,t)$。

令$\boldsymbol{A}=(a_0,a_1,\cdots,a_{t-1})^{\mathrm{T}}$，$\boldsymbol{Y}=(y_1,y_2,\cdots,y_t)^{\mathrm{T}}$，

$$\boldsymbol{X}=\begin{bmatrix}1&x_1^1&\cdots&x_1^{t-1}\\1&x_2^1&\cdots&x_2^{t-1}\\\vdots&\vdots&\ddots&\vdots\\1&x_t^1&\cdots&x_t^{t-1}\end{bmatrix},\text{则有}$$

$$\boldsymbol{XA}=\boldsymbol{Y}\tag{1}$$

其中系数行列式为 $\pi=\begin{vmatrix}1&x_1^1&\cdots&x_1^{t-1}\\1&x_2^1&\cdots&x_2^{t-1}\\\vdots&\vdots&\ddots&\vdots\\1&x_t^1&\cdots&x_t^{t-1}\end{vmatrix}=\prod_{\substack{i,j=1,\cdots,t\\ \wedge i>j}}(x_i-x_j)$。

该行列式是范德蒙行列式，所以当$x_1,x_2,\cdots,x_t$互不相同时，其值非零。

再令$\boldsymbol{X}$在整数环上的伴随矩阵为$\boldsymbol{X}^*$，即满足

$$\boldsymbol{X}^*\boldsymbol{X}=\pi\boldsymbol{I}\ (\boldsymbol{I}\text{为单位矩阵})\tag{2}$$

其中，$\boldsymbol{X}^*=\begin{bmatrix}x_{1,1}^*&x_{1,2}^*&\cdots&x_{1,t}^*\\x_{2,1}^*&x_{2,2}^*&\cdots&x_{2,t}^*\\\vdots&\vdots&\ddots&\vdots\\x_{t,1}^*&x_{t,2}^*&\cdots&x_{t,t}^*\end{bmatrix}$，按照伴随矩阵的定义，有 $x_{i,j}^*\in Z,(i,j=1,\cdots,t)$。

通过式(1)，式(2)可以得到

$$\pi \boldsymbol{A}=\boldsymbol{X}^{*}\boldsymbol{Y} \tag{3}$$

于是，由式(3)即可得到

$$\begin{aligned}\pi k &= \pi(a_0+a_1+\cdots+a_{k-1})\\ &= y_1\sum_{j=1}^{t}x_{j,1}^{*}+y_2\sum_{j=1}^{t}x_{j,2}^{*}+\cdots+y_t\sum_{j=1}^{t}x_{j,t}^{*}=\sum_{i=1}^{t}y_i\sum_{j=1}^{t}x_{j,i}^{*}\end{aligned} \tag{4}$$

这样就可以通过t个子秘密(x_i,y_i) (i=1,⋯,t)共同恢复出共享秘密k的π倍πk，而在上述恢复过程中所用到的数y_i及 x_{ij}^{*} (1≤I ,j≤t)均为整数，因此并不需要在环Z_p中进行任何求逆操作，当然也不需要对Z_p进行代数扩张。同时，从上述过程还可以看到，该改进的Shamir秘密共享方案并没有直接恢复出k，而仅恢复出了πk，其目的是为了避免求k $\left(k=\pi^{-1}\sum_{i=1}^{t}y_i\sum_{j=1}^{t}x_{j,i}^{*} \bmod p\right)$时需要计算$\pi$在剩余环$Z_p$中的乘法逆元$\pi^{-1} \bmod p$的问题。为此，在下文所提出的基于该改进的Shamir秘密共享方法的门限RSA签名方案中，将以合理的方法构造出形式为 $S=m^{\pi d} \bmod N$ (如式(11)所示)的门限群签名，及其验证方程 $S^e \equiv m^{\pi} (\bmod N)$ (如式(9)所示)，其中d相当于上文中的k。从下文的证明过程可以看到，在这种形式的门限群签名的生成和验证中并不需要单独恢复出秘密密钥d，而只需计算出πd即可，从而进一步避免了剩余环$Z_{\varphi(N)}$中的求逆运算。该门限RSA签名方案的详细实现和证明过程由下文给出。

3　基于改进的 Shamir 秘密共享方法的门限 RSA 签名方案

3.1 系统设置和密钥生成阶段

密钥分发中心 SDC(即可信任中心)任务如下：

(1) 选择模数 $N=pq$ (p,q 为安全大素数，即 $p=2p'+1$，$q=2q'+1$， p' 且和 q' 也为大素数)和满足 $de=1 \bmod \lambda(N)$(其中 $\lambda(N)=lcm(p-1,q-1)=2p'q'$)的秘密密钥 d 和公开密钥 e；

(2) 构造$Z_{\varphi(N)}$中的$t-1$ 次多项式$f(x)=a_0+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}$ ($a_i\in Z_{\varphi(N)}$，i=1,⋯,$t-1$)，使得$a_0,a_1,\cdots,a_{t-1}$满足同余等式：$d\equiv a_0+a_1+\cdots+a_{t-1} (\bmod \varphi(N))$；

(3) 设签名群体U中共有n个成员，则选取n个较小的整数$x_i\in Z_{\varphi(N)}$ (i=1,⋯,n)作为U中成员U_i的化名，并保证各x_i互异，然后计算$y_i=f(x_i) \bmod \varphi(N)$，使$y_i$满足 0≤$y_i$≤$\varphi(N)-1$；

(4) 公开N，e和x_i (i=1,⋯,n)并将子密钥y_i秘密的发送给成员U_i。

3.2　部分签名生成阶段

(1) 产生签名的小组$U(B)$ ($|B|=t$)中的每个成员U_{Bi} ($B_i\in B$, i=1,⋯,t且$B_{i-1}<B_i$)计算部分签名：

$$S_{Bi}=m^{y_{Bi}} \bmod N,\ B_i\in B,\ i=1,\cdots,t且B_{i-1}<B_i \tag{5}$$

(2) 将部分签名$(x_{Bi},\ S_{Bi})$ ($B_i\in B$, i=1,⋯,t且$B_{i-1}<B_i$)发送给签名合成者DC。

3.3　门限群签名生成阶段

(1) 首先，签名合成者DC在整数环$Z_{\varphi(N)}$上计算π和r_{Bi} (i=1,⋯,t)的值，并使它们满足 0<π, r_{Bi}<$\varphi(N)$：

$$\pi=\prod_{Bi,Bj\in B\wedge i>j}(x_{Bi}-x_{Bj}) \bmod \varphi(N) \tag{6}$$

$$r_{Bi}=\sum_{j=1}^{t}x_{j,i}^{*} \bmod \varphi(N) \tag{7}$$

其中$x^{*}_{i,j}$为$\boldsymbol{X}=\begin{bmatrix}1 & x_{B1}^{1} & \cdots & x_{B1}^{t-1}\\ 1 & x_{B2}^{1} & \cdots & x_{B2}^{t-1}\\ \vdots & \vdots & \ddots & \vdots\\ 1 & x_{Bt}^{1} & \cdots & x_{Bt}^{t-1}\end{bmatrix}$ ($B_i\in B$, i=1,⋯,t且$B_{i-1}<B_i$)的伴随矩阵$\boldsymbol{X}^{*}$中各对应项的值。

易知，π，$x^{*}_{i,j}$和r_{Bi}的值均为整数，从而有效地避免了在环$Z_{\varphi(N)}$中的求逆运算；此外，通过对π和r_{Bi}的模$\varphi(N)$运算，可将它们化为小余$\varphi(N)$的正整数，即 0<π, r_{Bi}<$\varphi(N)$。这样做的目的是为了避免如果π或r_{Bi}为负数，则在后面计算群签名 $S=\prod_{Bi\in B\wedge i=1}^{t}S_{Bi}^{r_{Bi}} \bmod N$ 或验证群签名 $S^e\equiv m^{\pi}(\bmod N)$ 时需要进行模N的求逆运算(由于N为合数，所以Z_N也是环而不是域，其中元素不一定存在逆元)。而此时的π和r_{Bi}均已化为小余$\varphi(N)$的正整数，因此可以避免该类求逆运算。

(2) 然后，DC 计算群签名 S：

$$S=\prod_{Bi\in B\wedge i=1}^{t}S_{Bi}^{r_{Bi}} \bmod N \tag{8}$$

至此，DC 就生成了对消息 m 的门限群签名(m, S, π)。

3.4　门限群签名验证阶段

验证者根据下面同余式是否成立来验证门限签名是否有效：

$$S^e\equiv m^{\pi}(\bmod N) \tag{9}$$

4　方案的正确性

方案的正确性由下面的定理给出：

定理 1(方案的正确性)　若本方案中的 t 个成员都是诚实的，于是都产生了正确的部分签名 $S_{Bi}(B_i\in B, i=1,\cdots,t且B_{i-1}<B_i)$，则由 $S=\prod_{Bi\in B\wedge i=1}^{t}S_{Bi}^{r_{Bi}} \bmod N$ 计算出的门限群签名 S，满足门限签名验证等式：$S^e\equiv m^{\pi}(\bmod N)$。

证明 由改进的 Shamir 秘密共享理论及式(4)可知：

$$\pi d=\pi(a_0+a_1+\cdots+a_{k-1})=y_{B1}\sum_{j=1}^{t}x_{j,1}^{*}+y_{B2}\sum_{j=1}^{t}x_{j,2}^{*}+\cdots+y_{Bt}\sum_{j=1}^{t}x_{j,t}^{*}$$

$=\sum_{Bi\in B\wedge i=1}^{t}y_{Bi}\sum_{j=1}^{t}x_{j,i}^{*}$，其中$x_{i,j}^{*}$定义同 3.3 节，即在整数环$Z$上有以下等式成立：

$$\pi d=\sum_{Bi\in B\wedge i=1}^{t}y_{Bi}\sum_{j=1}^{t}x_{j,i}^{*} \tag{10}$$

因此，由式(5), (7), (8)和式(10)可得门限签名 S 满足：

$$S=\prod_{Bi\in B\wedge i=1}^{t}S_{Bi}^{r_{Bi}}\bmod N=\prod_{Bi\in B\wedge i=1}^{t}S_{Bi}^{\sum_{j=1}^{t}x_{j,i}^{*}\bmod\varphi(N)}\bmod N$$

$$=m^{\sum_{Bi\in B\wedge i=1}^{t}y_{Bi}\sum_{j=1}^{t}x_{j,i}^{*}}\bmod N=m^{\pi d}\bmod N \tag{11}$$

又由于(d,e)是 RSA 的密钥对，于是有 $de\equiv 1\bmod\varphi(N)$，即存在整数 $k\in Z$，使得：

$$de=k\varphi(N)+1 \tag{12}$$

因此，根据式(11)，式(12)即可得到：

$$S^{e}=m^{\pi ed}\bmod N=m^{k\pi\varphi(N)+\pi}\bmod N=m^{\pi}\bmod N$$

这里用到了 Fermat 小定理。至此，即证明了门限签名 $S=\prod_{Bi\in B\wedge i=1}^{t}S_{Bi}^{r_{Bi}}\bmod N$ 满足验证等式 $S^{e}\equiv m^{\pi}(\bmod N)$ 成立。

证毕

5 方案的安全性及性能分析

5.1 方案的安全性分析

定理 2 (方案的安全性) 若 RSA 假设和 DDH 假设是成立的，则本文提出的基于改进的 Shamir 秘密共享方法的门限 RSA 签名方案是安全的(即稳健的且不可伪造的)。

证明 本签名方案实际上是建立在RSA签名体制和改进的Shamir秘密共享体制的基础上的。其中可以证明改进的Shamir秘密共享体制是一种基于离散对数难题的完美的秘密共享体制(也就是分发的子密钥不会泄漏共享秘密的任何信息，或者说当已知的子密钥数目少于t时，即使为$t-1$，也不能获得关于签名密钥的任何有用信息)。由于在部分签名阶段，$U_{Bi}(Bi\in B)$提供的部分签名为 $S_{Bi}=m^{y_{Bi}}\bmod N$，因此要想从S_{Bi}中获得y_{Bi}，其难度等同于计算离散对数的复杂性。于是S_{Bi}是计算不可伪造的，且从中不能获取任何有用信息。此外，由于本方案是基于RSA的门限签名体制，想直接伪造消息m的签名 $S=m^{\pi d}\bmod N$ (其中d为签名密钥，是保密的)的难度等同于进行大整数分解的困难性(对N进行分解)，因此，当p, q为安全素数时是计算不可行的。所以，通过上述讨论可以证明，本文提出的基于改进的Shamir秘密共享方法的门限RSA签名方案是安全的。 证毕

此外，容易证明：本文方案的安全性高于或等于文献[8]中方案的安全性。

5.2 方案的性能分析

目前已有的门限RSA签名方案均是采用基于Lagrange插值公式的秘密共享方法的。然而，通过Lagrange插值公式计算得到的数值往往是分数，若想在其基础上实现门限RSA签名方案，就需要在代数结构$Z_{\varphi(N)}$中进行求逆运算。但是由于RSA密钥结构的特殊性，使得$Z_{\varphi(N)}$是环而不是域，其中的元素未必可逆，因此，就不得不对环$Z_{\varphi(N)}$进行代数扩张或对系统参数进行严格的限制并预先计算出所需的逆元素。但是，这些方法均是复杂烦琐且不易实现的。

相对于现有方案，本文提出的新型门限RSA签名方案，没有使用基于Lagrange插值公式的秘密共享方法，而是采用了基于矩阵计算的改进的Shamir秘密共享方法。该方法通过在整数矩阵上的一系列运算来恢复群体的签名密钥(秘密密钥)，其中涉及到的参数均为整数，没有分数，因此可以有效地避免在剩余类环$Z_{\varphi(N)}$中进行的求逆运算，也可以避免对$Z_{\varphi(N)}$进行的代数扩张。因此，从以上讨论可以看出，本文提出的门限RSA签名方案具有运算量小，实现方便简单的特点。

6 结束语

本文首先提出了一种改进的Shamir秘密共享方法，然后在此方法的基础上，提出了一种新的门限RSA签名方案，并讨论了该方案的正确性和安全性。由于本方案能够完全避免在任何代数结构中进行求逆运算，进而无须对环$Z_{\varphi(N)}$进行复杂的代数扩张，因此在应用中更为方便、有效。

参 考 文 献

[1] Desmedt Y. Society and group oriented cryptography: A new concept. In: Pomerance C ed., Advances in Cryptolog-Crypto'87 Proceedings, LNCS 293. Berlin, Springer-Verlag, 1988: 120-127.

[2] Boyd C. Digital multisignatures. In: Baker H and Piper F editors, Cryptography and Coding, Oxford, Clarendon Press, 1989: 241-246.

[3] Croft R A, Harris S P. Public-key cryptography and reusable shared secrets. In: Baker H and Piper F editors, Cryptography and Coding, Oxford, Clarendon Press, 1989: 189-201.

[4] Desmedt Y, Frankel Y. Threshold cryptosystems. In: Brassard G ed., Advances in Cryptology-Crypto'89 Proceedings, LNCS 435. Berlin, Springer-Verlag, 1990: 307-315.

[5] Desmedt Y, Frankel Y. Shared generation of authenticators and signatures. In: Feigenbaum J ed., Advances in Cryptology - Crypto'91 Proceedings, Lecture Notes in Computer Science 576, Berlin, Springer-Verlag, 1992: 457- 469.

[6] Santis A D, Desmedt Y, Frankel Y, *et al*.. How to share a function securely. In: Proceedings of the 26th ACM Symp on Theory of Computing, Montreal, Quebec, Canada, 1994: 522- 533.

[7] Gennaro R, Jarecki S, Krawczyk H, *et a1*.. Robust and efficient sharing of RSA functions. In: Koblitz N ed., Advances in Cryptology-Crypto'96 Proceedings. Lecture Notes in Computer Science 1109. Berlin, Springer-Verlag, 1996: 157-172.

[8] 徐秋亮. 改进门限 RSA 数字签名体制. 计算机学报, 2000, 23(5): 449-453.

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

张文芳： 女，1978 年生，博士生，研究方向为网络信息安全与通信保密、秘密分享与门限密码学.

何大可： 男，1944 年生，教授，博士生导师，长期从事通信系统安全保密、网络信息安全与保密、密码设计与密码分析等领域的研究工作.

王小敏： 男，1974 年生，博士生，研究方向为虚拟企业敏捷制造及网络信息安全.

郑　宇： 男，1979 年生，博士生，研究方向为无线网络安全、PKI 及数字证书.